KOMISJA
EUROPEJSKA

Bruksela, dnia 15.9.2022 r.
COM(2022) 454 final

2022/0272 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020

(Tekst mający znaczenie dla EOG)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Sprzęt i oprogramowanie coraz częściej padają celem udanych cyberataków, które do 2021 r. doprowadziły do szacowanego globalnego rocznego kosztu cyberprzestępczości w wysokości 5,5 bln EUR. Z takimi produktami wiążą się dwa główne problemy zwiększające koszty dla użytkowników i społeczeństwa: 1) niski poziom cyberbezpieczeństwa, który przejawia się w powszechnych podatnościach oraz niewystarczającym i niespójnym dostarczaniu aktualizacji zabezpieczeń w celu wyeliminowania tych podatności, oraz 2) niedostateczne zrozumienie i dostęp do informacji przez użytkowników, co uniemożliwia im wybór produktów o odpowiednich właściwościach w zakresie cyberbezpieczeństwa lub korzystanie z nich w sposób bezpieczny. W środowisku połączonym z siecią cyberincydent dotyczący jednego produktu może mieć wpływ na całą organizację lub cały łańcuch dostaw i często w ciągu kilku minut rozprzestrzenia się poza granice rynku wewnętrznego. Może to prowadzić do poważnych zakłóceń w działalności gospodarczej i społecznej, a nawet zagrażać życiu.

Cyberbezpieczeństwo produktów z elementami cyfrowymi ma wyraźny wymiar transgraniczny, ponieważ produkty wytwarzane w jednym państwie są często wykorzystywane na całym rynku wewnętrznym. Ponadto incydenty początkowo dotyczące pojedynczego podmiotu lub jednego państwa członkowskiego często w ciągu kilku minut rozprzestrzeniają się na cały rynek wewnętrzny.

Chociaż obowiązujące przepisy dotyczące rynku wewnętrznego mają zastosowanie do niektórych produktów z elementami cyfrowymi, większość sprzętu i oprogramowania nie jest obecnie objęta żadnymi przepisami UE regulującymi ich cyberbezpieczeństwo. W szczególności obecne ramy prawne UE nie odnoszą się do cyberbezpieczeństwa oprogramowania niewbudowanego, nawet jeśli naruszenia bezpieczeństwa w wyniku cyberataku w coraz większym stopniu są wymierzone w podatności tych produktów, co powoduje znaczne koszty społeczne i gospodarcze. Jest wiele przykładów istotnych cyberataków będących wynikiem nieoptymalnego bezpieczeństwa produktu, takich jak robak oprogramowania szantażującego WannaCry, który wykorzystał podatność Windows i w 2017 r. zainfekował 200 000 komputerów w 150 krajach, powodując szkody o wartości miliardów USD, atak na łańcuch dostaw Kaseya VSA, podczas którego użyto oprogramowania zarządzającego siecią Kaseya do zaatakowania ponad 1 000 przedsiębiorstw i zmuszenia sieci supermarketów do zamknięcia wszystkich należących do niej 500 sklepów w całej Szwecji, lub liczne incydenty hakowania aplikacji bankowych w celu kradzieży środków pieniężnych od nieświadomych konsumentów.

Wskazano dwa główne cele służące zapewnieniu prawidłowego funkcjonowania rynku wewnętrznego: 1) stworzenie warunków dla rozwoju bezpiecznych produktów z elementami cyfrowymi przez zapewnienie, aby sprzęt i oprogramowanie były wprowadzane do obrotu z mniejszą liczbą podatności, a także aby producenci poważnie traktowali bezpieczeństwo w całym cyklu życia produktu, oraz 2) stworzenie warunków umożliwiających użytkownikom uwzględnianie cyberbezpieczeństwa przy wyborze produktów z elementami cyfrowymi i korzystaniu z nich. Określono cztery cele szczegółowe: (i) zapewnienie, aby producenci poprawiali bezpieczeństwo produktów z elementami cyfrowymi, począwszy od etapu projektowania i opracowywania oraz przez cały cykl życia; (ii) zapewnienie spójnych ram cyberbezpieczeństwa, ułatwiających producentom sprzętu i oprogramowania przestrzeganie

przepisów; (iii) zwiększenie przejrzystości zabezpieczeń produktów z elementami cyfrowymi oraz (iv) umożliwienie przedsiębiorstwom i konsumentom bezpiecznego korzystania z produktów z elementami cyfrowymi.

Wyraźnie transgraniczny charakter cyberbezpieczeństwa i coraz częstsze incydenty, których skutki uboczne są odczuwalne w innych krajach oraz dotykają inne sektory i produkty, oznaczają, że państwa członkowskie nie są w stanie skutecznie osiągnąć wspomnianych celów samodzielnie. Biorąc pod uwagę globalny charakter rynków produktów z elementami cyfrowymi, państwa członkowskie stoją w obliczu takiego samego ryzyka w przypadku tego samego produktu z elementami cyfrowymi na swoim terytorium. Pojawiające się rozdrobione ramy potencjalnie rozbieżnych przepisów krajowych mogą zakłócić otwarty i konkurencyjny jednolity rynek produktów z elementami cyfrowymi. Wspólne działanie na szczeblu UE jest zatem konieczne, aby wzbudzić większe zaufanie użytkowników i poprawić atrakcyjność unijnych produktów z elementami cyfrowymi. Przyniosłoby to również korzyści rynkowi wewnętrznemu, gdyż zapewniłoby pewność prawa i równe warunki działania sprzedawcom produktów z elementami cyfrowymi, co podkreślono również w sprawozdaniu końcowym Konferencji w sprawie przyszłości Europy, w którym obywatele wzywają do zwiększenia roli UE w przeciwdziałaniu zagrożeniom cyberbezpieczeństwa.

- **Wzajemne powiązania z przepisami obowiązującymi w tej dziedzinie polityki**

Na ramy UE składa się szereg horyzontalnych aktów prawnych, które obejmują niektóre aspekty związane z cyberbezpieczeństwem z różnych punktów widzenia (produkty, usługi, zarządzanie kryzysowe i przestępstwa). W 2013 r. weszła w życie dyrektywa dotycząca ataków na systemy informatyczne[1], którą ujednolicono podejście do kryminalizacji i kar za szereg przestępstw przeciwko systemom informatycznym. W sierpniu 2016 r. weszła w życie dyrektywa (UE) 2016/1148 w sprawie bezpieczeństwa sieci i systemów informatycznych („dyrektywa w sprawie bezpieczeństwa sieci i informacji")[2], która stanowiła pierwszy akt prawny w ogólnounijnych przepisach dotyczących cyberbezpieczeństwa. Trwa proces rewizji tej dyrektywy – w zmienionej dyrektywie [dyrektywie XXX/XXXX (NIS 2)] podniesiony zostanie wspólny unijny poziom ambicji. W 2019 r. wszedł w życie unijny akt o cyberbezpieczeństwie[3], którego celem jest zwiększenie bezpieczeństwa produktów ICT, usług ICT i procesów ICT przez wprowadzenie dobrowolnych europejskich ram certyfikacji cyberbezpieczeństwa[4].

O zapewnieniu cyberbezpieczeństwa całego łańcucha dostaw można mówić tylko wówczas, gdy wszystkie jego elementy są cyberbezpieczne. W wyżej wymienionych przepisach UE

---

1 Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).

2 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194/1 z 19.7.2016, s. 1).

3 Rozporządzenie 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 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

4 Akt o cyberbezpieczeństwie umożliwia opracowanie specjalnych programów certyfikacji. Każdy program zawiera odesłanie do odpowiednich norm, specyfikacji technicznych lub innych wymogów cyberbezpieczeństwa określonych w programie. Decyzja o opracowaniu certyfikacji cyberbezpieczeństwa jest decyzją opartą na analizie ryzyka.

występują jednak znaczące luki w tym zakresie, ponieważ nie obejmują one obowiązkowych wymogów dotyczących bezpieczeństwa produktów z elementami cyfrowymi.

Chociaż proponowany akt dotyczący cyberodporności obejmuje produkty z elementami cyfrowymi wprowadzane do obrotu, celem dyrektywy [dyrektywy XXX/XXX (NIS 2)] jest zapewnienie wysokiego poziomu cyberbezpieczeństwa usług świadczonych przez podmioty niezbędne i istotne. W dyrektywie [dyrektywie XXX/XXXX (NIS 2)] zobowiązano państwa członkowskie do zapewnienia, aby podmioty niezbędne i istotne objęte zakresem jej stosowania, takie jak świadczeniodawcy opieki zdrowotnej lub dostawcy usług w chmurze oraz podmioty administracji publicznej, wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w zakresie cyberbezpieczeństwa. Środki te obejmują między innymi wymóg zapewnienia bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku wykrycia podatności i ich ujawnianie. W dyrektywie [dyrektywie XXX/XXXX (NIS 2)] zobowiązano Komisję do przyjęcia aktów wykonawczych określających wymogi techniczne i metodyczne dotyczące tych środków w terminie 21 miesięcy od daty wejścia w życie tej dyrektywy w odniesieniu do niektórych rodzajów podmiotów, takich jak dostawcy usług w chmurze. W odniesieniu do wszystkich innych podmiotów Komisja może przyjąć akt wykonawczy określający wymogi techniczne i metodyczne, jak również wymogi sektorowe. Ramy te zapewnią wdrożenie specyfikacji technicznych i środków podobnych do zasadniczych wymogów cyberbezpieczeństwa określonych w akcie dotyczącym cyberodporności również w odniesieniu do projektowania, opracowywania i postępowania w przypadku wykrycia podatności oprogramowania dostarczanego jako usługa (oprogramowanie jako usługa). Może to być na przykład środek zapewniający wysoki poziom cyberbezpieczeństwa w takich przypadkach jak systemy elektronicznej dokumentacji medycznej (EHR), w tym gdy są dostarczane w postaci oprogramowania jako usługa (SaaS) lub opracowywane w ramach instytucji zdrowia publicznego (wewnętrznie), zgodnie z proponowanym [rozporządzeniem w sprawie europejskiej przestrzeni danych dotyczących zdrowia].

- **Wzajemne powiązania z innymi politykami Unii**

Jak określono w komunikacie zatytułowanym „Kształtowanie cyfrowej przyszłości Europy”[5], Unia musi wykorzystać wszystkie możliwości, jakie daje epoka cyfrowa, a także wzmocnić swoje zdolności przemysłowe i innowacyjne, w granicach bezpieczeństwa i norm etycznych. W europejskiej strategii w zakresie danych wskazano cztery filary – ochronę danych, prawa podstawowe, bezpieczeństwo i cyberbezpieczeństwo – jako podstawowe warunki wstępne istnienia społeczeństwa posiadającego mocną pozycję dzięki korzystaniu z danych.

Obecne ramy UE[6] mające zastosowanie do produktów, które mogą również zawierać elementy cyfrowe, obejmują szereg aktów prawnych, w tym przepisy UE dotyczące konkretnych produktów, obejmujące aspekty związane z bezpieczeństwem oraz ogólne przepisy dotyczące odpowiedzialności za produkty. Niniejszy wniosek jest spójny z obecnymi unijnymi ramami regulacyjnymi dotyczącymi produktów, a także z niedawno

[5] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Kształtowanie cyfrowej przyszłości Europy” z 19 lutego 2020 r., COM(2020) 67 final.

[6] Głównie przepisy nowych ram prawnych.

przedstawionymi wnioskami ustawodawczymi, jak np. wniosek Komisji dotyczący rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji][7].

Proponowane rozporządzenie miałoby zastosowanie do wszystkich urządzeń radiowych objętych zakresem stosowania rozporządzenia delegowanego Komisji (UE) 2022/30. Ponadto wymogi określone w proponowanym rozporządzeniu obejmują wszystkie elementy zasadniczych wymagań, o których mowa w art. 3 ust. 3 lit. d), e) i f) dyrektywy 2014/53/UE, w tym główne elementy określone w [decyzji wykonawczej Komisji XXX/2022 w sprawie wniosku o normalizację do europejskich organizacji normalizacyjnych] wydanej na podstawie tego rozporządzenia delegowanego. Aby uniknąć nakładania się przepisów, przewiduje się, że Komisja uchyli lub zmieni wspomniane rozporządzenie delegowane w odniesieniu do urządzeń radiowych objętych proponowanym rozporządzeniem, tak aby to nowe rozporządzenie miało do nich zastosowanie, gdy zacznie obowiązywać.

Ponadto, aby uniknąć powielania prac, przewiduje się, że Komisja i europejskie organizacje normalizacyjne uwzględnią prace normalizacyjne przeprowadzone w kontekście decyzji wykonawczej Komisji C(2022) 5637 w sprawie wniosku o normalizację odnośnie do rozporządzenia delegowanego (UE) 2022/30 dotyczącego dyrektywy w sprawie urządzeń radiowych przy przygotowywaniu i opracowywaniu norm zharmonizowanych w celu ułatwienia wykonania niniejszego rozporządzenia.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawę prawną niniejszego wniosku stanowi art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), w którym przewidziano przyjęcie środków mających na celu zapewnienie ustanowienia i funkcjonowania rynku wewnętrznego. Celem wniosku jest ujednolicenie wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi we wszystkich państwach członkowskich oraz usunięcie przeszkód w swobodnym przepływie towarów.

Art. 114 TFUE może być stosowany jako podstawa prawna, aby zapobiegać występowaniu takich przeszkód wynikających z niejednolitego rozwoju ustawodawstw krajowych i rozbieżnych podejść do rozwiązania problemu braku pewności prawa i luk w istniejących ramach prawnych[8]. Ponadto Trybunał Sprawiedliwości uznał, że niejednolite stosowanie wymagań technicznych może stanowić ważną przesłankę do zastosowania art. 114 TFUE[9].

Obecne ramy prawne UE mające zastosowanie do produktów z elementami cyfrowymi opierają się na art. 114 TFUE i obejmują szereg aktów prawnych, w tym przepisy dotyczące konkretnych produktów i obejmujące aspekty związane z bezpieczeństwem czy ogólne przepisy dotyczące odpowiedzialności za produkty. Obejmują one jednak tylko niektóre aspekty związane z cyberbezpieczeństwem materialnych produktów cyfrowych i, w stosownych przypadkach, oprogramowania wbudowanego w te produkty. Na szczeblu

---

[7] Wniosek z 21 kwietnia 2021 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii, COM(2021) 206 final.

[8] Wyrok Trybunału Sprawiedliwości Unii Europejskiej (wielka izba) z dnia 3 grudnia 2019 r., Republika Czeska/Parlament Europejski i Rada Unii Europejskiej, sprawa C-482/17, pkt 35.

[9] Wyrok Trybunału Sprawiedliwości Unii Europejskiej (wielka izba) z dnia 2 maja 2006 r., Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej/Parlament Europejski i Rada Unii Europejskiej, sprawa C-217/04, pkt 62–63.

krajowym państwa członkowskie zaczynają wprowadzać środki krajowe, którymi nakładają na sprzedawców produktów cyfrowych wymóg zwiększenia cyberbezpieczeństwa[10]. Jednocześnie cyberbezpieczeństwo produktów cyfrowych ma szczególnie wyraźny wymiar transgraniczny, ponieważ produkty wytwarzane w jednym państwie są często wykorzystywane przez organizacje i konsumentów na całym rynku wewnętrznym. Incydenty, które początkowo dotyczą jednego podmiotu lub państwa członkowskiego, często w ciągu kilku minut rozprzestrzeniają się na inne organizacje, sektory i państwa członkowskie.

Różne akty przyjęte dotychczas na szczeblu unijnym i krajowym oraz różne unijne i krajowe inicjatywy jedynie częściowo rozwiązują stwierdzone problemy i stwarzają ryzyko niejednolitego rozwoju ustawodawstwa na rynku wewnętrznym, co pogłębia brak pewności prawa po stronie zarówno sprzedawców, jak i użytkowników tych produktów, a także wiąże się z nakładaniem na przedsiębiorstwa niepotrzebnych obciążeń związanych z przestrzeganiem szeregu wymogów dotyczących podobnych rodzajów produktów.

Proponowane rozporządzenie może się przyczynić do ujednolicenia i usprawnienia otoczenia regulacyjnego UE przez wprowadzenie wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi, a także do uniknięcia nakładania się wymogów wynikających z różnych aktów prawnych. To z kolei może zagwarantować większą pewność prawa podmiotom gospodarczym i użytkownikom w całej Unii, a także umożliwić lepszą harmonizację jednolitego rynku europejskiego, co przełoży się na dogodniejsze warunki dla podmiotów chcących wejść na rynek UE.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

Wyraźnie transgraniczny charakter cyberbezpieczeństwa w ujęciu ogólnym i rosnąca liczba zagrożeń i incydentów, których skutki uboczne są odczuwalne w innych krajach oraz dotykają inne sektory i produkty, oznaczają, że państwa członkowskie nie są w stanie skutecznie osiągnąć celów niniejszego wniosku samodzielnie. Krajowe podejścia do rozwiązywania tych problemów, w szczególności podejścia zakładające wprowadzanie obowiązkowych wymogów, pogłębią brak pewności prawa i stworzą dodatkowe bariery prawne. Przedsiębiorstwa mogą stracić możliwość płynnej ekspansji na inne państwa członkowskie, co pozbawi użytkowników korzyści płynących z oferowanych przez nie produktów.

Wspólne działanie na szczeblu UE jest zatem konieczne, aby wzbudzić większe zaufanie użytkowników i poprawić atrakcyjność unijnych produktów z elementami cyfrowymi. Przyniosłoby to również korzyści jednolitemu rynkowi cyfrowemu i całemu rynkowi wewnętrznemu, gdyż zapewniłoby pewność prawa i równe warunki działania producentom produktów z elementami cyfrowymi.

Ponadto w konkluzjach Rady z dnia 23 maja 2022 r. o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni wezwano Komisję do zaproponowania do końca 2022 r. wspólnych wymogów cyberbezpieczeństwa w odniesieniu do urządzeń podłączonych do internetu.

[10] Na przykład w 2019 r. Finlandia opracowała system etykietowania urządzeń IoT, takich jak inteligentne telewizory, smartfony i zabawki, oparty na normach ETSI. Niemcy wprowadziły niedawno etykietę bezpieczeństwa dla konsumentów w odniesieniu do routerów szerokopasmowych, inteligentnych telewizorów, aparatów fotograficznych, głośników, zabawek, a także robotów sprzątających i ogrodowych.

- **Proporcjonalność**

Jeżeli chodzi o proporcjonalność proponowanego rozporządzenia, środki przewidziane w rozważanych wariantach strategicznych nie wykraczałyby poza to, co jest konieczne do osiągnięcia celów ogólnych i szczegółowych, i nie wiązałyby się z nieproporcjonalnymi kosztami. Dokładniej rzecz ujmując, rozważana interwencja zapewniłaby zabezpieczenie produktów z elementami cyfrowymi w całym ich cyklu życia i w sposób proporcjonalny do występującego ryzyka dzięki ukierunkowanym na osiągnięcie celów i neutralnym pod względem technologicznym wymogom, które pozostają rozsądne i zasadniczo odpowiadają interesom zaangażowanych podmiotów.

Zasadnicze wymogi cyberbezpieczeństwa zawarte we wniosku opierają się na powszechnie stosowanych normach, a ponadto w późniejszym procesie normalizacyjnym uwzględniono by specyfikę techniczną przedmiotowych produktów. Oznacza to, że tam gdzie jest to konieczne z uwagi na dany poziom ryzyka, środki kontroli bezpieczeństwa zostałyby dostosowane. Ponadto planowane przepisy horyzontalne przewidują ocenę przez stronę trzecią jedynie w przypadku produktów krytycznych. Obejmuje to jedynie wąski fragment rynku produktów z elementami cyfrowymi. Wpływ na MŚP będzie zależał od ich obecności na rynku tych konkretnych kategorii produktów.

Jeżeli chodzi o proporcjonalność kosztów oceny zgodności, przy ustalaniu wysokości pobieranych opłat jednostki notyfikowane przeprowadzające takie oceny jako strona trzecia brałyby pod uwagę wielkość przedsiębiorstwa. Przewidziano również rozsądny okres przejściowy wynoszący 24 miesiące na przygotowanie się do wdrożenia, co powinno zapewnić właściwym rynkom czas na przygotowanie się przy jednoczesnym wskazaniu jasnego kierunku inwestycji w badania i rozwój. Wszelkie koszty przestrzegania przepisów ponoszone przez przedsiębiorstwa zostałyby zrównoważone korzyściami płynącymi z wyższego poziomu bezpieczeństwa produktów z elementami cyfrowymi, a ostatecznie wzrostem zaufania użytkowników do tych produktów.

- **Wybór instrumentu**

Interwencja regulacyjna wymaga przyjęcia rozporządzenia, a nie dyrektywy. Wynika to z faktu, że w przypadku tego konkretnego rodzaju przepisów dotyczących produktów rozporządzenie umożliwia skuteczniejsze rozwiązanie zidentyfikowanych problemów i osiągnięcie wyznaczonych celów, ponieważ jest to interwencja warunkująca wprowadzanie na rynek wewnętrzny bardzo szerokiej kategorii produktów. Proces transpozycji w przypadku dyrektywy w odniesieniu do takiej interwencji mógłby pozostawić zbyt dużą swobodę uznania na szczeblu krajowym, potencjalnie prowadząc do braku jednolitości niektórych zasadniczych wymogów cyberbezpieczeństwa, braku pewności prawa, dalszej fragmentacji lub nawet dyskryminacji w wymiarze transgranicznym, tym bardziej biorąc pod uwagę fakt, że produkty objęte tą interwencją mogą mieć wielorakie przeznaczenie lub zastosowanie oraz że producenci mogą produkować wiele kategorii takich produktów.

3. WYNIKI OCEN *EX POST,* KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Konsultacje z zainteresowanymi stronami**

Komisja przeprowadziła konsultacje z wieloma zainteresowanymi stronami. Zaproszono państwa członkowskie i zainteresowane strony do udziału w otwartych konsultacjach publicznych oraz w ankietach i warsztatach zorganizowanych w kontekście badania przeprowadzonego przez konsorcjum wspierające prace przygotowawcze Komisji w zakresie oceny skutków w składzie: Wavestone, Centrum Studiów nad Polityką Europejską (CEPS)

oraz ICF. Przeprowadzono konsultacje między innymi z następującymi zainteresowanymi stronami: krajowymi organami nadzoru rynku, organami unijnymi zajmującymi się cyberbezpieczeństwem, producentami sprzętu i oprogramowania, importerami i dystrybutorami sprzętu i oprogramowania, stowarzyszeniami branżowymi, organizacjami konsumenckimi i użytkownikami produktów z elementami cyfrowymi i obywatelami, badaczami i środowiskiem akademickim, jednostkami notyfikowanymi i jednostkami akredytującymi oraz specjalistami z branży cyberbezpieczeństwa.

Konsultacje obejmowały:

- pierwsze badanie przeprowadzone przez konsorcjum w składzie ICF, Wavestone, Carsa i CEPS, opublikowane w grudniu 2021 r.[11], w którym zidentyfikowano szereg niedoskonałości rynku i oceniono możliwość interwencji regulacyjnej;
- otwarte konsultacje publiczne z udziałem obywateli, zainteresowanych stron i ekspertów w dziedzinie cyberbezpieczeństwa, w których otrzymano 176 odpowiedzi i dzięki którym udało się zgromadzić różne opinie i doświadczenia wszystkich grup zainteresowanych stron;
- warsztaty zorganizowane w ramach badania wspierającego prace przygotowawcze Komisji nad aktem dotyczącym cyberodporności, w których wzięło udział około 100 przedstawicieli ze wszystkich 27 państw członkowskich reprezentujących różne zainteresowane strony;
- rozmowy ze specjalistami, które pozwoliły lepiej zrozumieć obecne wyzwania w zakresie cyberbezpieczeństwa związane z produktami z elementami cyfrowymi oraz omówić warianty strategiczne dotyczące potencjalnej interwencji regulacyjnej;
- dwustronne rozmowy z krajowymi organami ds. cyberbezpieczeństwa, sektorem prywatnym i organizacjami konsumenckimi;
- ukierunkowane działania informacyjne skierowane do głównych zainteresowanych stron będących MŚP.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Celem konsultacji było uzyskanie informacji na temat pięciu głównych kryteriów oceny opartych na wytycznych UE dotyczących lepszego stanowienia prawa (skuteczność, efektywność, adekwatność, spójność, wartość dodana UE), a także potencjalnych przyszłych skutków możliwych wariantów. Wykonawca nie tylko dotarł do zainteresowanych stron, na które proponowane rozporządzenie miałoby bezpośredni wpływ, ale także przeprowadził konsultacje z szerokim gronem ekspertów w dziedzinie cyberbezpieczeństwa.

- **Ocena skutków**

Komisja przeprowadziła ocenę skutków w odniesieniu do niniejszego wniosku, która została zbadana przez działającą przy Komisji Radę ds. Kontroli Regulacyjnej. W dniu 6 lipca 2022 r.

[11] „Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715" (Badanie dotyczące potrzeby wprowadzenia wymogów cyberbezpieczeństwa w odniesieniu do produktów ICT – nr 2020-0715), sprawozdanie końcowe z badania, dostępne pod adresem https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products

odbyło się spotkanie z Radą ds. Kontroli Regulacyjnej, po którym Rada wydała pozytywną opinię. Ocenę skutków dostosowano tak, aby uwzględnić w niej zalecenia i uwagi Rady.

Komisja przeanalizowała różne warianty strategiczne osiągnięcia ogólnego celu niniejszego wniosku:

- Podejście oparte na prawie miękkim i środki dobrowolne (wariant 1): w przypadku tego wariantu nie zakłada się interwencji regulacyjnej o charakterze obowiązkowym. Zamiast tego Komisja wydawałaby komunikaty, wytyczne, zalecenia i potencjalne kodeksy postępowania w celu zachęcania do stosowania środków dobrowolnych. Systemy krajowe, dobrowolne lub obowiązkowe, byłyby nadal opracowywane, aby zrekompensować brak unijnych przepisów horyzontalnych.
- Interwencja regulacyjna *ad hoc* dotycząca cyberbezpieczeństwa materialnych produktów z elementami cyfrowymi i odpowiedniego oprogramowania wbudowanego (wariant 2): wariant ten wiązałby się z interwencją regulacyjną *ad hoc* dotyczącą konkretnych produktów, która ograniczałaby się do dodania lub zmiany wymogów cyberbezpieczeństwa w już istniejących przepisach lub wprowadzenia nowych przepisów w miarę pojawiania się nowych zagrożeń, w tym potencjalnie dotyczących oprogramowania niewbudowanego.

Warianty 3 i 4 wiążą się z horyzontalną interwencją regulacyjną o różnym zakresie, w dużej mierze zgodną z nowymi ramami prawnymi. W ramach tych określono zasadnicze wymogi jako warunek wprowadzania niektórych produktów na rynek wewnętrzny. W nowych ramach prawnych zazwyczaj przewiduje się również ocenę zgodności – proces przeprowadzany przez producenta w celu wykazania, czy spełniono określone wymogi dotyczące produktu.

- Podejście mieszane, w tym horyzontalne przepisy bezwzględnie obowiązujące dotyczące cyberbezpieczeństwa materialnych produktów z elementami cyfrowymi i odpowiedniego oprogramowania wbudowanego, a także podejście stopniowe do oprogramowania niewbudowanego (wariant 3): wariant ten zakładałby przyjęcie rozporządzenia wprowadzającego horyzontalne wymogi cyberbezpieczeństwa w odniesieniu do wszystkich materialnych produktów z elementami cyfrowymi i wbudowanego w nie oprogramowania jako warunek wprowadzenia do obrotu i obejmowałby dwa podwarianty z obowiązkową oceną przeprowadzoną przez stronę trzecią i bez takiej oceny (3(i) i 3(ii)). Oprogramowanie niewbudowane nie byłoby uregulowane.
- Horyzontalna interwencja regulacyjna wprowadzająca wymogi cyberbezpieczeństwa w odniesieniu do szerokiego zakresu materialnych i niematerialnych produktów z elementami cyfrowymi, w tym oprogramowania niewbudowanego (wariant 4): wariant ten przypomina wariant 3, z wyjątkiem zakresu. Wariant 4 zakładałby uwzględnienie oprogramowania niewbudowanego (z dwoma podwariantami obejmującymi odpowiednio tylko krytyczne (4a) lub całe oprogramowanie (4b)) w zakresie stosowania potencjalnego rozporządzenia. W przypadku każdego z podwariantów rozważono by te same podwarianty związane z oceną zgodności, co w przypadku wariantu 3.

Wariant 4 (w tym podwarianty obejmujące całe oprogramowanie i zakładające obowiązkową ocenę przez stronę trzecią w przypadku produktów krytycznych) okazał się wariantem preferowanym na podstawie oceny skuteczności względem celów szczegółowych oraz

efektywności kosztów w stosunku do korzyści. Wariant ten zapewnił określenie szczegółowych horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do wszystkich produktów z elementami cyfrowymi wprowadzanych do obrotu lub udostępnianych na rynku wewnętrznym i jest jedynym wariantem obejmującym cały cyfrowy łańcuch dostaw. Taka interwencja regulacyjna obejmowałaby również oprogramowanie niewbudowane, często narażone na podatności, a tym samym zapewniłaby spójne podejście do wszystkich produktów z elementami cyfrowymi z wyraźnym podziałem odpowiedzialności różnych podmiotów gospodarczych.

Ten wariant strategiczny wnosi również wartość dodaną, ponieważ obejmuje aspekty dotyczące dochowania należytej staranności i całego cyklu życia po wprowadzeniu do obrotu produktów z elementami cyfrowymi, aby zapewnić między innymi odpowiednie informacje na temat wsparcia w zakresie zabezpieczeń i zapewnienia aktualizacji zabezpieczeń. Ten wariant strategiczny byłby również najskuteczniejszym uzupełnieniem niedawnego przeglądu ram prawnych dotyczących bezpieczeństwa sieci i systemów informatycznych dzięki zapewnieniu warunków wstępnych wzmocnienia bezpieczeństwa łańcucha dostaw.

Preferowany wariant może przynieść znaczące korzyści dla poszczególnych zainteresowanych stron. W przypadku przedsiębiorstw pozwoli on zapobiec rozbieżnym przepisom dotyczącym bezpieczeństwa produktów z elementami cyfrowymi oraz obniżyć koszty przestrzegania związanych z nimi przepisów dotyczących cyberbezpieczeństwa. Może się on przyczynić do zmniejszenia liczby cyberincydentów, obniżenia kosztów postępowania w przypadku incydentu oraz uniknięcia nadszarpnięcia reputacji. W przypadku całej UE szacuje się, że inicjatywa może doprowadzić do obniżenia kosztów związanych z incydentami dotyczącymi przedsiębiorstw o około 180–290 mld EUR rocznie. Inicjatywa może spowodować wzrost obrotu ze względu na coraz większy popyt na produkty z elementami cyfrowymi. Może poprawić światową reputację przedsiębiorstw, co spowodowałoby wzrost popytu również spoza UE. Jeżeli chodzi o użytkowników, preferowany wariant może zwiększyć przejrzystość zabezpieczeń i ułatwić korzystanie z produktów z elementami cyfrowymi. Konsumenci i obywatele odniosą także korzyść polegającą na lepszej ochronie ich praw podstawowych, takich jak prywatność i ochrona danych.

Zapytani o ocenę skuteczności interwencji politycznych respondenci biorący udział w konsultacjach publicznych zgodzili się, że wariant 4 byłby najskuteczniejszym środkiem (4,08 w skali od 1 do 5). Do respondentów tych należą organizacje konsumenckie (5,00), respondenci określający się jako użytkownicy (4,22), jednostki notyfikowane (4,17), organy nadzoru rynku (5,00) oraz producenci produktów z elementami cyfrowymi (3,85), w tym mali i średni producenci (4,05).

- **Sprawność regulacyjna i uproszczenie**

W niniejszym wniosku ustanawia się wymogi, które będą miały zastosowanie do producentów sprzętu i oprogramowania. Istnieje potrzeba zapewnienia pewności prawa i uniknięcia dalszej fragmentacji wymogów cyberbezpieczeństwa dotyczących konkretnych produktów na rynku wewnętrznym, czego dowodem jest szerokie poparcie różnych zainteresowanych stron dla interwencji horyzontalnej. Wniosek doprowadzi do zminimalizowania obciążenia regulacyjnego nałożonego na producentów na mocy kilku aktów prawnych dotyczących bezpieczeństwa produktów. Dostosowanie do nowych ram prawnych oznacza lepsze funkcjonowanie interwencji i jej egzekwowanie. Niniejszy wniosek usprawnia proces dotyczący procedur zabezpieczających dzięki zaangażowaniu producentów i państw członkowskich przed powiadomieniem Komisji. Znaczna część producentów objętych zakresem wniosku jest już zaznajomiona z funkcjonowaniem nowych ram prawnych, co przyczyni się do ich zrozumienia i wdrożenia. Jeżeli chodzi o konsumentów

i przedsiębiorstwa, wniosek będzie zwiększał zaufanie do produktów z elementami cyfrowymi.

- **Prawa podstawowe**

Oczekuje się, że wszystkie warianty strategiczne w pewnym stopniu poprawią ochronę podstawowych praw i wolności, takich jak prywatność, ochrona danych osobowych, wolność prowadzenia działalności gospodarczej oraz ochrona własności lub godności i integralności osoby. W szczególności preferowany wariant strategiczny 4, obejmujący horyzontalną interwencję regulacyjną i szeroki zakres polityki, byłby najskuteczniejszy w tym względzie, ponieważ jest bardziej prawdopodobne, że przyczyni się do zmniejszenia liczby i dotkliwości incydentów, w tym naruszeń ochrony danych osobowych. Wariant ten może również zwiększyć pewność prawa i zapewnić równe warunki działania podmiotom gospodarczym, a także zwiększyć zaufanie użytkowników i poprawić atrakcyjność unijnych produktów z elementami cyfrowymi ogółem, zapewniając tym samym ochronę własności i poprawę warunków prowadzenia działalności gospodarczej przez podmioty gospodarcze.

Horyzontalne wymogi cyberbezpieczeństwa poprawią bezpieczeństwo danych osobowych przez ochronę poufności, integralności i dostępności informacji w produktach z elementami cyfrowymi. Zgodność z tymi wymogami ułatwi przestrzeganie wymogu w zakresie bezpieczeństwa przetwarzania danych osobowych wynikającego z rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych, RODO)[12]. Niniejszy wniosek zwiększy przejrzystość i poprawi informowanie użytkowników, w tym użytkowników o potencjalnie mniejszych umiejętnościach w dziedzinie cyberbezpieczeństwa. Użytkownicy będą również lepiej poinformowani o zagrożeniach, możliwościach i ograniczeniach związanych z produktami z elementami cyfrowymi, co sprawi, że będą lepiej przygotowani do wdrożenia niezbędnych środków zapobiegawczych i łagodzących w celu ograniczenia ryzyka szczątkowego.

4. WPŁYW NA BUDŻET

Aby zrealizować zadania przydzielone Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) na mocy niniejszego rozporządzenia, ENISA będzie musiała ponownie przydzielić zasoby ludzkie odpowiadające około 4,5 EPC. Komisja będzie musiała przydzielić zasoby odpowiadające 7 EPC, aby wywiązać się ze swoich obowiązków związanych z egzekwowaniem przepisów wynikających z niniejszego rozporządzenia.

Szczegółowy przegląd odnośnych kosztów znajduje się w ocenie skutków finansowych regulacji dołączonej do niniejszego wniosku.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Komisja będzie monitorować wdrażanie i stosowanie tych nowych przepisów oraz zgodność z nimi w celu oceny ich skuteczności. W rozporządzeniu Komisja zostanie wezwana do dokonania oceny i przeglądu oraz przedłożenia publicznego sprawozdania w tym zakresie

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

Parlamentowi Europejskiemu i Radzie przed upływem 36 miesięcy od daty rozpoczęcia stosowania, a następnie co cztery lata.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Przepisy ogólne (rozdział I)

Rozporządzeniem, którego dotyczy niniejszy wniosek, ustanawia się: a) przepisy dotyczące wprowadzania do obrotu produktów z elementami cyfrowymi w celu zapewnienia cyberbezpieczeństwa takich produktów; b) zasadnicze wymogi dotyczące projektowania, opracowywania i produkcji produktów z elementami cyfrowymi oraz obowiązki podmiotów gospodarczych w odniesieniu do tych produktów w zakresie cyberbezpieczeństwa; c) zasadnicze wymogi dotyczące procedur postępowania w przypadku wykrycia podatności wprowadzonych przez producentów w celu zapewnienia cyberbezpieczeństwa produktów z elementami cyfrowymi w całym cyklu życia oraz obowiązki podmiotów gospodarczych w odniesieniu do tych procedur; d) przepisy dotyczące nadzoru rynku i egzekwowania wyżej wymienionych przepisów i wymogów.

Proponowane rozporządzenie będzie miało zastosowanie do wszystkich produktów z elementami cyfrowymi, których przeznaczenie i racjonalnie przewidywalne wykorzystanie obejmuje bezpośrednie lub pośrednie logiczne lub fizyczne połączenie danych z urządzeniem lub siecią.

Proponowane rozporządzenie nie będzie miało zastosowania do produktów z elementami cyfrowymi objętych zakresem rozporządzenia (UE) 2017/745 [tj. do wyrobów medycznych stosowanych u ludzi oraz wyposażenia takich wyrobów] oraz rozporządzenia (UE) 2017/746 [tj. do wyrobów medycznych do diagnostyki *in vitro* stosowanych u ludzi oraz wyposażenia takich wyrobów], ponieważ oba te rozporządzenia zawierają wymogi dotyczące wyrobów, w tym dotyczące oprogramowania i ogólnych obowiązków producentów, obejmujące cały cykl życia produktów, a także procedury oceny zgodności. Niniejsze rozporządzenie nie będzie miało zastosowania do produktów z elementami cyfrowymi, które zostały certyfikowane zgodnie z rozporządzeniem (UE) 2018/1139 [w sprawie wysokiego jednolitego poziomu bezpieczeństwa lotnictwa cywilnego], ani do produktów, do których stosuje się rozporządzenie (UE) 2019/2144 [w sprawie wymogów dotyczących homologacji typu pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów].

Produkty krytyczne z elementami cyfrowymi podlegają szczególnym procedurom oceny zgodności i są podzielone na klasy I i II, jak określono w załączniku III, które odzwierciedlają ich poziom ryzyka w cyberprzestrzeni, przy czym klasa II oznacza większe ryzyko. Produkt z elementami cyfrowymi uznaje się za krytyczny i w związku z tym uwzględnia się go w załączniku III, biorąc pod uwagę wpływ potencjalnych podatności takiego produktu wpływających na cyberbezpieczeństwo. Przy określaniu ryzyka w cyberprzestrzeni uwzględnia się związane z cyberbezpieczeństwem funkcje produktu z elementami cyfrowymi oraz jego przeznaczenie we wrażliwych środowiskach, takich jak otoczenie przemysłowe.

Komisja jest również uprawniona do przyjmowania aktów delegowanych w celu uzupełnienia niniejszego rozporządzenia przez określenie kategorii produktów wysoce krytycznych z elementami cyfrowymi, w odniesieniu do których producenci mają obowiązek uzyskać europejski certyfikat cyberbezpieczeństwa w ramach europejskiego programu certyfikacji cyberbezpieczeństwa, aby wykazać zgodność z zasadniczymi wymogami określonymi w załączniku I lub jego częściach. Przy określaniu takich kategorii produktów wysoce krytycznych z elementami cyfrowymi Komisja uwzględnia poziom ryzyka w cyberprzestrzeni

związanego z kategorią produktów z elementami cyfrowymi w świetle co najmniej jednego kryterium branego pod uwagę przy sporządzaniu wykazu produktów krytycznych z elementami cyfrowymi zawartego w załączniku III, a także w kontekście oceny, czy ta kategoria produktów jest wykorzystywana przez podmioty niezbędne takie jak podmioty, o których mowa w załączniku [załączniku I] do dyrektywy [dyrektywy XXX/XXXX (NIS 2)], czy wspomniane podmioty polegają na tej kategorii produktów lub czy będzie ona miała potencjalne przyszłe znaczenie dla działalności tych podmiotów, bądź czy jest ona istotna dla odporności całego łańcucha dostaw produktów z elementami cyfrowymi na zdarzenia powodujące zakłócenia.

Obowiązki podmiotów gospodarczych (rozdział II)

Wniosek obejmuje obowiązki producentów, importerów i dystrybutorów na podstawie przepisów odniesienia przewidzianych w decyzji 768/2008/WE. Zgodnie z zasadniczymi wymogami cyberbezpieczeństwa i obowiązkami w tym zakresie wszystkie produkty z elementami cyfrowymi udostępnia się na rynku wyłącznie wówczas, gdy – jeżeli są należycie dostarczane, prawidłowo zainstalowane, utrzymywane i wykorzystywane zgodnie z ich przeznaczeniem lub w warunkach, które można racjonalnie przewidzieć – spełniają zasadnicze wymogi cyberbezpieczeństwa określone w niniejszym rozporządzeniu.

Zgodnie z zasadniczymi wymogami i obowiązkami producenci będą zobowiązani do uwzględnienia kwestii cyberbezpieczeństwa w projektowaniu, opracowywaniu i produkcji produktów z elementami cyfrowymi, do zachowania należytej staranności w odniesieniu do aspektów bezpieczeństwa przy projektowaniu i opracowywaniu swoich produktów, do zachowania przejrzystości w odniesieniu do aspektów cyberbezpieczeństwa, które należy podać do wiadomości klientów, do zapewnienia wsparcia w zakresie zabezpieczeń (aktualizacji) w sposób proporcjonalny oraz do spełnienia wymogów dotyczących postępowania w przypadku wykrycia podatności.

Zostaną ustanowione obowiązki dla podmiotów gospodarczych, począwszy od producentów, aż po dystrybutorów i importerów, w odniesieniu do wprowadzania do obrotu produktów z elementami cyfrowymi, stosownie do ich roli i zadań w łańcuchu dostaw.

Zgodność produktu z elementami cyfrowymi (rozdział III)

W przypadku produktów z elementami cyfrowymi spełniających normy zharmonizowane lub części norm zharmonizowanych, do których odniesienie opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, zakłada się, że spełniają one zasadnicze wymogi określone w rozporządzeniu, którego dotyczy niniejszy wniosek. W przypadku gdy normy zharmonizowane nie istnieją lub są niewystarczające lub jeżeli występują nieuzasadnione opóźnienia w procedurze normalizacji, lub jeżeli wniosek Komisji nie zostanie zaakceptowany przez europejskie organizacje normalizacyjne, Komisja może – w drodze aktów wykonawczych – przyjąć wspólne specyfikacje.

Ponadto produkty z elementami cyfrowymi, które uzyskały certyfikację lub w odniesieniu do których wydano unijną deklarację zgodności bądź certyfikat w ramach europejskiego programu certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 i w przypadku których Komisja określiła w akcie wykonawczym, że mogą zapewnić domniemanie zgodności z niniejszym rozporządzeniem, uznaje się za zgodne z zasadniczymi wymogami określonymi w niniejszym rozporządzeniu lub jego częściach w zakresie, w jakim unijna deklaracja zgodności bądź certyfikat cyberbezpieczeństwa lub ich części obejmują te wymogi.

Aby uniknąć nałożenia na producentów nadmiernego obciążenia administracyjnego, w stosownych przypadkach Komisja powinna określić, czy certyfikat cyberbezpieczeństwa

wydany w ramach takiego europejskiego programu certyfikacji cyberbezpieczeństwa zwalnia producentów z obowiązku przeprowadzenia oceny zgodności przez stronę trzecią, jak przewidziano w niniejszym rozporządzeniu w odniesieniu do odpowiednich wymogów.

Producent dokonuje oceny zgodności produktu z elementami cyfrowymi i swoimi własnymi procedurami postępowania w przypadku wykrycia podatności w celu wykazania zgodności z zasadniczymi wymogami określonymi w załączniku I, stosując jedną z procedur określonych w załączniku VI. Producenci produktów krytycznych klasy I i II stosują odpowiednie moduły niezbędne do osiągnięcia zgodności. Producenci produktów krytycznych klasy II muszą zaangażować stronę trzecią do oceny zgodności.

Notyfikacja jednostek oceniających zgodność (rozdział IV)

Prawidłowe funkcjonowanie jednostek notyfikowanych ma zasadnicze znaczenie dla zagwarantowania wysokiego cyberbezpieczeństwa oraz zaufania wszystkich zainteresowanych stron do systemu nowego podejścia. Dlatego też, zgodnie z decyzją 768/2008/WE, we wniosku określono wymogi dotyczące organów krajowych odpowiedzialnych za jednostki oceniające zgodność (jednostki notyfikowane). W związku z tym ostateczną odpowiedzialność za wyznaczanie i monitorowanie jednostek notyfikowanych ponoszą państwa członkowskie. Państwa członkowskie wyznaczają organ notyfikujący, który odpowiada za opracowanie i stosowanie procedur koniecznych do oceny i notyfikowania jednostek oceniających zgodność oraz do monitorowania jednostek notyfikowanych.

Nadzór rynku i egzekwowanie przepisów (rozdział V)

Zgodnie z rozporządzeniem (UE) 2019/1020 nadzór rynku na terytorium danego państwa członkowskiego sprawują krajowe organy nadzoru rynku. Państwa członkowskie mogą wyznaczyć do pełnienia funkcji organu nadzoru rynku dowolny istniejący lub nowy organ, w tym ustanowione właściwe organy krajowe, o których mowa w art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)], lub wyznaczone krajowe organy ds. certyfikacji cyberbezpieczeństwa, o których mowa w art. 58 rozporządzenia (UE) 2019/881. Podmioty gospodarcze powinny w pełni współpracować z organami nadzoru rynku i innymi właściwymi organami.

Przekazane uprawnienia i procedury komitetowe (rozdział VI)

Aby zapewnić możliwość dostosowania ram regulacyjnych w stosownych przypadkach, przekazuje się Komisji uprawnienia do przyjmowania na podstawie art. 290 TFUE aktów w celu aktualizacji wykazu produktów krytycznych klasy I i II oraz określenia definicji tych produktów; określenia, czy konieczne jest ograniczenie lub wyłączenie w odniesieniu do produktów z elementami cyfrowymi objętych innymi przepisami unijnymi określającymi wymogi zapewniające taki sam poziom ochrony jak niniejsze rozporządzenie; wprowadzenia obowiązku certyfikacji niektórych produktów wysoce krytycznych z elementami cyfrowymi w oparciu o kryteria określone w niniejszym rozporządzeniu; określenia minimalnego zakresu deklaracji zgodności UE oraz uzupełnienia elementów, które należy uwzględnić w dokumentacji technicznej.

Komisja jest również uprawniona do przyjmowania aktów wykonawczych w celu: określenia formatu lub elementów dotyczących obowiązków w zakresie zgłaszania incydentów oraz zestawienia podstawowych materiałów do produkcji oprogramowania; określania europejskich programów certyfikacji cyberbezpieczeństwa, które można stosować w celu wykazania zgodności z zasadniczymi wymogami lub ich częściami określonymi w niniejszym rozporządzeniu; przyjęcia wspólnych specyfikacji; ustanowienia specyfikacji technicznych dotyczących umieszczania oznakowania CE; przyjęcia na poziomie Unii środków

naprawczych lub ograniczających w wyjątkowych okolicznościach, które uzasadniają niezwłoczną interwencję w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego.

Poufność i kary (rozdział VII)

Wszystkie strony stosujące niniejsze rozporządzenie powinny przestrzegać zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań.

Aby zapewnić skuteczne egzekwowanie obowiązków przewidzianych w niniejszym rozporządzeniu, każdy organ nadzoru rynku powinien być uprawniony do nakładania lub żądania nałożenia administracyjnych kar pieniężnych. Podobnie w niniejszym rozporządzeniu określono maksymalne poziomy administracyjnych kar pieniężnych, które powinno się przewidzieć w przepisach krajowych za nieprzestrzeganie obowiązków określonych w niniejszym rozporządzeniu.

Przepisy przejściowe i końcowe (rozdział VIII)

Aby dać producentom, jednostkom notyfikowanym i państwom członkowskim czas na dostosowanie się do nowych wymogów, proponowane rozporządzenie zacznie być stosowane [24 miesięcy] po wejściu w życie, z wyjątkiem obowiązków w zakresie zgłaszania incydentów nałożonych na producentów, które zaczną mieć zastosowanie [12 miesięcy] po wejściu w życie.

2022/0272 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[1],

uwzględniając opinię Komitetu Regionów[2],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Należy koniecznie poprawić funkcjonowanie rynku wewnętrznego przez ustanowienie jednolitych ram prawnych w zakresie zasadniczych wymogów cyberbezpieczeństwa dotyczących wprowadzania produktów z elementami cyfrowymi na rynek unijny. Należy rozwiązać dwa główne problemy, które zwiększają koszty dla użytkowników i społeczeństwa: niski poziom cyberbezpieczeństwa produktów z elementami cyfrowymi, który przejawia się w powszechnych podatnościach oraz niewystarczającym i niespójnym dostarczaniu aktualizacji zabezpieczeń w celu wyeliminowania tych podatności, oraz niedostateczne zrozumienie i dostęp do informacji przez użytkowników, co uniemożliwia im wybór produktów o odpowiednich właściwościach w zakresie cyberbezpieczeństwa lub korzystanie z nich w sposób bezpieczny.

(2) Niniejsze rozporządzenie ma na celu stworzenie warunków brzegowych dla rozwoju bezpiecznych produktów z elementami cyfrowymi przez zapewnienie, aby sprzęt i oprogramowanie były wprowadzane do obrotu z mniejszą liczbą podatności, a także aby producenci poważnie traktowali bezpieczeństwo w całym cyklu życia produktu. Ma również na celu stworzenie warunków umożliwiających użytkownikom uwzględnianie cyberbezpieczeństwa przy wyborze produktów z elementami cyfrowymi i korzystaniu z nich.

(3) Odpowiednie obowiązujące obecnie przepisy Unii obejmują szereg grup przepisów horyzontalnych, które na różne sposoby odnoszą się do niektórych aspektów związanych z cyberbezpieczeństwem, w tym środków mających na celu poprawę

[1] Dz.U. C […] z […], s. […].
[2] Dz.U. C […] z […], s. […].

bezpieczeństwa cyfrowego łańcucha dostaw. Istniejące przepisy Unii związane z cyberbezpieczeństwem, w tym [dyrektywa XXX/XXXX (NIS 2)] i rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881[3], nie przewidują jednak bezpośrednio obowiązkowych wymogów dotyczących bezpieczeństwa produktów z elementami cyfrowymi.

(4) Chociaż obowiązujące przepisy Unii mają zastosowanie do niektórych produktów z elementami cyfrowymi, nie istnieją horyzontalne unijne ramy regulacyjne ustanawiające kompleksowe wymogi cyberbezpieczeństwa dotyczące wszystkich produktów z elementami cyfrowymi. Różne akty przyjęte dotychczas na szczeblu unijnym i krajowym oraz różne unijne i krajowe inicjatywy jedynie częściowo rozwiązują stwierdzone problemy związane z cyberbezpieczeństwem i stwarzają ryzyko niejednolitego rozwoju ustawodawstwa na rynku wewnętrznym, co pogłębia brak pewności prawa po stronie zarówno producentów, jak i użytkowników tych produktów, a także wiąże się z nakładaniem na przedsiębiorstwa niepotrzebnych obciążeń związanych z przestrzeganiem szeregu wymogów dotyczących podobnych rodzajów produktów. Cyberbezpieczeństwo tych produktów ma szczególnie wyraźny wymiar transgraniczny, ponieważ produkty wytwarzane w jednym państwie są często wykorzystywane przez organizacje i konsumentów na całym rynku wewnętrznym. W związku z tym konieczne jest uregulowanie tej dziedziny na poziomie Unii. Należy zharmonizować unijne otoczenie regulacyjne przez wprowadzenie wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi. Należy ponadto zagwarantować pewność podmiotom gospodarczym i użytkownikom w całej Unii, a także zapewnić lepszą harmonizację jednolitego rynku, co przełoży się na dogodniejsze warunki dla podmiotów chcących wejść na rynek Unii.

(5) Na poziomie Unii – w różnych dokumentach programowych i politycznych, takich jak Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[4], konkluzje Rady z dnia 2 grudnia 2020 r. i z dnia 23 maja 2022 r. lub rezolucja Parlamentu Europejskiego z dnia 10 czerwca 2021 r.[5] – wezwano do wprowadzenia konkretnych unijnych wymogów cyberbezpieczeństwa w odniesieniu do produktów cyfrowych lub podłączonych do internetu, przy czym szereg państw na świecie z własnej inicjatywy wprowadziło środki mające na celu rozwiązanie tej kwestii. W sprawozdaniu z wyników końcowych Konferencji w sprawie przyszłości Europy[6] obywatele wezwali do zwiększenia roli UE w przeciwdziałaniu zagrożeniom cyberbezpieczeństwa.

(6) Aby zwiększyć ogólny poziom cyberbezpieczeństwa wszystkich produktów z elementami cyfrowymi wprowadzanych na rynek wewnętrzny, należy ustanowić ukierunkowane na cel i neutralne technologicznie zasadnicze wymogi cyberbezpieczeństwa dotyczące tych produktów, które to wymogi byłyby stosowane horyzontalnie.

---

3 Rozporządzenie 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 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=JOIN:2020:18:FIN

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_PL.html

6 Konferencja w sprawie przyszłości Europy – sprawozdanie z wyników końcowych, maj 2022 r., propozycja nr 28 pkt 2. Konferencja odbyła się w okresie od kwietnia 2021 r. do maja 2022 r. Było to wyjątkowe, oddolne działanie z zakresu demokracji deliberatywnej na szczeblu paneuropejskim, w którym udział wzięły tysiące obywateli UE, a także podmioty polityczne, partnerzy społeczni, przedstawiciele społeczeństwa obywatelskiego i najważniejsze zainteresowane strony.

(7) W określonych warunkach wszystkie produkty z elementami cyfrowymi zintegrowane lub połączone z większym elektronicznym systemem informacyjnym mogą służyć jako wektor ataku dla podmiotów działających w złym zamiarze. W rezultacie nawet sprzęt i oprogramowanie uważane za mniej krytyczne mogą ułatwić rozpoczęcie ataku na urządzenie lub sieć, umożliwiając podmiotom działającym w złym zamiarze uzyskanie uprzywilejowanego dostępu do systemu lub przenikanie między różnymi systemami. Producenci powinni zatem zapewnić, aby wszystkie produkty z elementami cyfrowymi, które można podłączyć do internetu, były projektowane i opracowywane zgodnie z zasadniczymi wymogami określonymi w niniejszym rozporządzeniu. Dotyczy to zarówno produktów, które można podłączyć fizycznie za pomocą interfejsów sprzętowych, jak i produktów podłączanych na poziomie logicznym, np. za pomocą gniazd sieciowych, potoków, plików, interfejsów programowania aplikacji lub wszelkich innych rodzajów interfejsów oprogramowania. Ponieważ zagrożenia cyberbezpieczeństwa mogą rozprzestrzeniać się za pośrednictwem różnych produktów z elementami cyfrowymi, zanim dotrą do określonego celu, na przykład dzięki łącznemu wykorzystaniu wielu różnych exploitów, producenci powinni również zapewnić cyberbezpieczeństwo tych produktów, które są jedynie pośrednio połączone z innymi urządzeniami lub sieciami.

(8) Dzięki ustanowieniu wymogów cyberbezpieczeństwa dotyczących wprowadzania do obrotu produktów z elementami cyfrowymi produkty te będą bezpieczniejsze zarówno dla konsumentów, jak i dla przedsiębiorstw. Obejmuje to również wymogi dotyczące wprowadzania do obrotu produktów konsumenckich z elementami cyfrowymi przeznaczonych dla konsumentów podatnych na zagrożenia, takich jak zabawki i nianie elektroniczne.

(9) Niniejsze rozporządzenie zapewnia wysoki poziom cyberbezpieczeństwa produktów z elementami cyfrowymi. Nie reguluje się w nim usług, takich jak oprogramowanie jako usługa (SaaS), z wyjątkiem rozwiązań w zakresie zdalnego przetwarzania danych związanego z produktem z elementami cyfrowymi, rozumianego jako wszelkie przetwarzanie danych na odległość, na potrzeby którego oprogramowanie zostało zaprojektowane i opracowane przez producenta danego produktu lub na odpowiedzialność producenta danego produktu, a którego brak spowodowałby, że produkt z elementami cyfrowymi nie mógłby wykonywać jednej ze swoich funkcji. [Dyrektywa XXX/XXXX (NIS 2)] wprowadza wymogi cyberbezpieczeństwa i wymogi w zakresie zgłaszania incydentów w odniesieniu do podmiotów niezbędnych i istotnych takich jak infrastruktura krytyczna w celu zwiększenia odporności usług świadczonych przez te podmioty. [Dyrektywa XXX/XXXX (NIS 2)] ma zastosowanie do usług w chmurze oraz modeli świadczenia usług w chmurze takich jak oprogramowanie jako usługa. W zakres tej dyrektywy wchodzą wszystkie podmioty świadczące usługi w chmurze w Unii, które osiągają lub przekraczają próg dla średnich przedsiębiorstw.

(10) Aby nie utrudniać innowacji ani prowadzenia badań, niniejsze rozporządzenie nie powinno obejmować wolnego i otwartego oprogramowania, tworzonego lub dostarczanego poza działalnością handlową. Dotyczy to w szczególności oprogramowania, w tym jego kodu źródłowego i jego zmodyfikowanych wersji, które jest bezpłatnie dostępne dla każdego, z którego można korzystać oraz które można modyfikować i rozpowszechniać. Działalność handlowa związana z oprogramowaniem może obejmować nie tylko pobieranie zapłaty za produkt, ale również pobieranie opłat za usługi wsparcia technicznego, udostępnianie platformy oprogramowania, za pośrednictwem której producent zarabia na innych usługach, lub

wykorzystywanie danych osobowych z powodów innych niż tylko poprawa bezpieczeństwa, kompatybilności lub interoperacyjności oprogramowania.

(11) Bezpieczny internet jest niezbędny do funkcjonowania infrastruktury krytycznej i dla całego społeczeństwa. Celem [dyrektywy XXX/XXX (NIS 2)] jest zapewnienie wysokiego poziomu cyberbezpieczeństwa usług świadczonych przez podmioty niezbędne i istotne, w tym przez dostawców infrastruktury cyfrowej, którzy wspierają główne funkcje otwartego internetu, zapewniają dostęp do internetu oraz usługi internetowe. Ważne jest zatem, aby produkty z elementami cyfrowymi, które są niezbędne dostawcom infrastruktury cyfrowej do zapewnienia funkcjonowania internetu, były opracowywane w sposób bezpieczny oraz aby spełniały ugruntowane standardy bezpieczeństwa internetowego. Celem niniejszego rozporządzenia, które ma zastosowanie do wszelkiego sprzętu i oprogramowania, które można podłączyć do internetu, jest również ułatwienie dostawcom infrastruktury cyfrowej spełnienia wymogów dotyczących łańcucha dostaw określonych w [dyrektywie XXX/XXXX (NIS 2)] przez zapewnienie, aby produkty z elementami cyfrowymi wykorzystywane przez tych dostawców do świadczenia usług były opracowywane w sposób bezpieczny oraz aby dostawcy ci w odpowiednim czasie otrzymywali aktualizacje zabezpieczeń takich produktów.

(12) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745[7] ustanawia przepisy dotyczące wyrobów medycznych, a rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746[8] ustanawia przepisy dotyczące wyrobów medycznych do diagnostyki *in vitro*. Oba rozporządzenia dotyczą ryzyka w cyberprzestrzeni i zastosowano w nich szczególne podejścia, do których odniesiono się również w niniejszym rozporządzeniu. W szczególności w rozporządzeniach (UE) 2017/745 i (UE) 2017/746 określono zasadnicze wymogi dotyczące wyrobów medycznych, które funkcjonują za pośrednictwem systemu elektronicznego lub które same są oprogramowaniem. W zakres tych rozporządzeń wchodzą również niektóre rodzaje oprogramowania niewbudowanego, a przyjęto w nim także podejście oparte na całym cyklu życia. Wymogi te zobowiązują producentów do opracowywania i tworzenia produktów z zastosowaniem zasad zarządzania ryzykiem oraz podejścia obejmującego określenie wymogów dotyczących środków bezpieczeństwa IT, jak również odpowiednich procedur oceny zgodności. Ponadto od grudnia 2019 r. obowiązują szczegółowe wytyczne dotyczące cyberbezpieczeństwa wyrobów medycznych, w których przedstawiono wskazówki, jak producenci wyrobów medycznych, w tym wyrobów do diagnostyki *in vitro*, mogą spełnić wszystkie odpowiednie zasadnicze wymogi określone w załączniku I do każdego z tych rozporządzeń w odniesieniu do cyberbezpieczeństwa[9]. Produkty z elementami cyfrowymi, do których zastosowanie ma którekolwiek z tych rozporządzeń, nie powinny zatem podlegać niniejszemu rozporządzeniu.

---

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz.U. L 117 z 5.5.2017, s. 1).

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki *in vitro* oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz.U. L 117 z 5.5.2017, s. 176).

[9] Dokument MDCG 2019-16 zatwierdzony przez Grupę Koordynacyjną ds. Wyrobów Medycznych (MDCG) powołaną na mocy art. 103 rozporządzenia (UE) 2017/745.

(13) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/2144[10] ustanawia wymogi dotyczące homologacji typu pojazdów oraz ich układów i komponentów, wprowadza pewne wymogi cyberbezpieczeństwa, m.in. dotyczące funkcjonowania certyfikowanego systemu zarządzania cyberbezpieczeństwem, aktualizacji oprogramowania, obejmujące politykę i procesy organizacji dotyczące ryzyka w cyberprzestrzeni związanego z całym cyklem życia pojazdów, wyposażenia i usług zgodnie z mającymi zastosowanie regulaminami Organizacji Narodów Zjednoczonych dotyczącymi specyfikacji technicznych i cyberbezpieczeństwa[11], a także przewiduje określone procedury oceny zgodności. W obszarze lotnictwa głównym celem rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139[12] jest ustanowienie i utrzymanie wysokiego, jednolitego poziomu bezpieczeństwa lotnictwa cywilnego w Unii. Ustanowiono w nim ramy zasadniczych wymogów dotyczących zdatności do lotu lotniczych wyrobów, części i wyposażenia, w tym oprogramowania, w których uwzględniono obowiązki w zakresie ochrony przed zagrożeniami dla bezpieczeństwa informacji. Produkty z elementami cyfrowymi, do których zastosowanie ma rozporządzenie (UE) 2019/2144, oraz produkty certyfikowane zgodnie z rozporządzeniem (UE) 2018/1139 nie podlegają zatem zasadniczym wymogom i procedurom oceny zgodności określonym w niniejszym rozporządzeniu. Proces certyfikacji określony w rozporządzeniu (UE) 2018/1139 gwarantuje poziom pewności, który jest celem również niniejszego rozporządzenia.

(14) W niniejszym rozporządzeniu ustanawia się horyzontalne przepisy dotyczące cyberbezpieczeństwa, które nie ograniczają się do konkretnych sektorów ani niektórych produktów z elementami cyfrowymi. Można jednak wprowadzić unijne przepisy sektorowe lub dotyczące konkretnych produktów określające wymogi odnoszące się do wszystkich lub niektórych rodzajów ryzyka objętych zasadniczymi wymogami określonymi w niniejszym rozporządzeniu. W takich przypadkach stosowanie niniejszego rozporządzenia do produktów z elementami cyfrowymi objętych innymi przepisami unijnymi ustanawiającymi wymogi odnoszące się do wszystkich lub niektórych rodzajów ryzyka objętych zasadniczymi wymogami określonymi w załączniku I do niniejszego rozporządzenia może zostać ograniczone lub podlegać wyłączeniu, jeżeli takie ograniczenie lub wyłączenie jest spójne

---

10 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/2144 z dnia 27 listopada 2019 r. w sprawie wymogów dotyczących homologacji typu pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów, w odniesieniu do ich ogólnego bezpieczeństwa oraz ochrony osób znajdujących się w pojeździe i niechronionych uczestników ruchu drogowego, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/858 oraz uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 78/2009, (WE) nr 79/2009 i (WE) nr 661/2009 oraz rozporządzenia Komisji (WE) nr 631/2009, (UE) nr 406/2010, (UE) nr 672/2010, (UE) nr 1003/2010, (UE) nr 1005/2010, (UE) nr 1008/2010, (UE) nr 1009/2010, (UE) nr 19/2011, (UE) nr 109/2011, (UE) nr 458/2011, (UE) nr 65/2012, (UE) nr 130/2012, (UE) nr 347/2012, (UE) nr 351/2012, (UE) nr 1230/2012 i (UE) 2015/166 (Dz.U. L 325 z 16.12.2019, s. 1).

11 Regulamin ONZ nr 155 – Jednolite przepisy dotyczące homologacji pojazdów w zakresie cyberbezpieczeństwa i systemu zarządzania bezpieczeństwem [2021/387].

12 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 (Dz.U. L 212 z 22.8.2018, s. 1).

z ogólnymi ramami regulacyjnymi mającymi zastosowanie do tych produktów i jeżeli przepisy sektorowe zapewniają taki sam poziom ochrony jak ten przewidziany w niniejszym rozporządzeniu. Komisja jest uprawniona do przyjmowania aktów delegowanych w celu zmiany niniejszego rozporządzenia polegającej na wskazaniu takich produktów i przepisów. Niniejsze rozporządzenie zawiera przepisy szczegółowe precyzujące jego powiązania z obowiązującymi przepisami Unii, do których należy stosować takie ograniczenia lub wyłączenia.

(15) Rozporządzenie delegowane (UE) 2022/30 stanowi, że zasadnicze wymagania określone w art. 3 ust. 3 lit. d) (niepożądany wpływ na sieć i wykorzystanie zasobów sieciowych w nieodpowiedni sposób), lit. e) (dane osobowe i prywatność) oraz lit. f) (oszustwa) dyrektywy 2014/53/UE mają zastosowanie do określonych urządzeń radiowych. W [decyzji wykonawczej Komisji XXX/2022 w sprawie wniosku o normalizację do europejskich organizacji normalizacyjnych] ustanowiono wymogi dotyczące opracowania konkretnych norm doprecyzowujących sposób, w jaki należy zrealizować te trzy zestawy zasadniczych wymagań. Zasadnicze wymogi ustanowione w niniejszym rozporządzeniu obejmują wszystkie elementy zasadniczych wymagań, o których mowa w art. 3 ust. 3 lit. d), e) i f) dyrektywy 2014/53/UE. Co więcej, zasadnicze wymogi ustanowione w niniejszym rozporządzeniu są zgodne z celami wymogów dotyczących określonych norm zawartych w tym zleceniu normalizacji. Ponadto, jeżeli Komisja uchyli lub zmieni rozporządzenie delegowane (UE) 2022/30 z takim skutkiem, że przestanie ono mieć zastosowanie do określonych produktów objętych tym rozporządzeniem, Komisja i europejskie organizacje normalizacyjne powinny uwzględnić prace normalizacyjne przeprowadzone w kontekście decyzji wykonawczej Komisji C(2022) 5637 w sprawie wniosku o normalizację odnośnie do rozporządzenia delegowanego (UE) 2022/30 dotyczącego dyrektywy w sprawie urządzeń radiowych przy przygotowywaniu i opracowywaniu norm zharmonizowanych w celu ułatwienia wykonania niniejszego rozporządzenia.

(16) Dyrektywa 85/374/EWG[13] ma charakter uzupełniający w stosunku do niniejszego rozporządzenia. W dyrektywie tej określono przepisy dotyczące odpowiedzialności za produkty wadliwe, tak aby osoby poszkodowane mogły dochodzić kompensaty za szkodę wyrządzoną przez takie produkty. Ustanowiono w niej zasadę, że producent produktu jest odpowiedzialny za szkody spowodowane brakiem bezpieczeństwa produktu niezależnie od winy („odpowiedzialność na zasadzie ryzyka"). W przypadku gdy brak bezpieczeństwa polega na braku aktualizacji zabezpieczeń po wprowadzeniu produktu do obrotu, a produkt ten spowoduje szkodę, producenta można pociągnąć do odpowiedzialności. W niniejszym rozporządzeniu należy określić obowiązki producenta w zakresie zapewnienia takich aktualizacji zabezpieczeń.

(17) Niniejsze rozporządzenie nie powinno naruszać przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[14], w tym przepisów dotyczących ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych mających świadczyć o zgodności z tym

[13] Dyrektywa Rady 85/374/EWG z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz.U. L 210 z 7.8.85).

[14] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Takie operacje mogą być realizowane w produktach z elementami cyfrowymi. Najważniejszymi elementami rozporządzenia (UE) 2016/679 są uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych, jak również ogólnie pojęte cyberbezpieczeństwo. Dzięki zapewnieniu ochrony konsumentów i organizacji przed ryzykiem w cyberprzestrzeni ustanowione w niniejszym rozporządzeniu zasadnicze wymogi cyberbezpieczeństwa mają się też przyczynić do zwiększenia ochrony danych osobowych oraz prywatności osób fizycznych. Należy rozważyć możliwości synergii zarówno w obszarze normalizacji, jak i certyfikacji w zakresie aspektów cyberbezpieczeństwa w ramach współpracy między Komisją, europejskimi organizacjami normalizacyjnymi, Agencją Unii Europejskiej ds. Cyberbezpieczeństwa, Europejską Radą Ochrony Danych ustanowioną rozporządzeniem (UE) 2016/679 oraz krajowymi organami nadzorczymi odpowiedzialnymi za ochronę danych. Należy także zapewnić synergię między niniejszym rozporządzeniem a unijnymi przepisami o ochronie danych w dziedzinie nadzoru rynku i egzekwowania przepisów. W tym celu krajowe organy nadzoru rynku wyznaczone na podstawie niniejszego rozporządzenia powinny współpracować z organami nadzorującymi egzekwowanie unijnych przepisów o ochronie danych. Te ostatnie organy powinny także mieć dostęp do informacji istotnych dla realizacji ich zadań.

(18) W zakresie, w jakim ich produkty wchodzą w zakres niniejszego rozporządzenia, wydawcy europejskich portfeli tożsamości cyfrowej, o których mowa w art. [art. 6a ust. 2 rozporządzenia (UE) nr 910/2014 zmienionego przez wniosek dotyczący rozporządzenia zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej], powinni przestrzegać zarówno zasadniczych wymogów horyzontalnych ustanowionych w niniejszym rozporządzeniu, jak i szczególnych wymogów bezpieczeństwa ustanowionych w art. [art. 6a rozporządzenia (UE) nr 910/2014 zmienionego przez wniosek dotyczący rozporządzenia zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej]. W celu ułatwienia zapewnienia zgodności wydawcy portfeli powinni mieć możliwość wykazania zgodności europejskich portfeli tożsamości cyfrowej z wymogami określonymi odpowiednio w obu aktach przez certyfikowanie swoich produktów w ramach europejskiego programu certyfikacji cyberbezpieczeństwa ustanowionego na podstawie rozporządzenia (UE) 2019/881, w odniesieniu do którego Komisja określiła, w drodze aktu wykonawczego, domniemanie zgodności z niniejszym rozporządzeniem w zakresie, w jakim certyfikat lub jego części obejmują te wymogi.

(19) Niektóre zadania przewidziane w niniejszym rozporządzeniu powinny być wykonywane przez ENISA zgodnie z art. 3 ust. 2 rozporządzenia (UE) 2019/881. W szczególności ENISA powinna otrzymywać od producentów zgłoszenia aktywnie wykorzystywanych podatności zawartych w produktach z elementami cyfrowymi, jak również zgłoszenia incydentów wpływających na bezpieczeństwo tych produktów. ENISA powinna także przekazywać te zgłoszenia właściwym zespołom reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) lub odpowiednio właściwym pojedynczym punktom kontaktowym państw członkowskich wyznaczonych zgodnie z art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)] oraz informować właściwe organy nadzoru rynku o zgłoszonej podatności. Na podstawie gromadzonych przez siebie informacji ENISA powinna co dwa lata przygotowywać sprawozdanie techniczne na temat pojawiających się tendencji w zakresie ryzyka w cyberprzestrzeni dotyczącego produktów z elementami cyfrowymi oraz przedkładać je grupie

współpracy, o której mowa w dyrektywie [dyrektywie XXX/XXXX (NIS 2)]. Co więcej, zważywszy na jej wiedzę specjalistyczną i mandat, ENISA powinna mieć możliwość wspierania procesu wdrażania niniejszego rozporządzenia. W szczególności powinna mieć możliwość proponowania wspólnych działań, które miałyby być prowadzone przez organy nadzoru rynku, w oparciu o wskazania lub informacje dotyczące potencjalnej niezgodności z niniejszym rozporządzeniem produktów z elementami cyfrowymi w kilku państwach członkowskich lub wskazywania kategorii produktów, w odniesieniu do których należy zorganizować równoczesne skoordynowane działania kontrolne. W wyjątkowych okolicznościach, na wniosek Komisji, ENISA powinna mieć możliwość przeprowadzania ocen w odniesieniu do określonych produktów z elementami cyfrowymi, które stwarzają istotne ryzyko w cyberprzestrzeni, w przypadku gdy natychmiastowa interwencja jest niezbędna do utrzymania prawidłowego funkcjonowania rynku wewnętrznego.

(20) Produkty z elementami cyfrowymi powinny posiadać oznakowanie CE świadczące o ich zgodności z niniejszym rozporządzeniem, aby umożliwić ich swobodny przepływ na rynku wewnętrznym. Państwa członkowskie nie powinny stwarzać nieuzasadnionych przeszkód dla wprowadzania do obrotu produktów z elementami cyfrowymi zgodnych z wymogami określonymi w niniejszym rozporządzeniu i posiadających oznakowanie CE.

(21) Aby zapewnić producentom możliwość wydawania oprogramowania do celów testowania przed poddaniem produktów ocenie zgodności, państwa członkowskie nie powinny uniemożliwiać udostępniania nieukończonego oprogramowania, takiego jak wersje alfa, wersje beta lub kandydaci do wydania (ang. *release candidate*), o ile dana wersja jest udostępniana wyłącznie na okres niezbędny do jej przetestowania i uzyskania informacji zwrotnych. Producenci powinni zagwarantować, że oprogramowanie udostępniane na tych warunkach będzie wydawane dopiero po przeprowadzeniu oceny ryzyka oraz że będzie ono zgodne, w możliwie jak najszerszym zakresie, z wymogami bezpieczeństwa dotyczącymi właściwości produktów z elementami cyfrowymi nałożonymi w niniejszym rozporządzeniu. Producenci powinni także w możliwie jak najszerszym zakresie wdrożyć wymogi dotyczące postępowania w przypadku wykrycia podatności. Producenci nie powinni zmuszać użytkowników do aktualizacji do wersji, które wydano wyłącznie do celów testowania.

(22) W celu zapewnienia, aby produkty z elementami cyfrowymi po wprowadzeniu ich do obrotu nie stwarzały ryzyka w cyberprzestrzeni dla osób i organizacji, należy określić zasadnicze wymogi dotyczące takich produktów. Jeżeli takie produkty są następnie modyfikowane za pomocą środków fizycznych lub cyfrowych w sposób nieprzewidziany przez producenta i mogący oznaczać, że nie spełniają one już odpowiednich zasadniczych wymogów, taką modyfikację należy uznać za istotną. Na przykład aktualizacje lub naprawy oprogramowania można uznać za operacje w zakresie utrzymania pod warunkiem, że nie modyfikują one produktu już wprowadzonego do obrotu w sposób, który może wpływać na jego zgodność z obowiązującymi wymogami lub zmienić przeznaczenie, pod kątem którego dokonano oceny produktu. Podobnie jak w przypadku fizycznych napraw lub modyfikacji produkt z elementami cyfrowymi należy uznać za istotnie zmodyfikowany przez zmianę oprogramowania, jeżeli aktualizacja oprogramowania zmienia pierwotnie zamierzone funkcje, rodzaj lub działanie produktu, a zmian tych nie przewidziano we wstępnej ocenie ryzyka, lub gdy z powodu aktualizacji oprogramowania zmienił się charakter zagrożenia lub zwiększył się poziom ryzyka.

(23) Zgodnie z powszechnie przyjętym pojęciem istotnej zmiany w odniesieniu do produktów objętych unijnym prawodawstwem harmonizacyjnym za każdym razem, gdy następuje istotna modyfikacja, która może wpłynąć na zgodność produktu z niniejszym rozporządzeniem, lub gdy zmienia się przeznaczenie produktu, należy zweryfikować zgodność produktu z elementami cyfrowymi oraz, w stosownych przypadkach, poddać go nowej ocenie zgodności. W stosownych przypadkach, jeśli producent przeprowadza ocenę zgodności z udziałem strony trzeciej, należy powiadomić stronę trzecią o zmianach, które mogą prowadzić do istotnych modyfikacji.

(24) Odnawianie, utrzymanie i naprawa produktu z elementami cyfrowymi, zgodnie z definicją zawartą w rozporządzeniu [rozporządzeniu w sprawie ekoprojektu], niekoniecznie prowadzą do istotnej modyfikacji produktu, na przykład jeśli nie zmienią się przeznaczenie oraz funkcje oraz jeśli nie wpłynie to na poziom ryzyka. Unowocześnienie produktu przez producenta może jednak prowadzić do zmian w projektowaniu i opracowywaniu produktu i z tego względu może wpływać na przeznaczenie produktu oraz jego zgodność z wymogami określonymi w niniejszym rozporządzeniu.

(25) Produkt z elementami cyfrowymi należy uznać za krytyczny, jeśli negatywny wpływ wykorzystywania potencjalnych podatności wpływających na cyberbezpieczeństwo w produkcie może być dotkliwy, między innymi z uwagi na funkcje związane z cyberbezpieczeństwem lub przeznaczenie. W szczególności podatności w produktach z elementami cyfrowymi posiadających funkcje związane z cyberbezpieczeństwem, takie jak zabezpieczenia, mogą prowadzić do rozprzestrzeniania się problemów z bezpieczeństwem w całym łańcuchu dostaw. Dotkliwość wpływu cyberincydentu może zwiększyć się także wówczas, gdy uwzględnia się przeznaczenie produktu, np. wykorzystanie go w środowisku przemysłowym lub w kontekście podmiotu niezbędnego takiego jak podmioty, o których mowa w załączniku [załączniku I] do dyrektywy [dyrektywy XXX/ XXXX (NIS 2)], lub w odniesieniu do działania funkcji krytycznych lub wrażliwych, takich jak przetwarzanie danych osobowych.

(26) Produkty krytyczne z elementami cyfrowymi należy poddać bardziej rygorystycznym procedurom oceny zgodności przy jednoczesnym zachowaniu proporcjonalnego podejścia. W tym celu produkty krytyczne z elementami cyfrowymi należy podzielić na dwie klasy, odzwierciedlające poziom ryzyka w cyberprzestrzeni powiązanego z tymi kategoriami produktów. Potencjalny cyberincydent z udziałem produktów klasy II może prowadzić do poważniejszych negatywnych skutków niż incydent z udziałem produktów klasy I, na przykład z uwagi na charakter funkcji tych produktów związanej z cyberbezpieczeństwem lub ich przeznaczenie do wykorzystania w środowiskach wrażliwych, i z tego względu powinien on podlegać bardziej rygorystycznej procedurze oceny zgodności.

(27) Kategorie produktów krytycznych z elementami cyfrowymi, o których mowa w załączniku III do niniejszego rozporządzenia, należy rozumieć jako produkty, których podstawowa funkcjonalność jest jedną z funkcjonalności wymienionych w załączniku III do niniejszego rozporządzenia. Na przykład w załączniku III do niniejszego rozporządzenia wymieniono produkty, które na podstawie ich podstawowej funkcjonalności zdefiniowano jako mikroprocesory do zastosowań ogólnych w klasie II. W związku z tym mikroprocesory do zastosowań ogólnych podlegają obowiązkowej ocenie zgodności przez stronę trzecią. Taka sytuacja nie ma miejsca w przypadku innych produktów niewymienionych wprost w załączniku III do

niniejszego rozporządzenia, które mogą zawierać mikroprocesor do zastosowań ogólnych. Komisja powinna przyjąć akty delegowane [przed upływem 12 miesięcy od wejścia w życie niniejszego rozporządzenia] w celu określenia definicji kategorii produktów objętych klasą I i klasą II wymienionych w załączniku III.

(28) W niniejszym rozporządzeniu odniesiono się w sposób ukierunkowany do ryzyka w cyberprzestrzeni. Produkty z elementami cyfrowymi mogą jednak stwarzać inne ryzyko w zakresie bezpieczeństwa, które nie jest związane z cyberbezpieczeństwem. Takie rodzaje ryzyka powinny nadal być uregulowane przez inne właściwe przepisy unijne dotyczące produktów. W przypadku braku innego mającego zastosowanie unijnego prawodawstwa harmonizacyjnego te rodzaje ryzyka powinny podlegać rozporządzeniu [rozporządzeniu w sprawie ogólnego bezpieczeństwa produktów]. Z tego względu, w świetle ukierunkowanego charakteru niniejszego rozporządzenia, jako odstępstwo od art. 2 ust. 1 akapit trzeci lit. b) rozporządzenia [rozporządzenia w sprawie ogólnego bezpieczeństwa produktów] zastosowanie do produktów z elementami cyfrowymi, jeżeli nie podlegają one szczegółowym wymogom nałożonym przez inne unijne prawodawstwo harmonizacyjne w rozumieniu [art. 3 pkt 25 rozporządzenia w sprawie ogólnego bezpieczeństwa produktów], w odniesieniu do ryzyka w zakresie bezpieczeństwa nieobjętego niniejszym rozporządzeniem powinny mieć rozdział III sekcja 1, rozdziały V i VII oraz rozdziały IX–XI rozporządzenia [rozporządzenia w sprawie ogólnego bezpieczeństwa produktów].

(29) Produkty z elementami cyfrowymi sklasyfikowane jako systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. 6 rozporządzenia[15] [rozporządzenia w sprawie sztucznej inteligencji], wchodzące w zakres niniejszego rozporządzenia, powinny spełniać zasadnicze wymogi określone w niniejszym rozporządzeniu. Jeżeli systemy sztucznej inteligencji wysokiego ryzyka spełniają zasadnicze wymogi niniejszego rozporządzenia, należy je uznać za zgodne z wymogami w zakresie cyberbezpieczeństwa określonymi w art. [art. 15] rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji] w takim zakresie, w jakim wymogi te są objęte deklaracją zgodności UE lub jej częściami wydanymi na podstawie niniejszego rozporządzenia. Jeśli chodzi o procedury oceny zgodności dotyczące zasadniczych wymogów cyberbezpieczeństwa w odniesieniu do produktu z elementami cyfrowymi objętego niniejszym rozporządzeniem i sklasyfikowanego jako system sztucznej inteligencji wysokiego ryzyka, co do zasady zastosowanie powinny mieć nie przepisy niniejszego rozporządzenia, ale odpowiednie przepisy art. 43 rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji]. Zasada ta nie powinna jednak powodować zmniejszenia niezbędnego poziomu bezpieczeństwa w odniesieniu do produktów krytycznych z elementami cyfrowymi objętych niniejszym rozporządzeniem. Z tego względu, na zasadzie odstępstwa od tej zasady, systemy sztucznej inteligencji wysokiego ryzyka, które wchodzą w zakres rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji] i są również kwalifikowane jako produkty krytyczne z elementami cyfrowymi na podstawie niniejszego rozporządzenia oraz do których zastosowanie ma procedura oceny zgodności opierająca się na kontroli wewnętrznej, o której mowa w załączniku VI do rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji], powinny podlegać przepisom niniejszego rozporządzenia dotyczącym oceny zgodności w zakresie zasadniczych wymogów niniejszego rozporządzenia. W tym przypadku do wszystkich pozostałych aspektów objętych rozporządzeniem [rozporządzeniem w sprawie sztucznej inteligencji] należy

[15] Rozporządzenie [rozporządzenie w sprawie sztucznej inteligencji].

stosować odpowiednie przepisy dotyczące oceny zgodności opierającej się na kontroli wewnętrznej określone w załączniku VI do rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji].

(30) Produkty maszynowe wchodzące w zakres rozporządzenia [wniosku dotyczącego rozporządzenia w sprawie maszyn], które są produktami z elementami cyfrowymi w rozumieniu niniejszego rozporządzenia i w odniesieniu do których wydano deklarację zgodności na podstawie niniejszego rozporządzenia, należy uznać za zgodne z zasadniczymi wymaganiami w zakresie ochrony zdrowia i bezpieczeństwa określonymi w [sekcjach 1.1.9 i 1.2.1 załącznika III] do rozporządzenia [wniosku dotyczącego rozporządzenia w sprawie maszyn] w odniesieniu do zabezpieczenia przed uszkodzeniem oraz bezpieczeństwa i niezawodności układów sterowania w zakresie, w jakim zgodność z tymi wymaganiami wykazano w deklaracji zgodności UE wydanej na podstawie niniejszego rozporządzenia.

(31) Rozporządzenie [wniosek dotyczący rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia] uzupełnia zasadnicze wymogi określone w niniejszym rozporządzeniu. Systemy elektronicznej dokumentacji medycznej wchodzące w zakres rozporządzenia [wniosku dotyczącego rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia], które stanowią produkty z elementami cyfrowymi w rozumieniu niniejszego rozporządzenia, powinny zatem także być zgodne z zasadniczymi wymogami określonymi w niniejszym rozporządzeniu. Ich producenci powinni wykazać zgodność produktów zgodnie z przepisami rozporządzenia [wniosku dotyczącego rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia]. W celu ułatwienia zapewnienia zgodności producentom umożliwia się sporządzanie jednej dokumentacji technicznej zawierającej elementy wymagane przez oba akty prawne. Ponieważ niniejsze rozporządzenie nie obejmuje oprogramowania jako usługi, systemy elektronicznej dokumentacji medycznej oferowane w ramach modelu udzielania licencji na oprogramowanie jako usługę oraz jego dostawy nie wchodzą w zakres niniejszego rozporządzenia. Podobnie systemy elektronicznej dokumentacji medycznej, które są opracowywane i wykorzystywane wewnętrznie, nie wchodzą w zakres niniejszego rozporządzenia, ponieważ nie są one wprowadzane do obrotu.

(32) W celu zapewnienia, aby produkty z elementami cyfrowymi były bezpieczne zarówno w momencie wprowadzenia ich do obrotu, jak i przez cały cykl ich życia, konieczne jest określenie zasadniczych wymogów w zakresie postępowania w przypadku wykrycia podatności oraz zasadniczych wymogów cyberbezpieczeństwa w odniesieniu do właściwości produktów z elementami cyfrowymi. Chociaż producenci powinni przestrzegać wszystkich zasadniczych wymogów w zakresie postępowania w przypadku wykrycia podatności oraz zapewnić, aby wszystkie ich produkty dostarczano bez żadnych znanych i możliwych do wykorzystania podatności, powinni oni określić, jakie inne zasadnicze wymogi dotyczące właściwości produktu są istotne dla danego rodzaju produktu. W tym celu producenci powinni przeprowadzić ocenę ryzyka w cyberprzestrzeni związanego z produktem z elementami cyfrowymi, aby zidentyfikować istotne ryzyko oraz wskazać istotne zasadnicze wymogi, jak również aby właściwie zastosować odpowiednie normy zharmonizowane lub wspólne specyfikacje.

(33) W celu poprawy bezpieczeństwa produktów z elementami cyfrowymi wprowadzanych na rynek wewnętrzny niezbędne jest określenie zasadniczych wymogów. Zasadnicze wymogi powinny pozostawać bez uszczerbku dla unijnych skoordynowanych ocen ryzyka krytycznych łańcuchów dostaw ustanowionych na mocy [art. X] dyrektywy

[dyrektywy XXX/XXXX (NIS 2)][16], które uwzględniają zarówno techniczne, jak i – w stosownych przypadkach – pozatechniczne czynniki ryzyka, takie jak nadmierny wpływ państw trzecich na dostawców. Co więcej, powinny one pozostawać bez uszczerbku dla prerogatyw państw członkowskich w odniesieniu do określania dodatkowych wymogów, które uwzględniają czynniki pozatechniczne w celu zapewnienia wysokiego poziomu odporności, w tym te określone w zaleceniu (UE) 2019/534, w unijnej skoordynowanej ocenie ryzyka w zakresie bezpieczeństwa sieci 5G oraz w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G uzgodnionym przez grupę współpracy NIS, o której mowa w [dyrektywie XXX/XXXX (NIS 2)].

(34) W celu zapewnienia, aby krajowe zespoły CSIRT oraz pojedyncze punkty kontaktowe wyznaczone zgodnie z art. [art. X] dyrektywy [dyrektywy XX/XXXX (NIS 2)] otrzymywały informacje niezbędne do realizacji swoich zadań oraz podniesienia ogólnego poziomu cyberbezpieczeństwa podmiotów niezbędnych i istotnych, a także w celu zapewnienia skutecznego funkcjonowania organów nadzoru rynku producenci produktów z elementami cyfrowymi powinni zgłaszać ENISA podatności, które są aktywnie wykorzystywane. Ponieważ większość produktów z elementami cyfrowymi jest wprowadzana na obrotu na całym rynku wewnętrznym, każdą podatność wykorzystywaną w produkcie z elementami cyfrowymi należy uznać za zagrożenie dla funkcjonowania rynku wewnętrznego. Producenci powinni także rozważyć ujawnianie naprawionych podatności w europejskiej bazie danych dotyczących podatności utworzonej na podstawie dyrektywy [dyrektywy XX/XXXX (NIS 2)] i zarządzanej przez ENISA lub w jakiejkolwiek innej publicznie dostępnej bazie danych dotyczących podatności.

(35) Producenci powinni także zgłaszać do ENISA wszelkie incydenty wpływające na bezpieczeństwo produktu z elementami cyfrowymi. Niezależnie od obowiązków w zakresie zgłaszania incydentów nałożonych w dyrektywie [dyrektywie XXX/XXXX (NIS 2)] na podmioty niezbędne i istotne, konieczne jest, aby ENISA, pojedyncze punkty kontaktowe wyznaczone przez państwa członkowskie zgodnie z art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)] oraz organy nadzoru rynku otrzymywały od producentów produktów z elementami cyfrowymi informacje umożliwiające im ocenę bezpieczeństwa tych produktów. Aby zapewnić użytkownikom możliwość szybkiego reagowania na incydenty wpływające na bezpieczeństwo należących do nich produktów z elementami cyfrowymi, producenci powinni informować także użytkowników o wszelkich takich incydentach, a w stosownych przypadkach o wszelkich środkach naprawczych, które użytkownicy mogą zastosować w celu złagodzenia skutków incydentu, na przykład publikując odpowiednie informacje na swoich stronach internetowych lub, jeżeli producent jest w stanie skontaktować się z użytkownikami i jeżeli jest to uzasadnione przez ryzyko, docierając bezpośrednio do użytkowników.

(36) Producenci produktów z elementami cyfrowymi powinni wdrożyć politykę skoordynowanego ujawniania podatności, aby ułatwić zgłaszanie podatności przez osoby lub podmioty. W polityce skoordynowanego ujawniania podatności należy określić ustrukturyzowany proces, w ramach którego podatności zgłaszane są producentowi w sposób umożliwiający mu zdiagnozowanie i wyeliminowanie takich

[16] Dyrektywa Parlamentu Europejskiego i Rady XXX z dnia [data] [w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii, uchylająca dyrektywę (UE) 2016/1148 (Dz.U. L xx z [data], s. x)].

podatności, zanim szczegółowe informacje dotyczące podatności zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej. Biorąc pod uwagę fakt, że informacje na temat możliwych do wykorzystania podatności w powszechnie używanych produktach z elementami cyfrowymi mogą być sprzedawane po wysokich cenach na czarnym rynku, producenci takich produktów powinni mieć możliwość korzystania z programów, będących częścią ich polityki skoordynowanego ujawniania podatności, których celem jest zachęcanie do zgłaszania podatności przez zagwarantowanie osobom lub podmiotom uznania oraz wynagrodzenia za ich starania (tak zwane programy wynagrodzeń za wykryte błędy, ang. *bug bounty*).

(37) Aby ułatwić analizę podatności, producenci powinni identyfikować i dokumentować komponenty zawarte w produkcie z elementami cyfrowymi, w tym przez sporządzenie zestawienia podstawowych materiałów do produkcji oprogramowania. Dzięki zestawieniu podstawowych materiałów do produkcji oprogramowania osoby lub podmioty, które produkują, nabywają lub obsługują oprogramowanie, mogą uzyskać informacje podnoszące ich poziom zrozumienia łańcucha dostaw, co przynosi liczne korzyści, w szczególności pomaga producentom i użytkownikom w śledzeniu znanych i nowo pojawiających się podatności oraz ryzyka. Szczególnie istotne jest zapewnienie przez producentów, aby ich produkty nie zawierały opracowanych przez strony trzecie komponentów, w których mogą występować podatności.

(38) W celu ułatwienia oceny zgodności z wymogami określonymi w niniejszym rozporządzeniu należy przyjąć domniemanie zgodności produktów z elementami cyfrowymi, które są zgodne z normami zharmonizowanymi, w których zasadnicze wymogi niniejszego rozporządzenia przełożono na szczegółowe specyfikacje techniczne oraz które przyjęto zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012[17]. W rozporządzeniu (UE) nr 1025/2012 przewidziano procedurę sprzeciwu wobec norm zharmonizowanych, w przypadku gdy normy takie nie spełniają w pełni wymogów niniejszego rozporządzenia.

(39) W rozporządzeniu (UE) 2019/881 ustanowiono europejskie ramy dobrowolnej certyfikacji cyberbezpieczeństwa dotyczącej produktów, procesów i usług ICT. Europejskie programy certyfikacji cyberbezpieczeństwa mogą obejmować produkty z elementami cyfrowymi objęte niniejszym rozporządzeniem. Niniejsze rozporządzenie powinno stworzyć synergię z rozporządzeniem (UE) 2019/881. W celu ułatwienia oceny zgodności z wymogami określonymi w niniejszym rozporządzeniu produkty z elementami cyfrowymi, które uzyskały certyfikację lub w odniesieniu do których wydano deklarację zgodności w ramach programu certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881, co zostało określone przez Komisję w akcie wykonawczym, uznaje się za zgodne z zasadniczymi wymogami określonymi w niniejszym rozporządzeniu w zakresie, w jakim certyfikat cyberbezpieczeństwa bądź deklaracja zgodności lub ich części obejmują te wymogi. W świetle niniejszego rozporządzenia należy ocenić potrzebę nowych europejskich programów certyfikacji cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi. W takich przyszłych europejskich programach certyfikacji cyberbezpieczeństwa obejmujących produkty z elementami cyfrowymi należy

[17] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12).

uwzględnić zasadnicze wymogi określone w niniejszym rozporządzeniu oraz ułatwiać zapewnienie zgodności z niniejszym rozporządzeniem. Komisja powinna być uprawniona do określania, w drodze aktów wykonawczych, europejskich programów certyfikacji cyberbezpieczeństwa, które można stosować w celu wykazania zgodności z zasadniczymi wymogami określonymi w niniejszym rozporządzeniu. Co więcej, aby uniknąć nałożenia na producentów nadmiernego obciążenia administracyjnego, w stosownych przypadkach Komisja powinna określić, czy certyfikat cyberbezpieczeństwa wydany w ramach takich europejskich programów certyfikacji cyberbezpieczeństwa zwalnia producentów z obowiązku przeprowadzenia oceny zgodności przez stronę trzecią, jak przewidziano w niniejszym rozporządzeniu w odniesieniu do odpowiednich wymogów.

(40) Po wejściu w życie aktu wykonawczego określającego [rozporządzenia wykonawczego Komisji (UE) nr …/... z dnia XXX w sprawie europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach] (EUCC), który dotyczy sprzętu komputerowego objętego niniejszym rozporządzeniem, takiego jak sprzętowe moduły bezpieczeństwa i mikroprocesory, Komisja może określić, w drodze aktu wykonawczego, w jaki sposób EUCC zapewnia domniemanie zgodności z zasadniczymi wymogami, o których mowa w załączniku I do niniejszego rozporządzenia lub jego części. Co więcej, w takim akcie wykonawczym można określić, w jaki sposób certyfikat wydany w ramach EUCC zwalnia producentów z obowiązku przeprowadzenia oceny przez stronę trzecią, wymaganej w niniejszym rozporządzeniu w odniesieniu do odpowiednich wymogów.

(41) W przypadkach, w których nie przyjęto żadnych norm zharmonizowanych lub w których normy zharmonizowane nie realizują zasadniczych wymogów niniejszego rozporządzenia w wystarczającym stopniu, Komisja powinna mieć możliwość przyjęcia wspólnych specyfikacji w drodze aktów wykonawczych. Powodem opracowania takich wspólnych specyfikacji zamiast opierania się na normach zharmonizowanych może być odmowa realizacji zlecenia normalizacji przez którąkolwiek z europejskich organizacji normalizacyjnych, nieuzasadniona zwłoka w ustanowieniu właściwych norm zharmonizowanych lub brak zgodności opracowanych norm z wymogami niniejszego rozporządzenia lub z wnioskiem Komisji. W celu ułatwienia oceny zgodności z zasadniczymi wymogami określonymi w niniejszym rozporządzeniu należy przyjąć domniemanie zgodności w odniesieniu do produktów z elementami cyfrowymi, które są zgodne ze wspólnymi specyfikacjami przyjętymi przez Komisję zgodnie z niniejszym rozporządzeniem w celu wyrażenia szczegółowych specyfikacji technicznych dotyczących tych wymogów.

(42) Producenci powinni sporządzić deklarację zgodności UE zawierającą wymagane na podstawie niniejszego rozporządzenia informacje na temat zgodności produktów z elementami cyfrowymi z zasadniczymi wymogami zawartymi w niniejszym rozporządzeniu oraz, w stosownych przypadkach, w innym właściwym unijnym prawodawstwie harmonizacyjnym, którym objęty jest produkt. Inne przepisy Unii również mogą nakładać na producentów obowiązek sporządzenia deklaracji zgodności UE. Aby zagwarantować skuteczny dostęp do informacji do celów nadzoru rynku, należy sporządzić jedną deklarację zgodności UE dotyczącą zgodności ze wszystkimi właściwymi aktami Unii. Aby zmniejszyć obciążenie administracyjne podmiotów gospodarczych, należy umożliwić, aby ta jedna deklaracja zgodności UE mogła mieć formę folderu złożonego z odpowiednich poszczególnych deklaracji zgodności.

(43) Oznakowanie CE, symbolizujące zgodność produktu, jest widoczną konsekwencją całego procesu obejmującego ocenę zgodności w szerokim znaczeniu. Ogólne zasady

regulujące oznakowanie CE ustanowiono w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 765/2008[18]. W niniejszym rozporządzeniu należy ustanowić zasady regulujące umieszczanie oznakowania CE na produktach z elementami cyfrowymi. Oznakowanie CE powinno być jedynym oznakowaniem gwarantującym, że produkty z elementami cyfrowymi spełniają wymogi niniejszego rozporządzenia.

(44) Aby podmioty gospodarcze mogły wykazać zgodność z zasadniczymi wymogami określonymi w niniejszym rozporządzeniu, a organy nadzoru rynku mogły zapewnić zgodność produktów z elementami cyfrowymi udostępnianych na rynku z tymi wymogami, należy ustanowić procedury oceny zgodności. Decyzją Parlamentu Europejskiego i Rady nr 768/2008/WE[19] ustanowiono moduły procedur oceny zgodności proporcjonalnie do poziomu występującego ryzyka oraz wymaganego poziomu bezpieczeństwa. Aby zapewnić spójność między sektorami oraz uniknąć wariantów *ad hoc*, na tych modułach oparto procedury oceny zgodności odpowiednie do celów weryfikacji zgodności produktów z elementami cyfrowymi z zasadniczymi wymogami określonymi w niniejszym rozporządzeniu. W procedurze oceny zgodności należy zbadać i zweryfikować wymogi dotyczące zarówno produktu, jak i procesu, obejmujące cały cykl życia produktów z elementami cyfrowymi, w tym planowanie, projektowanie, opracowywanie lub produkcję, testowanie i utrzymanie produktu.

(45) Co do zasady ocenę zgodności produktów z elementami cyfrowymi powinien przeprowadzać producent na własną odpowiedzialność zgodnie z procedurą na podstawie modułu A określonego w decyzji 768/2008/WE. Producent powinien zachować elastyczność co do możliwości wyboru bardziej rygorystycznej procedury oceny zgodności z udziałem strony trzeciej. Jeżeli produkt sklasyfikowano jako produkt krytyczny klasy I, niezbędny jest zwiększony poziom pewności w celu wykazania zgodności z zasadniczymi wymogami określonymi w niniejszym rozporządzeniu. Jeśli producent chce przeprowadzić ocenę zgodności na własną odpowiedzialność (moduł A), powinien stosować normy zharmonizowane, wspólne specyfikacje lub programy certyfikacji cyberbezpieczeństwa na podstawie rozporządzenia (UE) 2019/881 wskazane przez Komisję w akcie wykonawczym. Jeśli producent nie stosuje takich norm zharmonizowanych, wspólnych specyfikacji ani programów certyfikacji cyberbezpieczeństwa, powinien przeprowadzić ocenę zgodności z udziałem strony trzeciej. Uwzględniając obciążenie administracyjne nałożone na producenta oraz fakt, że cyberbezpieczeństwo odgrywa ważną rolę na etapie projektowania i opracowywania materialnych i niematerialnych produktów z elementami cyfrowymi, wybrano procedury oceny zgodności oparte odpowiednio na modułach B+C lub module H określonych w decyzji 768/2008/WE jako najbardziej odpowiednie do celów przeprowadzenia oceny zgodności produktów krytycznych z elementami cyfrowymi w sposób proporcjonalny i skuteczny. Producent, który organizuje przeprowadzenie oceny zgodności przez stronę trzecią, może wybrać procedurę, która najlepiej odpowiada jego procesom projektowania i produkcji. Biorąc pod uwagę jeszcze większe ryzyko w cyberprzestrzeni związane z używaniem

[18] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30).

[19] Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG (Dz.U. L 218 z 13.8.2008, s. 82).

produktów sklasyfikowanych jako produkty krytyczne klasy II, ocena zgodności powinna zawsze obejmować stronę trzecią.

(46) Chociaż tworzenie materialnych produktów z elementami cyfrowymi zazwyczaj wymaga od producentów podejmowania istotnych starań na etapach projektowania, opracowywania i produkcji, tworzenie produktów z elementami cyfrowymi w formie oprogramowania jest skoncentrowane prawie wyłącznie na projektowaniu i opracowywaniu, natomiast etap produkcji odgrywa mniej znaczącą rolę. Niemniej jednak w wielu przypadkach oprogramowanie przed wprowadzeniem do obrotu nadal należy skompilować, zbudować, zapakietować, udostępnić do pobierania lub skopiować na nośniki fizyczne. Działania te należy uznać za działania odpowiadające produkcji przy stosowaniu odpowiednich modułów oceny zgodności w celu weryfikacji zgodności produktu z zasadniczymi wymaganiami niniejszego rozporządzenia na etapach projektowania, opracowywania i produkcji.

(47) Do celów oceny zgodności produktów z elementami cyfrowymi przeprowadzanej przez osobę trzecią krajowe organy notyfikujące powinny notyfikować Komisji i pozostałym państwom członkowskim jednostki oceniające zgodność, pod warunkiem że spełniają one szereg wymogów, w szczególności dotyczących niezależności, kompetencji i braku konfliktu interesów.

(48) W celu zapewnienia spójnego poziomu jakości podczas przeprowadzania oceny zgodności produktów z elementami cyfrowymi należy także określić wymogi w odniesieniu do organów notyfikujących i innych organów uczestniczących w ocenianiu, notyfikowaniu i monitorowaniu jednostek notyfikowanych. System określony w niniejszym rozporządzeniu należy uzupełnić o system akredytacji przewidziany w rozporządzeniu (WE) nr 765/2008. Ponieważ akredytacja stanowi istotny środek weryfikacji kompetencji jednostek oceniających zgodność, powinno się stosować ją również do celów notyfikacji.

(49) Za preferowaną metodę wykazywania kompetencji technicznych jednostek oceniających zgodność krajowe organy publiczne w całej Unii powinny uznać przejrzystą akredytację zgodną z rozporządzeniem (WE) nr 765/2008, zapewniającą niezbędny poziom zaufania do certyfikatów zgodności. Organy krajowe mogą jednak uznać, że dysponują odpowiednimi środkami do samodzielnego przeprowadzenia takiej oceny. W takich przypadkach w celu zapewnienia odpowiedniego stopnia wiarygodności ocen przeprowadzanych przez inne organy krajowe organy te powinny przedstawić Komisji i innym państwom członkowskim niezbędne dowody w postaci dokumentów wykazujące, że poddane ocenie jednostki oceniające zgodność spełniają odpowiednie wymogi regulacyjne.

(50) Jednostki oceniające zgodność często zlecają realizację części zadań związanych z oceną zgodności podwykonawcom lub korzystają z usług jednostek zależnych. W celu zapewnienia poziomu bezpieczeństwa wymaganego w przypadku produktu z elementami cyfrowymi, który ma zostać wprowadzony do obrotu, zasadnicze znaczenie ma to, aby w ramach wykonywania zadań oceny zgodności podwykonawcy i spółki zależne spełniali te same wymogi co jednostki notyfikowane.

(51) Organ notyfikujący powinien wysłać notyfikację jednostki oceniającej zgodność Komisji i pozostałym państwom członkowskim za pomocą systemu informacyjnego NANDO. NANDO jest elektronicznym narzędziem do notyfikacji, opracowanym i zarządzanym przez Komisję, w którym można znaleźć wykaz wszystkich jednostek notyfikowanych.

(52) Ponieważ jednostki notyfikowane mają możliwość oferowania swoich usług w całej Unii, należy zapewnić pozostałym państwom członkowskim i Komisji możliwość wnoszenia sprzeciwu wobec jednostek notyfikowanych. Istotne zatem jest ustalenie terminu, w jakim możliwe będzie wyjaśnienie jakichkolwiek wątpliwości lub obaw co do kompetencji jednostek oceniających zgodność, zanim zaczną one prowadzić działalność jako jednostki notyfikowane.

(53) Z punktu widzenia konkurencyjności bardzo ważne jest, aby jednostki notyfikowane stosowały procedury oceny zgodności bez tworzenia zbędnego obciążenia dla podmiotów gospodarczych. Z tego samego powodu oraz w celu zapewnienia równego traktowania podmiotów gospodarczych należy zapewnić spójność stosowania procedur oceny zgodności pod względem technicznym. Najlepszym sposobem na osiągnięcie tego celu jest odpowiednia koordynacja jednostek notyfikowanych i współpraca między nimi.

(54) Nadzór rynku jest instrumentem istotnym dla zapewnienia właściwego i jednolitego stosowania przepisów Unii. Dlatego właściwe jest stworzenie ram prawnych, w których nadzór rynku może być sprawowany w sposób odpowiedni. Do produktów z elementami cyfrowymi objętymi niniejszym rozporządzeniem stosuje się przepisy dotyczące nadzoru rynku unijnego oraz kontroli produktów wprowadzanych na rynek Unii przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/1020[20].

(55) Zgodnie z rozporządzeniem (UE) 2019/1020 nadzór rynku na terytorium danego państwa członkowskiego sprawują organy nadzoru rynku. Niniejsze rozporządzenie nie powinno uniemożliwiać państwom członkowskim wyboru właściwych organów do wykonywania tych zadań. Każde państwo członkowskie powinno wyznaczyć na swoim terytorium co najmniej jeden organ nadzoru rynku. Państwa członkowskie mogą wyznaczyć do pełnienia funkcji organu nadzoru rynku dowolny istniejący lub nowy organ, w tym właściwe organy krajowe, o których mowa w art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)], lub wyznaczone krajowe organy ds. certyfikacji cyberbezpieczeństwa, o których mowa w art. 58 rozporządzenia (UE) 2019/881. Podmioty gospodarcze powinny w pełni współpracować z organami nadzoru rynku i innymi właściwymi organami. Każde państwo członkowskie powinno poinformować Komisję i pozostałe państwa członkowskie o swoich organach nadzoru rynku oraz obszarach kompetencji każdego z tych organów, a także zagwarantować zasoby i umiejętności niezbędne do wykonywania zadań z zakresu nadzoru związanych z niniejszym rozporządzeniem. Zgodnie z art. 10 ust. 2 i 3 rozporządzenia (UE) 2019/1020 każde państwo członkowskie powinno wyznaczyć jednolity urząd łącznikowy, który powinien być odpowiedzialny między innymi za reprezentowanie skoordynowanego stanowiska organów nadzoru rynku oraz wspomaganie współpracy między organami nadzoru rynku w różnych państwach członkowskich.

(56) Na podstawie art. 30 ust. 2 rozporządzenia (UE) 2019/1020 należy ustanowić specjalną grupę współpracy administracyjnej (grupę ADCO) w celu jednolitego stosowania niniejszego rozporządzenia. Grupa ADCO powinna składać się z przedstawicieli wyznaczonych krajowych organów nadzoru rynku oraz – w razie potrzeby – z przedstawicieli jednolitych urzędów łącznikowych. Komisja powinna

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.U. L 169 z 25.6.2019, s. 1).

wspierać współpracę między organami nadzoru rynku i zachęcać do takiej współpracy za pośrednictwem Unijnej Sieci ds. Zgodności Produktów ustanowionej na mocy art. 29 rozporządzenia (UE) 2019/1020 i składającej się z przedstawicieli każdego państwa członkowskiego, w tym przedstawiciela każdego z jednolitych urzędów łącznikowych, o których mowa w art. 10 rozporządzenia (UE) 2019/1020, oraz – fakultatywnie – eksperta krajowego, przewodniczących grup ADCO oraz przedstawicieli Komisji. Komisja powinna uczestniczyć w posiedzeniach Sieci, jej podgrup i odpowiedniej grupy ADCO. Powinna także wspierać tę grupę ADCO za pośrednictwem sekretariatu wykonawczego zapewniającego wsparcie techniczne i logistyczne.

(57) W celu zapewnienia terminowych, proporcjonalnych i skutecznych środków dotyczących produktów z elementami cyfrowymi stwarzającymi istotne ryzyko w cyberprzestrzeni należy przewidzieć unijną procedurę ochronną, w ramach której zainteresowane strony będą informowane o planowanych środkach dotyczących takich produktów. Powinna ona również umożliwiać organom nadzoru rynku podejmowanie w razie potrzeby – we współpracy z zainteresowanymi podmiotami gospodarczymi – działań na wcześniejszym etapie. W przypadku gdy państwa członkowskie i Komisja osiągną porozumienie co do zasadności środka przyjętego przez państwo członkowskie, nie należy wymagać dalszego zaangażowania Komisji, z wyjątkiem przypadków, w których niezgodność można przypisać brakom w normie zharmonizowanej.

(58) W określonych przypadkach produkt z elementami cyfrowymi, który jest zgodny z niniejszym rozporządzeniem, może jednak stwarzać istotne ryzyko w cyberprzestrzeni lub stwarzać ryzyko dla zdrowia lub bezpieczeństwa osób, dla wypełnienia obowiązków wynikających z prawa Unii lub prawa krajowego mających na celu ochronę praw podstawowych, dostępności, autentyczności, integralności lub poufności usług oferowanych przy użyciu elektronicznego systemu informacyjnego przez podmioty niezbędne takie jak podmioty, o których mowa w [załączniku I do dyrektywy XXX/XXXX (NIS 2)], lub dla innych aspektów ochrony interesu publicznego. Z tego względu niezbędne jest ustanowienie zasad gwarantujących zmniejszenie tego rodzaju ryzyka. W związku z tym organy nadzoru rynku powinny wprowadzić środki w celu nałożenia na podmioty gospodarcze obowiązku zapewnienia, aby produkt przestał stwarzać dane ryzyko, odzyskania produktu lub wycofania go, w zależności od ryzyka. Gdy tylko organ nadzoru rynku ograniczy swobodny przepływ lub zakaże swobodnego przepływu produktu, państwo członkowskie powinno bezzwłocznie powiadomić Komisję i pozostałe państwa członkowskie o środkach tymczasowych, podając powody oraz uzasadnienie tej decyzji. W przypadku gdy organ nadzoru rynku wprowadza takie środki w odniesieniu do produktów stwarzających ryzyko, Komisja powinna niezwłocznie rozpocząć konsultacje z odnośnymi państwami członkowskimi i zainteresowanym podmiotem gospodarczym lub zainteresowanymi podmiotami gospodarczymi oraz dokonać oceny tego środka krajowego. Na podstawie wyników tej oceny Komisja powinna zdecydować, czy środek krajowy jest uzasadniony czy nie. Komisja powinna skierować swoją decyzję do wszystkich państw członkowskich i natychmiast przekazać ją państwom członkowskim oraz stosownemu podmiotowi lub stosownym podmiotom gospodarczym. Jeśli środek zostanie uznany za uzasadniony, Komisja może również rozważyć przyjęcie wniosków dotyczących zmiany właściwych przepisów Unii.

(59) W przypadku produktów z elementami cyfrowymi stwarzających istotne ryzyko w cyberprzestrzeni oraz w przypadkach, w których istnieją powody, aby przypuszczać, że produkty te nie są zgodne z niniejszym rozporządzeniem, lub w przypadku produktów, które są zgodne z niniejszym rozporządzeniem, ale stwarzają inne istotne ryzyko, takie jak ryzyko dla zdrowia lub bezpieczeństwa osób, praw podstawowych lub świadczenia usług przez podmioty niezbędne takie jak podmioty, o których mowa w [załączniku I do dyrektywy XXX/XXXX (NIS 2)], Komisja może zwrócić się do ENISA o przeprowadzenie oceny. Na podstawie tej oceny Komisja może przyjąć, w drodze aktów wykonawczych, środki naprawcze lub ograniczające na szczeblu Unii, w tym nakaz wycofania z obrotu lub odzyskania przedmiotowych produktów w rozsądnym terminie, stosownym do charakteru ryzyka. Komisja może skorzystać z takiej interwencji wyłącznie w wyjątkowych okolicznościach, które uzasadniają niezwłoczną interwencję w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego oraz wyłącznie wówczas, gdy organy nadzoru nie wprowadziły żadnych skutecznych środków w celu zaradzenia sytuacji. Takimi wyjątkowymi okolicznościami mogą być sytuacje nadzwyczajne, w których przykładowo niezgodny produkt jest szeroko udostępniany przez producenta w kilku państwach członkowskich i wykorzystywany także w kluczowych sektorach przez podmioty objęte zakresem [dyrektywy XXX/XXXX (NIS 2)], mimo że zawiera znane podatności, które są wykorzystywane przez podmioty działające w złym zamiarze i w odniesieniu do których producent nie zapewnia dostępnych poprawek. W takich sytuacjach nadzwyczajnych Komisja może interweniować wyłącznie na czas trwania wyjątkowych okoliczności oraz jeśli niezgodność z niniejszym rozporządzeniem lub istotne ryzyko stwarzane przez produkt się utrzymują.

(60) W przypadkach, w których istnieją przesłanki wskazujące na niezgodność z niniejszym rozporządzeniem w kilku państwach członkowskich, organy nadzoru rynku powinny mieć możliwość podjęcia wspólnych działań z innymi organami w celu weryfikacji zgodności oraz identyfikacji ryzyka w cyberprzestrzeni dotyczącego produktów z elementami cyfrowymi.

(61) Jednoczesne skoordynowane działania kontrolne („akcje kontrolne”) są określonymi akcjami kontrolnymi przeprowadzanymi przez organy nadzoru rynku, które mogą jeszcze bardziej wzmocnić bezpieczeństwo produktu. Akcje kontrolne należy przeprowadzać w szczególności wówczas, gdy tendencje rynkowe, skargi konsumentów lub inne przesłanki wskazują, że określone kategorie produktów są często uznawane za stwarzające ryzyko w cyberprzestrzeni. ENISA powinna składać wnioski dotyczące kategorii produktów, w odniesieniu do których organy nadzoru rynku mogą organizować akcje kontrolne, między innymi na podstawie otrzymywanych zgłoszeń podatności produktu oraz incydentów.

(62) Aby w razie potrzeby zapewnić możliwość dostosowania ram regulacyjnych, należy przekazać Komisji uprawnienia do przyjmowania na podstawie art. 290 Traktatu aktów w celu aktualizacji wykazu produktów krytycznych zawartych w załączniku III oraz sprecyzowania definicji tych kategorii produktów. Należy też przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z tym artykułem w celu wskazania produktów z elementami cyfrowymi objętych innymi przepisami unijnymi, które zapewniają taki sam poziom ochrony jak niniejsze rozporządzenie, w których Komisja powinna określić, czy konieczne jest ograniczenie lub wyłączenie z zakresu niniejszego rozporządzenia, jak również – w stosownych przypadkach – zakres tego ograniczenia. Należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z tym artykułem w odniesieniu do potencjalnego upoważnienia do certyfikacji

określonych produktów wysoce krytycznych z elementami cyfrowymi w oparciu o kryteria krytyczności wskazane w niniejszym rozporządzeniu, jak również do określenia minimalnego zakresu deklaracji zgodności UE oraz uzupełnienia elementów, które należy uwzględnić w dokumentacji technicznej. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[21]. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(63) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze do: określenia formatu i elementów zestawienia podstawowych materiałów do produkcji oprogramowania, dokładniejszego określenia rodzaju informacji przekazywanych w zgłoszeniach aktywnie wykorzystywanych podatności oraz incydentów składanych w ENISA przez producentów oraz formatu tych zgłoszeń i procedury ich składania, określenia przyjętych na podstawie rozporządzenia (UE) 2019/881 europejskich programów certyfikacji cyberbezpieczeństwa, z których można korzystać w celu wykazania zgodności z zasadniczymi wymogami lub ich częściami wskazanymi w załączniku I do niniejszego rozporządzenia, przyjmowania wspólnych specyfikacji dotyczących zasadniczych wymogów określonych w załączniku I, określania specyfikacji technicznych dotyczących piktogramów lub wszelkich innych znaków związanych z bezpieczeństwem produktów z elementami cyfrowymi oraz mechanizmów służących promowaniu ich wykorzystania, podejmowania decyzji o zastosowaniu środków naprawczych lub ograniczających na szczeblu Unii w wyjątkowych okolicznościach, które uzasadniają natychmiastową interwencję w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[22].

(64) W celu zapewnienia opartej na zaufaniu i konstruktywnej współpracy organów nadzoru rynku na szczeblu unijnym i krajowym wszystkie strony zaangażowane w stosowanie niniejszego rozporządzenia powinny przestrzegać zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań.

(65) Aby zapewnić skuteczne egzekwowanie obowiązków przewidzianych w niniejszym rozporządzeniu, każdy organ nadzoru rynku powinien być uprawniony do nakładania lub żądania nałożenia administracyjnych kar pieniężnych. Z tego względu należy określić maksymalne poziomy administracyjnych kar pieniężnych, które powinno się przewidzieć w przepisach krajowych za nieprzestrzeganie obowiązków określonych w niniejszym rozporządzeniu. Decydując o wysokości administracyjnej kary pieniężnej w każdym indywidualnym przypadku, należy uwzględnić wszystkie istotne okoliczności konkretnej sytuacji, a co najmniej te wyraźnie określone w niniejszym rozporządzeniu, w tym to, czy wobec tego samego podmiotu gospodarczego za

[21] Dz.U. L 123 z 12.5.2016, s. 1.

[22] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

podobne naruszenia inne organy nadzoru rynku zastosowały już administracyjne kary pieniężne. Mogą to być zarówno okoliczności obciążające, w sytuacjach, w których naruszenie popełnione przez ten sam podmiot gospodarczy utrzymuje się na terytorium państw członkowskich innych niż to, w którym już zastosowano administracyjną karę pieniężną, lub okoliczności łagodzące, które polegają na zapewnieniu, aby w każdej innej administracyjnej karze pieniężnej rozważanej przez inny organ nadzoru rynku dla tego samego podmiotu gospodarczego lub za taki sam rodzaj naruszenia uwzględniono, oprócz innych istotnych określonych okoliczności, karę oraz jej wysokość nałożoną w innych państwach członkowskich. We wszystkich takich przypadkach przy wymierzaniu łącznej administracyjnej kary pieniężnej, którą mogą zastosować organy nadzoru rynku kilku państw członkowskich wobec tego samego podmiotu gospodarczego za ten sam rodzaj naruszenia, należy zagwarantować poszanowanie zasady proporcjonalności.

(66) Jeżeli administracyjne kary pieniężne są nakładane na osoby niebędące przedsiębiorstwem, właściwy organ, ustalając właściwą wysokość kary pieniężnej, powinien brać pod uwagę ogólny poziom dochodów w danym państwie członkowskim oraz sytuację ekonomiczną tej osoby. Państwa członkowskie powinny określić, czy i w jakim zakresie administracyjnym karom pieniężnym powinny podlegać organy publiczne.

(67) W stosunkach z państwami trzecimi UE dąży do promowania międzynarodowego handlu produktami regulowanymi. W celu ułatwienia handlu można stosować szeroki zakres środków, w tym kilka instrumentów prawnych, takich jak dwustronne (międzyrządowe) umowy o wzajemnym uznawaniu oceny zgodności oraz znakowanie produktów regulowanych. Umowy o wzajemnym uznawaniu są zawierane między Unią a państwami trzecimi, które znajdują się na porównywalnym poziomie rozwoju technicznego oraz mają podobne podejście do oceny zgodności. Umowy te są oparte na wzajemnej akceptacji certyfikatów, znaków zgodności oraz raportów z badań wydawanych przez jednostki oceniające zgodność którejkolwiek ze stron zgodnie z prawodawstwem drugiej strony. Obecnie umowy o wzajemnym uznawaniu obowiązują w odniesieniu do kilku krajów. Umowy zawarto w odniesieniu do szeregu sektorów, które mogą różnić się w zależności od kraju. Aby jeszcze bardziej ułatwić handel, a także z uwagi na fakt, że łańcuchy dostaw produktów z elementami cyfrowymi mają charakter globalny, umowy o wzajemnym uznawaniu dotyczące oceny zgodności mogą być zawierane przez Unię w odniesieniu do produktów regulowanych na podstawie niniejszego rozporządzenia zgodnie z art. 218 TFUE. W kontekście wzmocnienia cyberodporności w wymiarze globalnym ważna jest także współpraca z krajami partnerskimi, gdyż w perspektywie długoterminowej przyczyni się ona do wzmocnienia ram cyberbezpieczeństwa zarówno w Unii, jak i poza nią.

(68) Komisja powinna okresowo dokonywać przeglądu niniejszego rozporządzenia, w drodze konsultacji z zainteresowanymi stronami, w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się warunków społecznych, politycznych, technologicznych lub rynkowych.

(69) Podmiotom gospodarczym należy zapewnić wystarczająco dużo czasu na dostosowanie się do wymogów niniejszego rozporządzenia. Niniejsze rozporządzenie powinno mieć zastosowanie po upływie [24 miesięcy] od jego wejścia w życie, z wyjątkiem obowiązków w zakresie zgłaszania incydentów dotyczących aktywnie wykorzystywanych podatności oraz incydentów, które to przepisy powinny mieć zastosowanie po upływie [12 miesięcy] od wejścia w życie niniejszego rozporządzenia.

(70) Ponieważ cel niniejszego rozporządzenia nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na skutki działania możliwe jest lepsze jego osiągnięcie na poziomie Unii, Unia może podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(71) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 Parlamentu Europejskiego i Rady skonsultowano się z Europejskim Inspektorem Ochrony Danych[23], który wydał opinię dnia […] r.,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu ustanawia się:

a) przepisy dotyczące wprowadzania do obrotu produktów z elementami cyfrowymi w celu zapewnienia cyberbezpieczeństwa takich produktów;

b) zasadnicze wymogi dotyczące projektowania, opracowywania i produkcji produktów z elementami cyfrowymi oraz obowiązki podmiotów gospodarczych w odniesieniu do tych produktów w zakresie cyberbezpieczeństwa;

c) zasadnicze wymogi dotyczące procedur postępowania w przypadku wykrycia podatności wprowadzonych przez producentów w celu zapewnienia cyberbezpieczeństwa produktów z elementami cyfrowymi w całym cyklu życia oraz obowiązki podmiotów gospodarczych w odniesieniu do tych procedur;

d) przepisy dotyczące nadzoru rynku i egzekwowania wyżej wymienionych przepisów i wymogów.

Artykuł 2

Zakres

1. Niniejsze rozporządzenie stosuje się do produktów z elementami cyfrowymi, których przeznaczenie lub racjonalnie przewidywalne wykorzystanie obejmuje bezpośrednie lub pośrednie logiczne lub fizyczne połączenie danych z urządzeniem lub siecią.

2. Niniejszego rozporządzenia nie stosuje się do produktów z elementami cyfrowymi, do których zastosowanie mają następujące akty Unii:

   a) rozporządzenie (UE) 2017/745;

[23] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

b) rozporządzenie (UE) 2017/746;

c) rozporządzenie (UE) 2019/2144.

3. Niniejszego rozporządzenia nie stosuje się do produktów z elementami cyfrowymi, które uzyskały certyfikację zgodnie z rozporządzeniem (UE) 2018/1139.

4. Stosowanie niniejszego rozporządzenia do produktów z elementami cyfrowymi objętych innymi przepisami unijnymi ustanawiającymi wymogi odnoszące się do wszystkich lub niektórych rodzajów ryzyka objętych zasadniczymi wymogami określonymi w załączniku I może zostać ograniczone lub podlegać wyłączeniu, jeżeli:

a) takie ograniczenie lub wyłączenie jest spójne z ogólnymi ramami regulacyjnymi mającymi zastosowanie do tych produktów oraz

b) przepisy sektorowe zapewniają taki sam poziom ochrony jak ten przewidziany w niniejszym rozporządzeniu.

Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 50 w celu zmiany niniejszego rozporządzenia polegającej na określeniu, czy takie ograniczenie lub wyłączenie jest niezbędne, określeniu odnośnych produktów i przepisów, jak również – w stosownych przypadkach – zakresu ograniczenia.

5. Niniejszego rozporządzenia nie stosuje się do produktów z elementami cyfrowymi opracowanych wyłącznie na potrzeby bezpieczeństwa narodowego lub do celów wojskowych ani do produktów zaprojektowanych specjalnie w celu przetwarzania informacji niejawnych.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „produkt z elementami cyfrowymi” oznacza oprogramowanie komputerowe lub sprzęt komputerowy oraz powiązane z nimi rozwiązania w zakresie zdalnego przetwarzania danych, w tym komponenty oprogramowania lub sprzętu, które mają zostać oddzielnie wprowadzone do obrotu;

2) „zdalne przetwarzanie danych” oznacza przetwarzanie danych na odległość, na potrzeby którego oprogramowanie zostało zaprojektowane i opracowane przez producenta lub na odpowiedzialność producenta, a którego brak spowodowałby, że produkt z elementami cyfrowymi nie mógłby wykonywać jednej ze swoich funkcji;

3) „produkt krytyczny z elementami cyfrowymi” oznacza produkt z elementami cyfrowymi, który stwarza ryzyko w cyberprzestrzeni zgodnie z kryteriami określonymi w art. 6 ust. 2 oraz którego podstawowa funkcjonalność jest określona w załączniku III;

4) „produkt wysoce krytyczny z elementami cyfrowymi” oznacza produkt z elementami cyfrowymi, który stwarza ryzyko w cyberprzestrzeni zgodnie z kryteriami określonymi w art. 6 ust. 5;

5) „technologia operacyjna” oznacza programowalne cyfrowe systemy lub urządzenia, które wchodzą w interakcje ze środowiskiem fizycznym lub zarządzają urządzeniami, które wchodzą w interakcje ze środowiskiem fizycznym;

6) „oprogramowanie” oznacza część elektronicznego systemu informacyjnego, która składa się z kodu komputerowego;

7) „sprzęt” oznacza fizyczny elektroniczny system informacyjny lub jego części zdolne do przetwarzania, przechowywania lub przekazywania danych cyfrowych;

8) „komponent” oznacza oprogramowanie lub sprzęt przeznaczone do zintegrowania z elektronicznym systemem informacyjnym;

9) „elektroniczny system informacyjny” oznacza system, w tym sprzęt elektryczny lub elektroniczny, zdolny do przetwarzania, przechowywania lub przekazywania danych cyfrowych;

10) „połączenie logiczne” oznacza wirtualną reprezentację połączenia danych zrealizowanego za pośrednictwem interfejsu oprogramowania;

11) „połączenie fizyczne” oznacza każde połączenie między elektronicznymi systemami informacyjnymi lub komponentami zrealizowane przy użyciu środków fizycznych, w tym za pośrednictwem interfejsów elektrycznych lub mechanicznych, przewodów lub fal radiowych;

12) „połączenie pośrednie” oznacza połączenie z urządzeniem lub siecią, które nie jest nawiązywane bezpośrednio, lecz jako część większego systemu, który można bezpośrednio połączyć z takim urządzeniem lub siecią;

13) „uprawnienie” oznacza prawo dostępu przyznane konkretnym użytkownikom lub programom, aby umożliwić im wykonywanie działań istotnych dla bezpieczeństwa w ramach elektronicznego systemu informacyjnego;

14) „podwyższone uprawnienie” oznacza prawo dostępu przyznane konkretnym użytkownikom lub programom, aby umożliwić im wykonywanie rozszerzonego zakresu działań istotnych dla bezpieczeństwa w ramach elektronicznego systemu informacyjnego, które w razie nadużycia lub naruszenia może ułatwić podmiotowi działającemu w złym zamiarze uzyskanie szerszego dostępu do zasobów systemu lub organizacji;

15) „punkt końcowy” oznacza każde urządzenie, które jest połączone z siecią i służy jako punkt wejścia do tej sieci;

16) „zasoby sieciowe lub obliczeniowe” oznaczają funkcjonalność z zakresu danych lub sprzętu lub oprogramowania, która jest dostępna lokalnie albo za pośrednictwem sieci lub innego urządzenia podłączonego do internetu;

17) „podmiot gospodarczy” oznacza producenta, upoważnionego przedstawiciela, importera, dystrybutora lub każdą inną osobę fizyczną lub prawną, na której spoczywają obowiązki określone w niniejszym rozporządzeniu;

18) „producent” oznacza każdą osobę fizyczną lub prawną, która opracowuje lub wytwarza produkty z elementami cyfrowymi lub zleca zaprojektowanie, opracowanie lub wytworzenie produktów z elementami cyfrowymi i wprowadza te produkty do obrotu pod własną nazwą lub znakiem towarowym, odpłatnie lub nieodpłatnie;

19) „upoważniony przedstawiciel” oznacza każdą osobę fizyczną lub prawną, która ma miejsce zamieszkania lub siedzibę w Unii i otrzymała od producenta pisemne upoważnienie do występowania w jego imieniu w zakresie określonych zadań;

20) „importer” oznacza każdą osobę fizyczną lub prawną, która ma miejsce zamieszkania lub siedzibę w Unii i wprowadza do obrotu produkt z elementami cyfrowymi opatrzony nazwą handlową lub znakiem towarowym osoby fizycznej lub prawnej mającej miejsce zamieszkania lub siedzibę poza granicami Unii;

21) „dystrybutor” oznacza każdą osobę fizyczną lub prawną w łańcuchu dostaw, inną niż producent lub importer, która udostępnia produkt z elementami cyfrowymi na rynku unijnym bez zmiany jego właściwości;

22) „wprowadzenie do obrotu” oznacza udostępnienie produktu z elementami cyfrowymi na rynku Unii po raz pierwszy;

23) „udostępnienie na rynku” oznacza dostarczenie produktu z elementami cyfrowymi do celów dystrybucji lub używania na rynku Unii w ramach działalności handlowej, odpłatnie lub nieodpłatnie;

24) „przeznaczenie” oznacza zastosowanie, do którego produkt z elementami cyfrowymi został przeznaczony przez jego producenta, w tym określony kontekst i warunki wykorzystywania, wskazane w informacjach dostarczonych przez producenta w instrukcji obsługi, materiałach promocyjnych lub sprzedażowych i oświadczeniach, jak również w dokumentacji technicznej;

25) „racjonalnie przewidywalne wykorzystanie” oznacza zastosowanie, które niekoniecznie jest przeznaczeniem podanym przez producenta w instrukcji obsługi, materiałach promocyjnych lub sprzedażowych i oświadczeniach, jak również w dokumentacji technicznej, ale które prawdopodobnie wynika z dającego się racjonalnie przewidzieć zachowania człowieka, operacji technicznych lub interakcji;

26) „racjonalnie przewidywalne niewłaściwe wykorzystanie” oznacza wykorzystanie produktu z elementami cyfrowymi w sposób niezgodny z jego przeznaczeniem, które może jednak wynikać z dającego się racjonalnie przewidzieć zachowania człowieka lub interakcji z innymi systemami;

27) „organ notyfikujący” oznacza organ krajowy, który odpowiada za opracowanie i stosowanie procedur koniecznych do oceny, wyznaczania i notyfikowania jednostek oceniających zgodność oraz za ich monitorowanie;

28) „ocena zgodności” oznacza proces weryfikacji, czy spełniono zasadnicze wymogi określone w załączniku I;

29) „jednostka oceniająca zgodność” oznacza jednostkę zdefiniowaną w art. 2 pkt 13 rozporządzenia (UE) nr 765/2008;

30) „jednostka notyfikowana” oznacza jednostkę oceniającą zgodność wyznaczoną zgodnie z art. 33 niniejszego rozporządzenia i innym stosownym unijnym prawodawstwem harmonizacyjnym;

31) „istotna modyfikacja” oznacza zmianę w produkcie z elementami cyfrowymi po jego wprowadzeniu do obrotu, która wpływa na zgodność produktu z elementami cyfrowymi z zasadniczymi wymogami określonymi w sekcji 1 załącznika I lub powoduje zmianę przeznaczenia, w odniesieniu do którego oceniono produkt z elementami cyfrowymi;

32) „oznakowanie zgodności CE” oznacza oznakowanie, za pomocą którego producent wskazuje, że produkt z elementami cyfrowymi i procedury wprowadzone przez producenta spełniają zasadnicze wymogi określone w załączniku I i innych mających zastosowanie przepisach Unii harmonizujących warunki wprowadzania produktów

do obrotu („unijne prawodawstwo harmonizacyjne”), przewidujących umieszczanie takiego oznakowania;

33) „organ nadzoru rynku” oznacza organ nadzoru rynku zgodnie z definicją zawartą w art. 3 pkt 4 rozporządzenia (UE) 2019/1020;

34) „norma zharmonizowana” oznacza normę zharmonizowaną zgodnie z definicją zawartą w art. 2 pkt 1 lit. c) rozporządzenia (UE) nr 1025/2012;

35) „ryzyko w cyberprzestrzeni” oznacza ryzyko zgodnie z definicją zawartą w art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)];

36) „istotne ryzyko w cyberprzestrzeni” oznacza ryzyko w cyberprzestrzeni, w przypadku którego, na podstawie jego charakterystyki technicznej, można założyć wysokie prawdopodobieństwo wystąpienia incydentu, który mógłby doprowadzić do poważnych negatywnych skutków, w tym przez spowodowanie znacznej straty materialnej lub niematerialnej lub znacznego zakłócenia;

37) „zestawienie podstawowych materiałów do produkcji oprogramowania” oznacza formalny zapis zawierający szczegóły i relacje w łańcuchu dostaw składników wchodzących w skład elementów oprogramowania komputerowego produktu z elementami cyfrowymi;

38) „podatność” oznacza podatność zgodnie z definicją zawartą w art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)];

39) „aktywnie wykorzystywana podatność” oznacza podatność, w przypadku której istnieją wiarygodne dowody, że podmiot wprowadził do systemu kod złośliwy bez zgody właściciela systemu;

40) „dane osobowe” oznaczają dane zgodnie z definicją zawartą w art. 4 pkt 1 rozporządzenia (UE) 2016/679.

Artykuł 4

Swobodny przepływ

1. Państwa członkowskie nie mogą – w odniesieniu do spraw objętych zakresem niniejszego rozporządzenia – utrudniać udostępniania na rynku produktów z elementami cyfrowymi zgodnych z niniejszym rozporządzeniem.

2. Podczas targów, wystaw i pokazów lub podobnych imprez państwa członkowskie nie mogą uniemożliwiać prezentowania i używania produktu z elementami cyfrowymi, który nie jest zgodny z niniejszym rozporządzeniem.

3. Państwa członkowskie nie mogą uniemożliwiać udostępniania nieukończonego oprogramowania, które nie jest zgodne z niniejszym rozporządzeniem, pod warunkiem że oprogramowanie to jest udostępniane jedynie na ograniczony okres wymagany do celów testowania oraz że widoczny znak wyraźnie wskazuje, że nie jest ono zgodne z niniejszym rozporządzeniem i nie będzie dostępne na rynku do celów innych niż testowanie.

Artykuł 5

Wymogi dotyczące produktów z elementami cyfrowymi

Produkty z elementami cyfrowymi udostępnia się na rynku tylko wtedy, gdy:

1) spełniają one zasadnicze wymogi przewidziane w sekcji 1 załącznika I, pod warunkiem że zostały one prawidłowo zainstalowane oraz są prawidłowo utrzymywane i wykorzystywane zgodnie z ich przeznaczeniem lub w warunkach, które można racjonalnie przewidzieć, a także – w stosownych przypadkach – są aktualizowane, oraz

2) procedury wprowadzone przez producenta są zgodne z zasadniczymi wymogami określonymi w sekcji 2 załącznika I.

Artykuł 6

Produkty krytyczne z elementami cyfrowymi

1. Produkty z elementami cyfrowymi należące do kategorii wskazanej w załączniku III uważa się za produkty krytyczne z elementami cyfrowymi. Produkty, których podstawowa funkcjonalność należy do jednej z kategorii wymienionych w załączniku III do niniejszego rozporządzenia, uważa się za należące do tej kategorii. Kategorie produktów krytycznych z elementami cyfrowymi dzieli się na klasy I i II, jak określono w załączniku III, które odzwierciedlają poziom ryzyka w cyberprzestrzeni związanego z tymi produktami.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 50 w celu zmiany załącznika III przez uwzględnienie w wykazie kategorii produktów krytycznych z elementami cyfrowymi nowej kategorii lub usunięcie z tego wykazu istniejącej kategorii. Przy ocenianiu potrzeby zmiany wykazu zawartego w załączniku III Komisja bierze pod uwagę poziom ryzyka w cyberprzestrzeni związanego z kategorią produktów z elementami cyfrowymi. Przy określaniu poziomu ryzyka w cyberprzestrzeni bierze się pod uwagę co najmniej jedno z następujących kryteriów:

   a) funkcjonalność produktu z elementami cyfrowymi związaną z cyberbezpieczeństwem oraz posiadanie przez produkt z elementami cyfrowymi co najmniej jednej z następujących cech:

      (i) został zaprojektowany do eksploatacji przez użytkowników z podwyższonym uprawnieniem lub z uprawnieniami do zarządzania;

      (ii) ma bezpośredni lub uprzywilejowany dostęp do zasobów sieciowych lub obliczeniowych;

      (iii) jest przeznaczony do kontrolowania dostępu do danych lub technologii operacyjnej;

      (iv) pełni funkcję krytyczną dla zaufania, w szczególności funkcje bezpieczeństwa, takie jak kontrola sieci, ochrona punktów końcowych i ochrona sieci.

   b) przeznaczenie do stosowania w środowiskach wrażliwych, w tym w środowisku przemysłowym lub przez podmioty niezbędne takie jak podmioty, o których mowa w załączniku [załączniku I] do dyrektywy [dyrektywy XXX/XXXX (NIS 2)];

   c) przeznaczenie do wykonywania funkcji krytycznych lub wrażliwych, takich jak przetwarzanie danych osobowych;

   d) potencjalny zakres niekorzystnego wpływu, w szczególności pod względem jego nasilenia i możliwości oddziaływania na wiele osób;

e) zakres, w jakim wykorzystywanie produktów z elementami cyfrowymi spowodowało już stratę materialną lub niematerialną lub zakłócenie lub wzbudziło istotne obawy co do możliwości wystąpienia niekorzystnego wpływu.

3. Komisja jest uprawniona do przyjęcia aktu delegowanego zgodnie z art. 50 w celu uzupełnienia niniejszego rozporządzenia przez określenie definicji kategorii produktów w klasie I i klasie II zgodnie z załącznikiem III. Akt delegowany przyjmuje się [w terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia].

4. Produkty krytyczne z elementami cyfrowymi podlegają procedurom oceny zgodności, o których mowa w art. 24 ust. 2 i 3.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 50 w celu uzupełnienia niniejszego rozporządzenia przez określenie kategorii produktów wysoce krytycznych z elementami cyfrowymi, w odniesieniu do których producenci mają obowiązek uzyskać europejski certyfikat cyberbezpieczeństwa w ramach europejskiego programu certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881, aby wykazać zgodność z zasadniczymi wymogami określonymi w załączniku I lub jego częściach. Przy określaniu takich kategorii produktów wysoce krytycznych z elementami cyfrowymi Komisja uwzględnia poziom ryzyka w cyberprzestrzeni związanego z kategorią produktów z elementami cyfrowymi w świetle co najmniej jednego z kryteriów wymienionych w ust. 2, a także w kontekście oceny, czy ta kategoria produktów jest:

a) wykorzystywana przez podmioty niezbędne takie jak podmioty, o których mowa w załączniku [załączniku I] do dyrektywy [dyrektywy XXX/XXXX (NIS 2)], czy wspomniane podmioty polegają na tej kategorii produktów lub czy będzie ona miała potencjalne przyszłe znaczenie dla działalności tych podmiotów lub

b) istotna dla odporności całego łańcucha dostaw produktów z elementami cyfrowymi na zdarzenia powodujące zakłócenia.

Artykuł 7

Ogólne bezpieczeństwo produktów

Na zasadzie odstępstwa od art. 2 ust. 1 akapit trzeci lit. b) rozporządzenia [rozporządzenia w sprawie ogólnego bezpieczeństwa produktów], w przypadku gdy produkty z elementami cyfrowymi nie podlegają szczególnym wymogom określonym w innym unijnym prawodawstwie harmonizacyjnym w rozumieniu [art. 3 pkt 25 rozporządzenia w sprawie ogólnego bezpieczeństwa produktów], zastosowanie do tych produktów w odniesieniu do zagrożeń dla bezpieczeństwa nieobjętych niniejszym rozporządzeniem mają rozdział III sekcja 1, rozdziały V i VII oraz rozdziały IX–XI rozporządzenia [rozporządzenia w sprawie ogólnego bezpieczeństwa produktów].

Artykuł 8

Systemy sztucznej inteligencji wysokiego ryzyka

1. Produkty z elementami cyfrowymi sklasyfikowane jako systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. [art. 6] rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji], które wchodzą w zakres niniejszego

rozporządzenia i spełniają zasadnicze wymogi określone w sekcji 1 załącznika I do niniejszego rozporządzenia oraz w przypadku których procedury wprowadzone przez producenta są zgodne z zasadniczymi wymogami określonymi w sekcji 2 załącznika I, uznaje się za spełniające wymogi dotyczące cyberbezpieczeństwa określone w art. [art. 15] rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji], bez uszczerbku dla innych wymogów dotyczących dokładności i solidności zawartych w wyżej wymienionym artykule oraz w zakresie, w jakim osiągnięcie poziomu ochrony określonego w tych wymogach wykazano w deklaracji zgodności UE wydanej na podstawie niniejszego rozporządzenia.

2. W przypadku produktów i wymogów cyberbezpieczeństwa, o których mowa w ust. 1, stosuje się odpowiednią procedurę oceny zgodności wymaganą na mocy art. [art. 43] rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji]. Do celów tej oceny jednostki notyfikowane, które są uprawnione do kontroli zgodności systemów sztucznej inteligencji wysokiego ryzyka zgodnie z rozporządzeniem [rozporządzeniem w sprawie sztucznej inteligencji], są również uprawnione do kontroli zgodności systemów sztucznej inteligencji wysokiego ryzyka objętych zakresem niniejszego rozporządzenia z wymogami określonymi w załączniku I do niniejszego rozporządzenia, pod warunkiem że zgodność tych jednostek notyfikowanych z wymogami określonymi w art. 29 niniejszego rozporządzenia oceniono w kontekście procedury notyfikacyjnej zgodnie z rozporządzeniem [rozporządzeniem w sprawie sztucznej inteligencji].

3. Na zasadzie odstępstwa od ust. 2 produkty krytyczne z elementami cyfrowymi wymienione w załączniku III do niniejszego rozporządzenia, które muszą być objęte procedurami oceny zgodności, o których mowa w art. 24 ust. 2 lit. a) i b) oraz art. 24 ust. 3 lit. a) i b) niniejszego rozporządzenia, i które są również sklasyfikowane jako systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. [art. 6] rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji] i do których stosuje się procedurę oceny zgodności opierającą się na kontroli wewnętrznej, o której mowa w załączniku [załączniku VI] do rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji], podlegają procedurom oceny zgodności wymaganym zgodnie z niniejszym rozporządzeniem w zakresie, w jakim dotyczy to zasadniczych wymogów niniejszego rozporządzenia.

Artykuł 9

Produkty maszynowe

Produkty maszynowe objęte zakresem rozporządzenia [wniosku dotyczącego rozporządzenia w sprawie maszyn], które są produktami z elementami cyfrowymi w rozumieniu niniejszego rozporządzenia i w odniesieniu do których wydano deklarację zgodności UE na podstawie niniejszego rozporządzenia, uznaje się za zgodne z zasadniczymi wymaganiami w zakresie ochrony zdrowia i bezpieczeństwa określonymi w załączniku [sekcjach 1.1.9 i 1.2.1 załącznika III] do rozporządzenia [wniosku dotyczącego rozporządzenia w sprawie maszyn] w odniesieniu do zabezpieczenia przed uszkodzeniem oraz bezpieczeństwa i niezawodności układów sterowania oraz w zakresie, w jakim osiągnięcie poziomu ochrony przewidzianego w tych wymaganiach wykazano w deklaracji zgodności UE wydanej na podstawie niniejszego rozporządzenia.

ROZDZIAŁ II

OBOWIĄZKI PODMIOTÓW GOSPODARCZYCH

Artykuł 10

Obowiązki producentów

1. Wprowadzając produkt z elementami cyfrowymi do obrotu, producenci zapewniają, aby został on zaprojektowany, opracowany i wyprodukowany zgodnie z zasadniczymi wymogami określonymi w sekcji 1 załącznika I.

2. Aby spełnić obowiązek określony w ust. 1, producenci przeprowadzają ocenę ryzyka w cyberprzestrzeni związanego z produktem z elementami cyfrowymi i uwzględniają wynik tej oceny na etapie planowania, projektowania, opracowywania, produkcji, dostarczania i utrzymania produktu z elementami cyfrowymi w celu zminimalizowania ryzyka w cyberprzestrzeni, zapobiegania incydentom i zminimalizowania skutków takich incydentów, w tym w odniesieniu do zdrowia i bezpieczeństwa użytkowników.

3. Wprowadzając produkt z elementami cyfrowymi do obrotu, producent włącza ocenę ryzyka w cyberprzestrzeni do dokumentacji technicznej określonej w art. 23 i załączniku V. W przypadku produktów z elementami cyfrowymi, o których mowa w art. 8 i art. 24 ust. 4, podlegających również innym aktom Unii, ocena ryzyka w cyberprzestrzeni może być częścią oceny ryzyka wymaganej na podstawie tych odpowiednich aktów Unii. Jeżeli niektóre zasadnicze wymogi nie mają zastosowania do wprowadzonego do obrotu produktu z elementami cyfrowymi, producent zamieszcza w tej dokumentacji wyraźne uzasadnienie.

4. W celu wypełnienia obowiązku określonego w ust. 1 producenci dokładają należytej staranności przy integrowaniu z produktami z elementami cyfrowymi komponentów pochodzących od stron trzecich. Producenci zapewniają, aby takie komponenty nie naruszały bezpieczeństwa produktu z elementami cyfrowymi.

5. Producent systematycznie dokumentuje, w sposób proporcjonalny do charakteru i ryzyka w cyberprzestrzeni, istotne aspekty cyberbezpieczeństwa dotyczące produktu z elementami cyfrowymi, w tym podatności, o których się dowiedział, oraz wszelkie istotne informacje przekazane przez strony trzecie, a także, w stosownych przypadkach, aktualizuje ocenę ryzyka produktu.

6. Przy wprowadzaniu produktu z elementami cyfrowymi do obrotu oraz przez cały przewidywany okres eksploatacji produktu lub przez okres pięciu lat od wprowadzenia produktu do obrotu, w zależności od tego, który z tych okresów jest krótszy, producenci zapewniają skuteczne i zgodne z zasadniczymi wymogami określonymi w sekcji 2 załącznika I postępowanie w przypadku wykrycia podatności.

   Producenci muszą posiadać odpowiednią politykę i stosowne procedury, w tym politykę regulującą skoordynowane ujawnianie podatności, o której mowa w sekcji 2 pkt 5 załącznika I, do celów przetwarzania i eliminowania potencjalnych podatności produktu z elementami cyfrowymi, zgłoszonych przez źródła wewnętrzne lub zewnętrzne.

7. Przed wprowadzeniem produktu z elementami cyfrowymi do obrotu producenci sporządzają dokumentację techniczną, o której mowa w art. 23.

Producenci przeprowadzają wybrane procedury oceny zgodności, o których mowa w art. 24, lub zlecają ich przeprowadzenie.

W przypadku wykazania zgodności produktu z elementami cyfrowymi z zasadniczymi wymogami określonymi w sekcji 1 załącznika I oraz zgodności procedur wprowadzonych przez producenta z zasadniczymi wymogami określonymi w sekcji 2 załącznika I w wyniku przeprowadzenia takiej procedury oceny zgodności producenci sporządzają deklarację zgodności UE zgodnie z art. 20 i umieszczają oznakowanie zgodności CE zgodnie z art. 22.

8. Producenci przechowują dokumentację techniczną i deklarację zgodności UE – w stosownych przypadkach – do dyspozycji organów nadzoru rynku przez okres dziesięciu lat po wprowadzeniu produktu z elementami cyfrowymi do obrotu.

9. Producenci zapewniają wprowadzenie procedur mających na celu utrzymanie zgodności produktów z elementami cyfrowymi, które są częścią serii produkcyjnej. Producent odpowiednio uwzględnia zmiany w procesie rozwoju i produkcji lub w projekcie lub właściwościach produktu z elementami cyfrowymi oraz zmiany w normach zharmonizowanych, europejskich programach certyfikacji cyberbezpieczeństwa lub wspólnych specyfikacjach, o których mowa w art. 19, w odniesieniu do których deklaruje się zgodność produktu z elementami cyfrowymi lub przez stosowanie których weryfikuje się jego zgodność.

10. Producenci zapewniają, aby do produktów z elementami cyfrowymi dołączano informacje i instrukcje określone w załączniku II, w postaci elektronicznej lub fizycznej. Takie informacje i instrukcje podaje się w języku łatwo zrozumiałym dla użytkowników. Muszą być one jasne, zrozumiałe, przystępne i czytelne. Umożliwiają one bezpieczną instalację, obsługę i bezpieczne użytkowanie produktów z elementami cyfrowymi.

11. Producenci dołączają do produktu z elementami cyfrowymi deklarację zgodności UE albo umieszczają w instrukcjach oraz informacjach określonych w załączniku II adres strony internetowej, na której jest dostępna deklaracja zgodności UE.

12. Od chwili wprowadzenia do obrotu i przez cały oczekiwany okres eksploatacji produktu lub przez okres pięciu lat po wprowadzeniu do obrotu produktu z elementami cyfrowymi, w zależności od tego, który z tych okresów jest krótszy, producenci, którzy wiedzą lub mają powody, by sądzić, że produkt z elementami cyfrowymi lub procedury wprowadzone przez producenta nie są zgodne z zasadniczymi wymogami określonymi w załączniku I, niezwłocznie wprowadzają środki naprawcze niezbędne do zapewnienia zgodności tego produktu z elementami cyfrowymi lub procedur producenta, do wycofania produktu z obrotu lub odzyskania go, w stosownych przypadkach.

13. Na uzasadniony wniosek organu nadzoru rynku producenci przekazują temu organowi, w łatwo zrozumiałym dla niego języku, wszelkie informacje i dokumentację – w formie papierowej lub elektronicznej – niezbędne do wykazania zgodności produktu z elementami cyfrowymi i procedur wprowadzonych przez producenta z zasadniczymi wymogami określonymi w załączniku I. Na żądanie tego organu współpracują z nim w zakresie wszelkich środków wprowadzonych w celu wyeliminowania ryzyka w cyberprzestrzeni, jakie stwarza produkt z elementami cyfrowymi wprowadzony przez nich do obrotu.

14. Producent, który zaprzestaje działalności i w rezultacie nie jest w stanie spełnić obowiązków ustanowionych w niniejszym rozporządzeniu, informuje o tej sytuacji

przed zaprzestaniem działalności odpowiednie organy nadzoru rynku, a także, za pomocą wszelkich dostępnych środków i w możliwie jak najszerszym zakresie, użytkowników odnośnych produktów z elementami cyfrowymi wprowadzonych do obrotu.

15. Komisja może w drodze aktów wykonawczych określić format i elementy zestawienia podstawowych materiałów do produkcji oprogramowania określonego w sekcji 2 pkt 1 załącznika I. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 51 ust. 2.

Artykuł 11

Obowiązki producentów w zakresie zgłaszania incydentów

1. Producent bez zbędnej zwłoki, a w każdym razie w terminie 24 godzin od uzyskania informacji o jakiejkolwiek aktywnie wykorzystywanej podatności zawartej w produkcie z elementami cyfrowymi zgłasza taką podatność ENISA. W zgłoszeniu tym podaje się szczegóły dotyczące tej podatności oraz, w stosownych przypadkach, wszelkie wprowadzone środki naprawcze lub łagodzące. Po otrzymaniu zgłoszenia ENISA bez zbędnej zwłoki, chyba że opóźnienie wynika z uzasadnionych przyczyn związanych z ryzykiem w cyberprzestrzeni, przekazuje je do CSIRT wyznaczonego do celów skoordynowanego ujawniania podatności w zainteresowanym państwie członkowskim zgodnie z art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)], a także informuje organ nadzoru rynku o zgłoszonej podatności.

2. Producent bez zbędnej zwłoki, a w każdym razie w terminie 24 godzin od uzyskania informacji o jakimkolwiek incydencie mającym wpływ na bezpieczeństwo produktu z elementami cyfrowymi zgłasza taki incydent ENISA. ENISA bez zbędnej zwłoki, chyba że opóźnienie wynika z uzasadnionych przyczyn związanych z ryzykiem w cyberprzestrzeni, przekazuje zgłoszenia do pojedynczego punktu kontaktowego wyznaczonego w zainteresowanym państwie członkowskim zgodnie z art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)], a także informuje organ nadzoru rynku o zgłoszonych incydentach. W zgłoszeniu incydentu należy zawrzeć informacje na temat dotkliwości i wpływu incydentu oraz, w stosownych przypadkach, wskazać, czy producent podejrzewa, że incydent jest spowodowany działaniami niezgodnymi z prawem lub czynami dokonanymi w złym zamiarze, lub uważa, że ma on wpływ transgraniczny.

3. ENISA przekazuje europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) ustanowionej na mocy art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)] informacje zgłoszone zgodnie z ust. 1 i 2, jeżeli takie informacje są istotne z perspektywy skoordynowanego zarządzania cyberincydentami i cyberkryzysami na dużą skalę na szczeblu operacyjnym.

4. Po powzięciu informacji o wystąpieniu incydentu producent bez zbędnej zwłoki informuje użytkowników produktu z elementami cyfrowymi o takim incydencie oraz, w razie potrzeby, o środkach naprawczych, które użytkownik może wdrożyć w celu złagodzenia skutków incydentu.

5. Komisja może, w drodze aktów wykonawczych, doprecyzować rodzaj informacji przekazywanych w zgłoszeniach składanych na podstawie ust. 1 i 2, format takich zgłoszeń i procedurę ich składania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 51 ust. 2.

6. ENISA, na podstawie powiadomień otrzymywanych zgodnie z ust. 1 i 2, przygotowuje co dwa lata sprawozdanie techniczne na temat pojawiających się tendencji w zakresie ryzyka w cyberprzestrzeni dotyczącego produktów z elementami cyfrowymi oraz przedkłada je grupie współpracy, o której mowa w art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)]. Pierwsze takie sprawozdanie należy przedłożyć w terminie 24 miesięcy od rozpoczęcia stosowania obowiązków określonych w ust. 1 i 2.

7. Producenci po zidentyfikowaniu podatności w komponencie, w tym w komponencie ze źródeł otwartych, który jest zintegrowany z produktem z elementami cyfrowymi, zgłaszają podatność osobie lub podmiotowi utrzymującemu komponent.

Artykuł 12

Upoważnieni przedstawiciele

1. Producent może wyznaczyć upoważnionego przedstawiciela w drodze pisemnego pełnomocnictwa.

2. Obowiązki określone w art. 10 ust. 1–6, art. 10 ust. 7 tiret pierwsze i art. 10 ust. 9 nie wchodzą w zakres pełnomocnictwa upoważnionego przedstawiciela.

3. Upoważniony przedstawiciel wykonuje zadania określone w pełnomocnictwie otrzymanym od producenta. Pełnomocnictwo umożliwia upoważnionemu przedstawicielowi wykonywanie co najmniej następujących obowiązków:

   a) przechowywanie deklaracji zgodności UE, o której mowa w art. 20, oraz dokumentacji technicznej, o której mowa w art. 23, do dyspozycji organów nadzoru rynku przez okres dziesięciu lat po wprowadzeniu produktu z elementami cyfrowymi do obrotu;

   b) przekazywanie na uzasadniony wniosek organu nadzoru rynku wszelkich informacji i dokumentów niezbędnych do wykazania zgodności produktu z elementami cyfrowymi z wymogami;

   c) na wniosek organów nadzoru rynku podejmowanie z nimi współpracy w działaniach mających na celu na wyeliminowanie ryzyka, jakie stwarza produkt z elementami cyfrowymi objęty pełnomocnictwem upoważnionego przedstawiciela.

Artykuł 13

Obowiązki importerów

1. Importerzy wprowadzają do obrotu wyłącznie produkty z elementami cyfrowymi, które spełniają zasadnicze wymogi określone w sekcji 1 załącznika I i w przypadku których procedury wprowadzone przez producenta są zgodne z zasadniczymi wymogami określonymi w sekcji 2 załącznika I.

2. Przed wprowadzeniem produktu z elementami cyfrowymi do obrotu importerzy zapewniają, aby:

   a) producent przeprowadził odpowiednie procedury oceny zgodności, o których mowa w art. 24;

   b) producent sporządził dokumentację techniczną;

c) produkt z elementami cyfrowymi nosił oznakowanie CE, o którym mowa w art. 22, oraz by towarzyszyły mu informacje i instrukcje obsługi określone w załączniku II.

3. W przypadku gdy importer uznaje lub ma powody, by uważać, że produkt z elementami cyfrowymi lub procedury wprowadzone przez producenta nie są zgodne z zasadniczymi wymogami określonymi w załączniku I, nie wprowadza produktu do obrotu, dopóki nie zostanie zapewniona zgodność tego produktu lub tych procedur wprowadzonych przez producenta z zasadniczymi wymogami określonymi w załączniku I. Ponadto, jeżeli produkt z elementami cyfrowymi stwarza znaczne ryzyko w cyberprzestrzeni, importer informuje o tym producenta oraz organy nadzoru rynku.

4. Importerzy umieszczają na produkcie z elementami cyfrowymi albo – jeżeli nie jest to możliwe – na opakowaniu produktu z elementami cyfrowymi lub w załączonym do niego dokumencie swoje imię i nazwisko lub nazwę, zarejestrowaną nazwę handlową lub zarejestrowany znak towarowy, adres pocztowy i adres e-mail, pod którym można się z nimi skontaktować. Dane kontaktowe podaje się w języku łatwo zrozumiałym dla użytkowników i organów nadzoru rynku.

5. Importerzy zapewniają dołączenie do produktu z elementami cyfrowymi instrukcji obsługi oraz dostarczenie informacji określonych w załączniku II w języku łatwo zrozumiałym dla użytkowników.

6. Importerzy, którzy wiedzą lub mają powody, by uważać, że wprowadzony przez nich na rynek produkt z elementami cyfrowymi lub procedury wprowadzone przez producenta nie są zgodne z zasadniczymi wymogami określonymi w załączniku I, niezwłocznie wprowadzają środki naprawcze niezbędne do zapewnienia zgodności produktu z elementami cyfrowymi lub procedur wprowadzonych przez jego producenta z zasadniczymi wymogami określonymi w załączniku I lub do wycofania produktu z obrotu, lub odzyskania go, w stosownych przypadkach.

   Po stwierdzeniu podatności produktu z elementami cyfrowymi importerzy bez zbędnej zwłoki informują producenta o tej podatności. Ponadto, w przypadku gdy produkt z elementami cyfrowymi stwarza istotne ryzyko w cyberprzestrzeni, importerzy niezwłocznie informują o tym organy nadzoru rynku państw członkowskich, w których produkt z elementami cyfrowymi udostępniono na rynku, podając szczegółowe informacje, w szczególności na temat niezgodności oraz wszelkich wprowadzonych środków naprawczych.

7. Importerzy przechowują kopię deklaracji zgodności UE do dyspozycji organów nadzoru rynku przez dziesięć lat po wprowadzeniu produktu z elementami cyfrowymi do obrotu i na wniosek tych organów udostępniają im dokumentację techniczną.

8. Na uzasadniony wniosek organu nadzoru rynku importerzy przekazują mu wszelkie informacje i dokumentację – w formie papierowej lub elektronicznej – niezbędne do wykazania zgodności produktu z elementami cyfrowymi z zasadniczymi wymogami określonymi w sekcji 1 załącznika I, a także zgodności procedur wprowadzonych przez producenta z zasadniczymi wymogami określonymi w sekcji 2 załącznika I w języku łatwo zrozumiałym dla tego organu. Na wniosek tego organu importerzy współpracują z nim w zakresie wszelkich środków wprowadzonych w celu usunięcia ryzyka w cyberprzestrzeni, jakie stwarza produkt z elementami cyfrowymi wprowadzony przez nich do obrotu.

9. W przypadku gdy importer produktu z elementami cyfrowymi dowiaduje się, że producent tego produktu zaprzestał działalności i w związku z tym nie jest w stanie wypełnić obowiązków określonych w niniejszym rozporządzeniu, importer informuje o tej sytuacji odpowiednie organy nadzoru rynku, a także, za pomocą wszelkich dostępnych środków i w możliwie jak najszerszym zakresie, użytkowników produktów z elementami cyfrowymi wprowadzonych do obrotu.

Artykuł 14

Obowiązki dystrybutorów

1. Udostępniając produkt z elementami cyfrowymi na rynku, dystrybutorzy działają z należytą starannością w odniesieniu do wymogów niniejszego rozporządzenia.

2. Przed udostępnieniem produktu z elementami cyfrowymi na rynku dystrybutorzy sprawdzają, czy:

   a) produkt z elementami cyfrowymi jest opatrzony oznakowaniem CE;

   b) producent i importer wypełnili obowiązki określone odpowiednio w art. 10 ust. 10 i 11 oraz w art. 13 ust. 4.

3. W przypadku gdy dystrybutor uznaje lub ma powody, by uważać, że produkt z elementami cyfrowymi lub procedury wprowadzone przez producenta nie są zgodne z zasadniczymi wymogami określonymi w załączniku I, nie udostępnia on produktu z elementami cyfrowymi na rynku, dopóki nie zostanie zapewniona zgodność tego produktu lub tych procedur wprowadzonych przez producenta. Ponadto, jeżeli produkt z elementami cyfrowymi stwarza istotne ryzyko w cyberprzestrzeni, dystrybutor informuje o tym producenta oraz organy nadzoru rynku.

4. Dystrybutorzy, którzy wiedzą lub mają powody, by uważać, że udostępniony przez nich na rynku produkt z elementami cyfrowymi lub procedury wprowadzone przez producenta nie są zgodne z zasadniczymi wymogami określonymi w załączniku I, zapewniają wprowadzenie środków naprawczych niezbędnych do zapewnienia zgodności produktu z elementami cyfrowymi lub procedur wprowadzonych przez producenta lub do wycofania produktu z obrotu, lub odzyskania go, w stosownych przypadkach.

   Po stwierdzeniu podatności produktu z elementami cyfrowymi dystrybutorzy bez zbędnej zwłoki informują producenta o tej podatności. Ponadto, w przypadku gdy produkt z elementami cyfrowymi stwarza istotne ryzyko w cyberprzestrzeni, dystrybutorzy niezwłocznie informują o tym organy nadzoru rynku państw członkowskich, w których produkt z elementami cyfrowymi udostępniono na rynku, podając szczegółowe informacje, w szczególności na temat niezgodności oraz wszelkich wprowadzonych środków naprawczych.

5. Na uzasadniony wniosek organu nadzoru rynku dystrybutorzy przekazują mu wszelkie informacje i dokumentację – w formie papierowej lub elektronicznej – niezbędne do wykazania zgodności produktu z elementami cyfrowymi i procedur wprowadzonych przez jego producenta z zasadniczymi wymogami określonymi w załączniku I w języku łatwo zrozumiałym dla tego organu. Na wniosek tego organu dystrybutorzy współpracują z nim w zakresie wszelkich środków wprowadzonych w celu usunięcia ryzyka w cyberprzestrzeni, jakie stwarza produkt z elementami cyfrowymi udostępniony przez nich na rynku.

6. W przypadku gdy dystrybutor produktu z elementami cyfrowymi dowiaduje się, że producent tego produktu zaprzestał działalności i w związku z tym nie jest w stanie wypełnić obowiązków określonych w niniejszym rozporządzeniu, dystrybutor informuje o tej sytuacji odpowiednie organy nadzoru rynku, a także, za pomocą wszelkich dostępnych środków i w możliwie jak najszerszym zakresie, użytkowników produktów z elementami cyfrowymi wprowadzonych do obrotu.

Artykuł 15

Przypadki, w których obowiązki producentów mają zastosowanie do importerów i dystrybutorów

Importer lub dystrybutor uważany jest za producenta do celów niniejszego rozporządzenia i podlega on obowiązkom producenta określonym w art. 10 oraz art. 11 ust. 1, 2, 4 i 7, jeżeli ten importer lub dystrybutor wprowadza produkt z elementami cyfrowymi do obrotu pod własną nazwą lub znakiem towarowym albo dokonuje istotnej modyfikacji produktu z elementami cyfrowymi już wprowadzonego do obrotu.

Artykuł 16

Inne przypadki, w których mają zastosowanie obowiązki producentów

Osoba fizyczna lub prawna – inna niż producent, importer lub dystrybutor – która dokonuje istotnej modyfikacji produktu z elementami cyfrowymi, uważana jest za producenta do celów niniejszego rozporządzenia.

Osoba ta podlega obowiązkom producenta określonym w art. 10 oraz art. 11 ust. 1, 2, 4 i 7 w odniesieniu do części produktu poddanej istotnej modyfikacji lub, jeżeli taka istotna modyfikacja ma wpływ na cyberbezpieczeństwo produktu z elementami cyfrowymi jako całości, w odniesieniu do całego produktu.

Artykuł 17

Identyfikacja podmiotów gospodarczych

1. Na wniosek organów nadzoru rynku i pod warunkiem, że informacje są dostępne, podmioty gospodarcze przekazują tym organom następujące informacje:

   a) imię i nazwisko lub nazwę i adres każdego podmiotu gospodarczego, który dostarczył im produkt z elementami cyfrowymi;

   b) imię i nazwisko lub nazwę i adres każdego podmiotu gospodarczego, któremu dostarczyły produkt z elementami cyfrowymi.

2. Podmioty gospodarcze muszą być w stanie przedstawić informacje, o których mowa w ust. 1, przez dziesięć lat od dostarczenia im produktu z elementami cyfrowymi oraz przez dziesięć lat od dostarczenia przez nie produktu z elementami cyfrowymi.

ROZDZIAŁ III

ZGODNOŚĆ PRODUKTU Z ELEMENTAMI CYFROWYMI

Artykuł 18

Domniemanie zgodności

1. W przypadku produktów z elementami cyfrowymi i procedur wprowadzonych przez producenta spełniających normy zharmonizowane lub części norm zharmonizowanych, do których odniesienie opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, zakłada się, że spełniają one zasadnicze wymogi objęte tymi normami lub ich częściami, określone w załączniku I.

2. Produkty z elementami cyfrowymi i procedury wprowadzone przez producenta zgodne ze wspólnymi specyfikacjami, o których mowa w art. 19, uznaje się za spełniające zasadnicze wymogi określone w załączniku I w zakresie, w jakim wspomniane wspólne specyfikacje obejmują te wymogi.

3. Zakłada się, że produkty z elementami cyfrowymi i procedury wprowadzone przez producenta, w odniesieniu do których wydano unijną deklarację zgodności lub certyfikat w ramach europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego zgodnie z rozporządzeniem (UE) 2019/881 i określonego zgodnie z ust. 4, są zgodne z zasadniczymi wymogami określonymi w załączniku I w zakresie, w jakim unijna deklaracja zgodności lub certyfikat cyberbezpieczeństwa, lub ich części, obejmują te wymogi.

4. Komisja jest uprawniona do określenia, w drodze aktów wykonawczych, europejskich programów certyfikacji cyberbezpieczeństwa przyjętych na podstawie rozporządzenia (UE) 2019/881, które mogą być stosowane do wykazania zgodności z zasadniczymi wymogami lub ich częściami określonymi w załączniku I. Ponadto, w stosownych przypadkach, Komisja określa, czy certyfikat cyberbezpieczeństwa wydany w ramach takich programów zwalnia producenta z obowiązku przeprowadzenia oceny zgodności przez stronę trzecią w odniesieniu do odpowiednich wymogów, jak określono w art. 24 ust. 2 lit. a) i b) oraz w art. 24 ust. 3 lit. a) i b). Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 51 ust. 2.

Artykuł 19

Wspólne specyfikacje

Jeżeli normy zharmonizowane, o których mowa w art. 18, nie istnieją lub jeżeli Komisja uzna, że odpowiednie normy zharmonizowane są niewystarczające do spełnienia wymogów niniejszego rozporządzenia lub zastosowania się do wniosku Komisji o normalizację lub jeżeli występują nieuzasadnione opóźnienia w procedurze normalizacji, lub jeżeli wniosek Komisji w sprawie norm zharmonizowanych nie zostanie zaakceptowany przez europejskie organizacje normalizacyjne, Komisja jest uprawniona do przyjmowania – w drodze aktów wykonawczych – wspólnych specyfikacji w odniesieniu do zasadniczych wymogów określonych w załączniku I. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 51 ust. 2.

Artykuł 20

Deklaracja zgodności UE

1. Deklarację zgodności UE sporządzają producenci zgodnie z art. 10 ust. 7 i potwierdza się w niej, że wykazano spełnienie mających zastosowanie zasadniczych wymogów określonych w załączniku I.

2. Deklarację zgodności UE sporządza się według wzoru określonego w załączniku IV i zawiera ona elementy wyszczególnione w odpowiednich procedurach oceny

zgodności określonych w załączniku VI. Taka deklaracja jest stale aktualizowana. Deklarację udostępnia się w języku lub językach wymaganych przez państwo członkowskie, w którym produkt z elementami cyfrowymi jest wprowadzany do obrotu lub udostępniany.

3. W przypadku gdy produkt z elementami cyfrowymi podlega więcej niż jednemu aktowi Unii wymagającemu deklaracji zgodności UE, sporządzana jest jedna deklaracja zgodności UE odnosząca się do wszystkich takich aktów Unii. W takiej deklaracji wskazuje się odpowiednie akty Unii, łącznie z ich adresami publikacyjnymi.

4. Przez sporządzenie deklaracji zgodności UE producent przyjmuje na siebie odpowiedzialność za zgodność produktu.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 50 w celu uzupełnienia niniejszego rozporządzenia przez dodanie elementów do minimalnego zakresu treści deklaracji zgodności UE określonego w załączniku IV, aby uwzględnić rozwój technologiczny.

Artykuł 21

Ogólne zasady dotyczące oznakowania CE

Oznakowanie CE zdefiniowane w art. 3 pkt 32 podlega ogólnym zasadom określonym w art. 30 rozporządzenia (WE) nr 765/2008.

Artykuł 22

Reguły i warunki dotyczące umieszczania oznakowania CE

1. Oznakowanie CE umieszcza się na produkcie z elementami cyfrowymi w sposób widoczny, czytelny i trwały. W przypadku gdy jest to niemożliwe lub nieuzasadnione ze względu na charakter produktu z elementami cyfrowymi, oznakowanie CE umieszcza się na opakowaniu i deklaracji zgodności UE, o której mowa w art. 20, dołączonej do produktu z elementami cyfrowymi. W przypadku produktów z elementami cyfrowymi w formie oprogramowania oznakowanie CE umieszcza się na deklaracji zgodności UE, o której mowa w art. 20, albo na stronie internetowej poświęconej oprogramowaniu.

2. Ze względu na charakter produktu z elementami cyfrowymi wysokość oznakowania CE umieszczonego na produkcie z elementami cyfrowymi może być mniejsza niż 5 mm, pod warunkiem że pozostaje ono widoczne i czytelne.

3. Oznakowanie CE umieszcza się przed wprowadzeniem produktu z elementami cyfrowymi do obrotu. Po oznakowaniu CE można umieścić piktogram lub innego rodzaju oznakowanie wskazujące na szczególne ryzyko lub zastosowanie określone w aktach wykonawczych, o których mowa w ust. 6.

4. Po oznakowaniu CE podaje się numer identyfikacyjny jednostki notyfikowanej, jeżeli jednostka ta jest zaangażowana w procedurę oceny zgodności opartą na pełnym zapewnieniu jakości (zgodnie z modułem H), o której mowa w art. 24.

Numer identyfikacyjny jednostki notyfikowanej umieszcza sama jednostka lub producent albo jego upoważniony przedstawiciel według wskazówek jednostki notyfikowanej.

5. Państwa członkowskie korzystają z istniejących mechanizmów, aby zapewnić prawidłowe stosowanie systemu oznakowania CE, oraz podejmują odpowiednie działania w przypadku jego niewłaściwego wykorzystania. W przypadku gdy produkt z elementami cyfrowymi podlega innym przepisom Unii, w których również przewiduje się umieszczenie oznakowania CE, oznakowanie to wskazuje, że produkt spełnia również wymogi określone w tych innych przepisach.

6. Komisja może – w drodze aktów wykonawczych – ustanowić specyfikacje techniczne piktogramów lub wszelkich innych oznakowań związanych z bezpieczeństwem produktów z elementami cyfrowymi oraz mechanizmy zachęcające do ich stosowania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 51 ust. 2.

Artykuł 23

Dokumentacja techniczna

1. Dokumentacja techniczna zawiera wszelkie istotne dane lub informacje szczegółowe dotyczące środków zastosowanych przez producenta w celu zapewnienia, aby produkt z elementami cyfrowymi oraz procedury wprowadzone przez producenta spełniały zasadnicze wymogi określone w załączniku I. Zawiera ona co najmniej elementy określone w załączniku V.

2. Dokumentację techniczną sporządza się przed wprowadzeniem do obrotu produktu z elementami cyfrowymi i – w razie potrzeby – jest ona stale aktualizowana podczas przewidywanego okresu eksploatacji produktu lub w okresie pięciu lat od wprowadzenia do obrotu produktu z elementami cyfrowymi, w zależności od tego, który z tych okresów jest krótszy.

3. W przypadku produktów z elementami cyfrowymi, o których mowa w art. 8 i art. 24 ust. 4, podlegających również innym aktom Unii, sporządza się jedną dokumentację techniczną zawierającą informacje, o których mowa w załączniku V do niniejszego rozporządzenia, oraz informacje wymagane w tych odpowiednich aktach Unii.

4. Dokumentację techniczną i korespondencję odnoszącą się do procedury oceny zgodności sporządza się w języku urzędowym państwa członkowskiego, w którym ustanowiona jest jednostka notyfikowana, lub w języku możliwym do przyjęcia przez tę jednostkę.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 50 w celu uzupełnienia niniejszego rozporządzenia o elementy, które należy włączyć do dokumentacji technicznej określonej w załączniku V, aby uwzględnić rozwój technologiczny, jak również o zmiany napotkane w procesie wdrażania niniejszego rozporządzenia.

Artykuł 24

Procedury oceny zgodności dotyczące produktów z elementami cyfrowymi

1. Producent dokonuje oceny zgodności produktu z elementami cyfrowymi i procedur wprowadzonych przez producenta w celu ustalenia, czy spełniono zasadnicze wymogi określone w załączniku I. Producent lub upoważniony przedstawiciel producenta wykazuje zgodność z zasadniczymi wymogami, stosując jedną z następujących procedur:

a) procedurę kontroli wewnętrznej (zgodnie z modułem A) określoną w załączniku VI; lub

b) procedurę badania typu UE (zgodnie z modułem B) określoną w załączniku VI, po której następuje badanie zgodności z typem UE w oparciu o wewnętrzną kontrolę produkcji (zgodnie z modułem C) określoną w załączniku VI; lub

c) ocenę zgodności opartą na pełnym zapewnieniu jakości (zgodnie z modułem H) określoną w załączniku VI.

2. Jeżeli przy ocenie zgodności produktu krytycznego z elementami cyfrowymi klasy I określonego w załączniku III oraz procedur wprowadzonych przez jego producenta z zasadniczymi wymogami określonymi w załączniku I producent lub upoważniony przedstawiciel producenta nie zastosował norm zharmonizowanych, wspólnych specyfikacji lub europejskich programów certyfikacji cyberbezpieczeństwa, o których mowa w art. 18, lub zastosował je tylko częściowo bądź jeżeli takie normy zharmonizowane, wspólne specyfikacje lub europejskie programy certyfikacji cyberbezpieczeństwa nie istnieją, dany produkt z elementami cyfrowymi i procedury wprowadzone przez producenta podlegają w odniesieniu do tych zasadniczych wymogów jednej z następujących procedur:

a) procedurze badania typu UE (zgodnie z modułem B) określonej w załączniku VI, po której następuje badanie zgodności z typem UE w oparciu o wewnętrzną kontrolę produkcji (zgodnie z modułem C) określoną w załączniku VI; lub

b) ocenie zgodności opartej na pełnym zapewnieniu jakości (zgodnie z modułem H) określonej w załączniku VI.

3. Jeżeli produkt jest produktem krytycznym z elementami cyfrowymi klasy II określonym w załączniku III, producent lub upoważniony przedstawiciel producenta wykazuje zgodność z zasadniczymi wymogami określonymi w załączniku I, stosując jedną z następujących procedur:

a) procedurę badania typu UE (zgodnie z modułem B) określoną w załączniku VI, po której następuje badanie zgodności z typem UE w oparciu o wewnętrzną kontrolę produkcji (zgodnie z modułem C) określoną w załączniku VI; lub

b) ocenę zgodności opartą na pełnym zapewnieniu jakości (zgodnie z modułem H) określoną w załączniku VI.

4. Producenci produktów z elementami cyfrowymi, które sklasyfikowano jako systemy elektronicznej dokumentacji medycznej wchodzące w zakres rozporządzenia [rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia], wykazują zgodność z zasadniczymi wymogami określonymi w załączniku I do niniejszego rozporządzenia, stosując odpowiednią procedurę oceny zgodności zgodnie z wymogami rozporządzenia [rozdziału III rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia].

5. Jednostki notyfikowane przy ustalaniu opłat za procedury oceny zgodności uwzględniają szczególne interesy i potrzeby małych i średnich przedsiębiorstw (MŚP) i obniżają te opłaty proporcjonalnie do ich szczególnych interesów i potrzeb.

ROZDZIAŁ IV

NOTYFIKACJA JEDNOSTEK OCENIAJĄCYCH ZGODNOŚĆ

Artykuł 25

Notyfikacja

Państwa członkowskie notyfikują Komisji i pozostałym państwom członkowskim jednostki oceniające zgodność uprawnione do dokonywania oceny zgodności zgodnie z niniejszym rozporządzeniem.

Artykuł 26

Organy notyfikujące

1. Państwa członkowskie wyznaczają organ notyfikujący, który odpowiada za opracowanie i przeprowadzanie procedur koniecznych do oceny i notyfikowania jednostek oceniających zgodność oraz do monitorowania jednostek notyfikowanych, w tym na potrzeby zapewnienia zgodności z art. 31.
2. Państwa członkowskie mogą zdecydować, że ocena i monitorowanie, o których mowa w ust. 1, są przeprowadzane przez krajową jednostkę akredytującą w rozumieniu przepisów rozporządzenia (WE) nr 765/2008 i zgodnie z tymi przepisami.

Artykuł 27

Wymogi dotyczące organów notyfikujących

1. Organ notyfikujący ustanawia się w taki sposób, by nie dochodziło do konfliktu interesów między organem notyfikującym a jednostkami oceniającymi zgodność.
2. Sposób organizacji i funkcjonowania organu notyfikującego musi gwarantować obiektywizm i bezstronność jego działalności.
3. Sposób organizacji organu notyfikującego musi zapewniać podejmowanie każdej decyzji dotyczącej notyfikacji jednostki oceniającej zgodność przez kompetentne osoby spoza grona osób przeprowadzających ocenę.
4. Organ notyfikujący nie może oferować ani podejmować żadnych działań wykonywanych przez jednostki oceniające zgodność ani świadczyć usług doradczych na zasadach komercyjnych lub konkurencyjnych.
5. Organ notyfikujący zapewnia poufność informacji, które otrzymuje.
6. Organ notyfikujący musi dysponować odpowiednią liczbą pracowników mających kompetencje do właściwego wykonywania jego zadań.

Artykuł 28

Obowiązki informacyjne organów notyfikujących

1. Państwa członkowskie informują Komisję o swoich procedurach oceny i notyfikacji jednostek oceniających zgodność oraz monitorowania jednostek notyfikowanych, jak również o wszelkich zmianach w tym zakresie.

2. Komisja podaje te informacje do wiadomości publicznej.

Artykuł 29

Wymogi dotyczące jednostek notyfikowanych

1. Na potrzeby notyfikacji jednostka oceniająca zgodność musi spełnić wymogi określone w ust. 2–12.

2. Jednostka oceniająca zgodność jest powoływana na podstawie prawa krajowego i posiada osobowość prawną.

3. Jednostka oceniająca zgodność musi być osobą trzecią, funkcjonującą niezależnie od organizacji lub produktu, który ocenia.

   Jednostkę należącą do stowarzyszenia przedsiębiorców lub zrzeszenia zawodowego reprezentującego przedsiębiorstwa zaangażowane w projektowanie, opracowywanie, produkcję, dostarczanie, montowanie, użytkowanie lub konserwację produktów z elementami cyfrowymi, które ocenia, można uważać za taką jednostkę, pod warunkiem że wykazano jej niezależność i brak konfliktu interesów.

4. Jednostka oceniająca zgodność, jej kierownictwo najwyższego szczebla oraz pracownicy odpowiedzialni za realizację zadań związanych z oceną zgodności nie mogą być projektantami, twórcami, producentami, dostawcami, instalatorami, nabywcami, właścicielami, użytkownikami czy konserwatorami produktów z elementami cyfrowymi, które oceniają, ani upoważnionymi przedstawicielami wymienionych stron. Nie wyklucza to używania ocenianych produktów, które są niezbędne do prowadzenia działalności jednostki oceniającej zgodność, ani używania produktów do celów prywatnych.

   Jednostki oceniające zgodność, jej kierownictwo najwyższego szczebla oraz pracownicy odpowiedzialni za realizację zadań związanych z oceną zgodności nie angażują się bezpośrednio w projektowanie, opracowywanie, produkcję, wprowadzanie do obrotu, instalację, użytkowanie lub konserwację tych produktów ani nie reprezentują stron zaangażowanych w taką działalność. Nie mogą oni angażować się w działalność, która może zagrażać niezależności ich osądów lub wiarygodności w odniesieniu do działań związanych z oceną zgodności będących przedmiotem notyfikacji. Dotyczy to w szczególności usług doradczych.

   Jednostki oceniające zgodność zapewniają, aby działalność ich jednostek zależnych lub podwykonawców nie wpływała na poufność, obiektywizm ani bezstronność ich działalności związanej z oceną zgodności.

5. Jednostki oceniające zgodność i ich pracownicy muszą spełniać w toku realizacji działalności związanej z oceną zgodności najwyższe standardy zawodowe, posiadać konieczne kwalifikacje techniczne w danej dziedzinie oraz nie mogą być poddawani żadnym naciskom ani zachętom, zwłaszcza finansowym, mogącym wpływać na ich osąd lub wyniki działalności związanej z oceną zgodności, w szczególności ze strony osób lub grup osób, których interesy związane są z rezultatami tej działalności.

6. Jednostka oceniająca zgodność musi być zdolna do realizacji wszystkich zadań związanych z oceną zgodności, o których mowa w załączniku VI i w odniesieniu do których została notyfikowana, niezależnie od tego, czy dana jednostka oceniająca zgodność wykonuje te zadania samodzielnie, czy są one wykonywane w jej imieniu i na jej odpowiedzialność.

Przez cały czas i w odniesieniu do dowolnej procedury oceny zgodności oraz dowolnego rodzaju lub kategorii produktów z elementami cyfrowymi będących przedmiotem notyfikacji dana jednostka oceniająca zgodność musi dysponować niezbędnymi:

a) pracownikami mającymi wiedzę techniczną oraz wystarczające i odpowiednie doświadczenie do realizacji zadań z zakresu oceny zgodności;

b) opisami procedur, zgodnie z którymi przeprowadza się ocenę zgodności, zapewniającymi przejrzystość i powtarzalność tych procedur. Jednostka musi posiadać odpowiednią politykę i stosowne procedury, dzięki którym możliwe jest odróżnienie zadań wykonywanych jako jednostka notyfikowana od pozostałych działań;

c) procedurami służącymi wykonywaniu działań z należytym uwzględnieniem wielkości przedsiębiorstwa, sektora jego działalności, struktury przedsiębiorstwa, stopnia złożoności technologii danego produktu oraz masowego lub seryjnego charakteru procesu produkcji.

Jednostka musi dysponować środkami niezbędnymi do prawidłowej realizacji zadań o charakterze technicznym i administracyjnym z zakresu oceny zgodności oraz mieć dostęp do wszelkiego niezbędnego wyposażenia lub wszelkich niezbędnych obiektów.

7. Pracownicy odpowiedzialni za realizację działań związanych z oceną zgodności muszą mieć:

a) gruntowne przeszkolenie zawodowe i techniczne, obejmujące wszystkie działania związane z oceną zgodności w zakresie będącym przedmiotem notyfikacji jednostki oceniającej zgodność;

b) dostateczną znajomość wymogów dotyczących ocen, które przeprowadzają, oraz odpowiednie uprawnienia do dokonywania takich ocen;

c) odpowiednią znajomość i zrozumienie zasadniczych wymogów, obowiązujących norm zharmonizowanych oraz stosownych przepisów unijnego prawodawstwa harmonizacyjnego i aktów wykonawczych;

d) umiejętności wymagane do sporządzania certyfikatów, zapisów i sprawozdań potwierdzających, że oceny zostały przeprowadzone.

8. Gwarantuje się bezstronność jednostek oceniających zgodność, ich kierownictwa najwyższego szczebla i pracowników przeprowadzających ocenę.

Wynagrodzenie kierownictwa najwyższego szczebla jednostki oceniającej zgodność oraz jej pracowników przeprowadzających ocenę nie może zależeć od liczby przeprowadzonych ocen ani od ich wyników.

9. Jednostki oceniające zgodność muszą wykupić ubezpieczenie od odpowiedzialności cywilnej, chyba że na mocy prawa krajowego odpowiedzialność spoczywa na państwie lub za ocenę zgodności bezpośrednio odpowiada samo państwo członkowskie.

10. Pracownicy jednostki oceniającej zgodność są zobowiązani dochować tajemnicy zawodowej w odniesieniu do wszystkich informacji, które uzyskują w trakcie wykonywania swoich zadań zgodnie z załącznikiem VI lub przepisami prawa krajowego w danym zakresie, z wyjątkiem dochowania tajemnicy wobec organów nadzoru rynku państwa członkowskiego, w którym realizowane są zadania. Prawa

własności podlegają ochronie. Jednostka oceniająca zgodność musi posiadać udokumentowane procedury zapewniające zgodność z niniejszym ustępem.

11. Jednostki oceniające zgodność biorą udział w stosownej działalności normalizacyjnej i w działalności grupy koordynującej jednostki notyfikowanej, powołanej na podstawie art. 40, lub zapewniają informowanie o takiej działalności swoich pracowników przeprowadzających oceny oraz traktują jak ogólne wytyczne decyzje administracyjne i dokumenty opracowane w wyniku prac takiej grupy.

12. Jednostki oceniające zgodność prowadzą działalność na spójnych, uczciwych i rozsądnych warunkach, w szczególności biorąc pod uwagę interesy MŚP w odniesieniu do opłat.

Artykuł 30

Domniemanie zgodności jednostek notyfikowanych

Jeżeli jednostka oceniająca zgodność wykaże, że spełnia kryteria ustanowione w odpowiednich normach zharmonizowanych – lub ich częściach – do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, jednostka ta spełnia wymogi określone w art. 29 na zasadzie domniemania, jeżeli mające zastosowanie normy zharmonizowane obejmują te wymogi.

Artykuł 31

Jednostki zależne i podwykonawcy jednostek notyfikowanych

1. W przypadku gdy jednostka notyfikowana zleca podwykonawstwo określonych zadań związanych z oceną zgodności lub korzysta z usług jednostki zależnej, zapewnia ona, aby podwykonawca lub jednostka zależna spełniali wymogi określone w art. 29, oraz odpowiednio informuje o tym organ notyfikujący.

2. Jednostki notyfikowane ponoszą pełną odpowiedzialność za zadania wykonywane przez podwykonawców lub jednostki zależne, niezależnie od tego, gdzie podwykonawcy lub jednostki zależne mają siedzibę.

3. Działania te można zlecać podwykonawcom lub powierzać do wykonania jednostce zależnej wyłącznie za zgodą producenta.

4. Jednostki notyfikowane przechowują do dyspozycji organu notyfikującego odpowiednie dokumenty dotyczące oceny kwalifikacji podwykonawcy lub jednostki zależnej oraz prac wykonywanych przez podwykonawcę lub jednostkę zależną zgodnie z niniejszym rozporządzeniem.

Artykuł 32

Wniosek o notyfikację

1. Jednostka oceniająca zgodność przedkłada wniosek o notyfikację organowi notyfikującemu państwa członkowskiego, w którym ma swoją siedzibę.

2. Do wniosku załącza się opis działań związanych z oceną zgodności, procedury lub procedur oceny zgodności oraz produktu lub produktów wchodzących w zakres kompetencji danej jednostki, jak również certyfikat akredytacji, jeżeli istnieje, wydany przez krajową jednostkę akredytującą, potwierdzający, że jednostka oceniająca zgodność spełnia wymogi określone w art. 29.

3. Jeżeli dana jednostka oceniająca zgodność nie może dostarczyć certyfikatu akredytacji, przedkłada ona organowi notyfikującemu wszystkie dowody w postaci dokumentów niezbędne do sprawdzenia, uznania i regularnego monitorowania jej zgodności z wymogami określonymi w art. 29.

Artykuł 33

Procedura notyfikacji

1. Organy notyfikujące mogą notyfikować wyłącznie te jednostki oceniające zgodność, które spełniają wymogi określone w art. 29.

2. Organ notyfikujący notyfikuje Komisję i pozostałe państwa członkowskie za pomocą systemu informacyjnego NANDO opracowanego i zarządzanego przez Komisję.

3. Do notyfikacji załącza się wszystkie szczegółowe informacje dotyczące działań związanych z oceną zgodności, modułu lub modułów oceny zgodności, produktu lub produktów, których to dotyczy, oraz stosowne poświadczenie kompetencji.

4. W przypadku gdy podstawy notyfikacji nie stanowi certyfikat akredytacji, o którym mowa w art. 32 ust. 2, organ notyfikujący przedkłada Komisji i pozostałym państwom członkowskim dowody w postaci dokumentów potwierdzających kompetencje jednostki oceniającej zgodność oraz przedstawia ustalenia wprowadzone, aby zapewnić systematyczne monitorowanie tej jednostki i dalsze spełnianie przez nią wymogów określonych w art. 29.

5. Dana jednostka może prowadzić działalność jednostki notyfikowanej wyłącznie pod warunkiem, że Komisja lub pozostałe państwa członkowskie nie zgłosiły zastrzeżeń w terminie dwóch tygodni od notyfikacji w przypadku korzystania z certyfikatu akredytacji lub w terminie dwóch miesięcy od notyfikacji w przypadku niekorzystania z akredytacji.

   Wyłącznie taką jednostkę uznaje się za jednostkę notyfikowaną do celów niniejszego rozporządzenia.

6. O wszelkich kolejnych zmianach w notyfikacji powiadamia się Komisję i pozostałe państwa członkowskie.

Artykuł 34

Numery identyfikacyjne i wykazy jednostek notyfikowanych

1. Komisja przydziela jednostce notyfikowanej numer identyfikacyjny.

   Komisja przydziela jeden numer identyfikacyjny, nawet w przypadku gdy jednostka jest notyfikowana na mocy różnych aktów Unii.

2. Komisja podaje do wiadomości publicznej wykaz jednostek notyfikowanych na podstawie niniejszego rozporządzenia, wraz z przydzielonymi im numerami identyfikacyjnymi oraz informacją na temat rodzaju działań, w odniesieniu do których zostały notyfikowane.

   Komisja zapewnia bieżącą aktualizację tego wykazu.

Artykuł 35

Zmiany w notyfikacji

1. W przypadku gdy organ notyfikujący stwierdza lub otrzymuje informację, że jednostka notyfikowana przestała spełniać wymogi określone w art. 29 lub nie wykonuje swoich obowiązków, organ notyfikujący, odpowiednio, ogranicza, zawiesza lub cofa notyfikację, w zależności od powagi niespełnianych wymogów lub niewykonanych obowiązków. Niezwłocznie informuje o tym Komisję i pozostałe państwa członkowskie.

2. W przypadku ograniczenia, zawieszenia lub cofnięcia notyfikacji albo w przypadku zaprzestania działalności przez jednostkę notyfikowaną notyfikujące państwo członkowskie wdraża właściwe środki w celu zapewnienia, aby dokumentacją tej jednostki zajęła się inna jednostka notyfikowana lub aby była ona dostępna na żądanie odpowiedzialnych organów notyfikujących i organów nadzoru rynku.

Artykuł 36

Kwestionowanie kompetencji jednostek notyfikowanych

1. Komisja bada wszystkie przypadki, w których ma wątpliwości lub otrzymuje informacje o wątpliwościach co do kompetencji jednostki notyfikowanej lub dalszego spełniania wymogów, którym jednostka ta podlega, i wywiązywania się z nałożonych na nią obowiązków.

2. Na żądanie Komisji notyfikujące państwo członkowskie udziela jej wszelkich informacji dotyczących podstawy notyfikacji lub utrzymania kompetencji danej jednostki.

3. Komisja zapewnia poufne traktowanie wszystkich informacji szczególnie chronionych uzyskanych w trakcie prowadzonych postępowań wyjaśniających.

4. W przypadku gdy Komisja stwierdza, że jednostka notyfikowana nie spełnia wymogów notyfikacji lub przestała je spełniać, informuje o tym fakcie notyfikujące państwo członkowskie i zwraca się do niego o wprowadzenie koniecznych środków naprawczych, włącznie z wycofaniem notyfikacji, jeżeli zachodzi taka potrzeba.

Artykuł 37

Obowiązki operacyjne jednostek notyfikowanych

1. Jednostki notyfikowane przeprowadzają oceny zgodności zgodnie z procedurami oceny zgodności określonymi w art. 24 i załączniku VI.

2. Oceny zgodności przeprowadza się w sposób proporcjonalny, unikając przy tym zbędnych obciążeń dla podmiotów gospodarczych. Jednostki oceniające zgodność wykonują swoje działania, uwzględniając wielkość przedsiębiorstwa, sektora, w którym ono działa, strukturę przedsiębiorstwa, stopień złożoności technologii danego produktu oraz masowy lub seryjny charakter procesu produkcji.

3. Jednostki notyfikowane zachowują jednak odpowiednią rygorystyczność i odpowiedni poziom ochrony wymagane dla zagwarantowania zgodności produktu z przepisami rozporządzenia.

4. Jeżeli jednostka notyfikowana stwierdza, że producent nie spełnił wymogów określonych w załączniku I lub w odpowiednich normach zharmonizowanych czy wspólnych specyfikacjach, o których mowa w art. 19, zobowiązuje ona producenta do wprowadzenia stosownych środków naprawczych i nie wydaje mu certyfikatu zgodności.

5. W przypadku gdy w trakcie monitorowania zgodności po wydaniu certyfikatu jednostka notyfikowana stwierdza, że produkt przestał spełniać wymogi określone w niniejszym rozporządzeniu, zobowiązuje producenta do wprowadzenia stosownych środków naprawczych, a jeżeli zachodzi taka konieczność, zawiesza lub cofa dany certyfikat.

6. W przypadku niewprowadzenia środków naprawczych lub jeżeli środki te nie przynoszą wymaganych skutków, jednostka notyfikowana ogranicza, zawiesza lub cofa wszelkie certyfikaty, w stosownych przypadkach.

Artykuł 38

Obowiązki informacyjne jednostek notyfikowanych

1. Jednostki notyfikowane informują organ notyfikujący:

   a) o każdym przypadku odmowy wydania, ograniczenia, zawieszenia lub cofnięcia certyfikatu;

   b) o wszelkich okolicznościach, które mogą mieć negatywny wpływ na zakres i warunki notyfikacji;

   c) o każdym przypadku zażądania przez organ nadzoru rynku udzielenia informacji dotyczących działań związanych z oceną zgodności;

   d) na wniosek, o podejmowanych działaniach związanych z oceną zgodności wchodzących w zakres ich notyfikacji oraz o innych wykonywanych działaniach, w tym o działalności transgranicznej i podwykonawstwie.

2. Jednostki notyfikowane przekazują pozostałym jednostkom notyfikowanym na podstawie niniejszego rozporządzenia prowadzącym podobne działania związane z oceną zgodności i zajmującym się tymi samymi produktami odpowiednie informacje na temat kwestii, w przypadku których wyniki oceny zgodności były negatywne, a na wniosek, również tych, w przypadku których były one pozytywne.

Artykuł 39

Wymiana doświadczeń

Komisja organizuje wymianę doświadczeń między organami krajowymi państw członkowskich odpowiedzialnymi za strategię w zakresie notyfikacji.

Artykuł 40

Koordynacja jednostek notyfikowanych

1. Komisja zapewnia wprowadzenie i właściwą realizację odpowiedniej koordynacji i współpracy między jednostkami notyfikowanymi, w formie międzysektorowego zespołu jednostek notyfikowanych.

2. Państwa członkowskie zapewniają, aby notyfikowane przez nie jednostki uczestniczyły w pracach tego zespołu bezpośrednio lub za pośrednictwem wyznaczonych przedstawicieli.

ROZDZIAŁ V

NADZÓR RYNKU I EGZEKWOWANIE PRZEPISÓW

Artykuł 41

Nadzór rynku i kontrola produktów z elementami cyfrowymi na rynku Unii

1. W odniesieniu do produktów z elementami cyfrowymi objętych zakresem niniejszego rozporządzenia zastosowanie mają przepisy rozporządzenia (UE) 2019/1020.

2. Każde państwo członkowskie wyznacza co najmniej jeden organ nadzoru rynku do celów zapewnienia skutecznego wdrażania niniejszego rozporządzenia. Państwa członkowskie mogą wyznaczyć istniejący lub nowy organ, który będzie pełnił funkcję organu nadzoru rynku do celów niniejszego rozporządzenia.

3. W stosownych przypadkach organy nadzoru rynku współpracują z krajowymi organami ds. certyfikacji cyberbezpieczeństwa wyznaczonymi na podstawie art. 58 rozporządzenia (UE) 2019/881 i regularnie wymieniają informacje. Wyznaczone organy nadzoru rynku współpracują z ENISA w odniesieniu do nadzoru nad realizacją obowiązków w zakresie zgłaszania incydentów, o których mowa w art. 11 niniejszego rozporządzenia.

4. W stosownych przypadkach organy nadzoru rynku współpracują z innymi organami nadzoru rynku wyznaczonymi na podstawie innego unijnego prawodawstwa harmonizacyjnego dotyczącego innych produktów oraz regularnie wymieniają informacje.

5. W stosownych przypadkach organy nadzoru rynku współpracują z organami nadzorującymi egzekwowanie unijnych przepisów o ochronie danych. Taka współpraca obejmuje informowanie tych organów o wszelkich ustaleniach istotnych dla wykonywania zadań leżących w ich kompetencjach, w tym przy wydawaniu wskazówek i porad na podstawie ust. 8 niniejszego artykułu, jeżeli takie wskazówki i porady dotyczą przetwarzania danych osobowych.

   Organy nadzorujące egzekwowanie unijnych przepisów o ochronie danych są uprawnione do żądania dostępu do wszelkiej dokumentacji sporządzonej lub prowadzonej na podstawie niniejszego rozporządzenia, jeżeli dostęp do tej dokumentacji jest niezbędny do wykonywania ich zadań. Organy te informują wyznaczone organy nadzoru rynku danego państwa członkowskiego o każdym takim żądaniu.

6. Państwa członkowskie zapewniają, aby wyznaczone organy nadzoru rynku dysponowały odpowiednimi zasobami finansowymi i ludzkimi umożliwiającymi im wykonywanie zadań powierzonych im zgodnie z niniejszym rozporządzeniem.

7. Komisja sprzyja wymianie doświadczeń między wyznaczonymi organami nadzoru rynku.

8. Organy nadzoru rynku mogą udzielać podmiotom gospodarczym wskazówek i porad dotyczących wdrażania niniejszego rozporządzenia, przy wsparciu Komisji.

9. Organy nadzoru rynku przekazują Komisji coroczne sprawozdania dotyczące rezultatów stosownych działań w zakresie nadzoru rynku. Wyznaczone organy nadzoru rynku niezwłocznie przekazują Komisji i odpowiednim krajowym organom

ochrony konkurencji wszelkie informacje zgromadzone w trakcie podejmowania działań w zakresie nadzoru rynku, które mogą okazać się istotne z punku widzenia stosowania unijnego prawa konkurencji.

10. W przypadku produktów z elementami cyfrowymi objętych zakresem niniejszego rozporządzenia, zaklasyfikowanych jako systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. [art. 6] rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji], organy nadzoru rynku wyznaczone do celów rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji] są organami odpowiedzialnymi za działania w zakresie nadzoru rynku wymagane na podstawie niniejszego rozporządzenia. W stosownych przypadkach organy nadzoru rynku wyznaczone na podstawie rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji] współpracują z organami nadzoru rynku wyznaczonymi na podstawie niniejszego rozporządzenia oraz, w odniesieniu do sprawowania nadzoru nad wykonywaniem obowiązków w zakresie zgłaszania incydentów, o których mowa w art. 11, z ENISA. Organy nadzoru rynku wyznaczone na podstawie rozporządzenia [rozporządzenia w sprawie sztucznej inteligencji] informują w szczególności organy nadzoru rynku wyznaczone na podstawie niniejszego rozporządzenia o wszelkich ustaleniach istotnych dla realizacji ich zadań związanych z wdrożeniem niniejszego rozporządzenia.

11. Do celów jednolitego stosowania niniejszego rozporządzenia ustanawia się specjalną grupę współpracy administracyjnej (grupę ADCO), zgodnie z art. 30 ust. 2 rozporządzenia (UE) 2019/1020. W skład grupy ADCO wchodzą przedstawiciele wyznaczonych organów nadzoru rynku oraz, w razie potrzeby, przedstawiciele jednolitych urzędów łącznikowych.

Artykuł 42

Dostęp do danych i dokumentacji

Jeżeli jest to konieczne do oceny zgodności produktów z elementami cyfrowymi i procedur wprowadzonych przez ich producentów z zasadniczymi wymogami określonymi w załączniku I, a także na uzasadniony wniosek organom nadzoru rynku przyznaje się dostęp do danych niezbędnych do oceny projektu, procesu opracowywania, produkcji i postępowania w przypadku wykrycia podatności, w tym dostęp do powiązanej dokumentacji wewnętrznej dotyczącej danego podmiotu gospodarczego.

Artykuł 43

Procedura na szczeblu krajowym dotycząca produktów z elementami cyfrowymi stwarzających istotne ryzyko w cyberprzestrzeni

1. Jeżeli organ nadzoru rynku państwa członkowskiego ma wystarczające powody, aby uznać, że produkt z elementami cyfrowymi, w tym dotyczące go postępowanie w przypadku wykrycia podatności, stwarza istotne ryzyko w cyberprzestrzeni, organ przeprowadza ocenę tego produktu z elementami cyfrowymi pod kątem zgodności produktu ze wszystkimi wymogami określonymi w niniejszym rozporządzeniu. W razie potrzeby odpowiednie podmioty gospodarcze współpracują z danym organem nadzoru rynku.

   Jeżeli w trakcie tej oceny organ nadzoru rynku stwierdzi, że produkt z elementami cyfrowymi nie jest zgodny z wymogami określonymi w niniejszym rozporządzeniu, niezwłocznie zobowiązuje właściwy podmiot gospodarczy do podjęcia wszelkich

odpowiednich działań naprawczych w celu zapewnienia zgodności produktu z elementami cyfrowymi z tymi wymogami, wycofania go z obrotu lub odzyskania go w wyznaczonym przez organ rozsądnym terminie, stosownym do charakteru ryzyka.

Organ nadzoru rynku informuje o tym odpowiednią jednostkę notyfikowaną. Art. 18 rozporządzenia (UE) 2019/1020 ma zastosowanie do odpowiednich działań naprawczych.

2. W przypadku gdy organ nadzoru rynku uzna, że niezgodność z wymogami nie ogranicza się do jego terytorium krajowego, informuje Komisję oraz pozostałe państwa członkowskie o wynikach oceny oraz o działaniach, których podjęcia zażądał od danego podmiotu gospodarczego.

3. Producent zapewnia podjęcie wszelkich odpowiednich działań naprawczych w odniesieniu do wszystkich odnośnych produktów z elementami cyfrowymi, które udostępnił na rynku w całej Unii.

4. W przypadku niepodjęcia przez producenta produktu z elementami cyfrowymi odpowiednich działań naprawczych w terminie, o którym mowa w ust. 1 akapit drugi, organ nadzoru rynku wprowadza wszelkie odpowiednie środki tymczasowe w celu zakazania lub ograniczenia udostępniania tego produktu na rynku krajowym, wycofania produktu z obrotu lub odzyskania go.

   Organ ten niezwłocznie informuje Komisję i pozostałe państwa członkowskie o tych środkach.

5. Informacje, o których mowa w ust. 4, obejmują wszelkie dostępne informacje szczegółowe, w szczególności dane niezbędne do identyfikacji niezgodnego z przepisami produktu z elementami cyfrowymi, pochodzenie produktu z elementami cyfrowymi, charakter domniemanej niezgodności i związanego z nią ryzyka, charakter i okres obowiązywania wprowadzonych środków krajowych oraz argumenty przedstawione przez właściwy podmiot gospodarczy. W szczególności organ nadzoru rynku wskazuje, czy niezgodność wynika z co najmniej jednej z następujących przyczyn:

   a) niespełnienia przez produkt lub procedury wprowadzone przez producenta zasadniczych wymogów określonych w załączniku I;

   b) niedociągnięć w normach zharmonizowanych, programach certyfikacji cyberbezpieczeństwa lub wspólnych specyfikacjach, o których mowa w art. 18.

6. Organy nadzoru rynku państw członkowskich inne niż organ nadzoru rynku państwa członkowskiego wszczynającego procedurę niezwłocznie informują Komisję i pozostałe państwa członkowskie o wszelkich przyjętych środkach i przekazują wszelkie posiadane dodatkowe informacje dotyczące niezgodności danego produktu z przepisami lub przedstawiają swoje zastrzeżenia, jeżeli nie zgadzają się ze zgłoszonym środkiem krajowym.

7. W przypadku gdy w terminie trzech miesięcy od otrzymania informacji, o których mowa w ust. 4, żadne państwo członkowskie ani Komisja nie zgłosi sprzeciwu wobec środka tymczasowego wprowadzonego przez dane państwo członkowskie, środek ten uznaje się za uzasadniony. Pozostaje to bez uszczerbku dla praw procesowych danego podmiotu gospodarczego określonych w art. 18 rozporządzenia (UE) 2019/1020.

8. Organy nadzoru rynku we wszystkich państwach członkowskich zapewniają niezwłoczne wprowadzenie odpowiednich środków ograniczających w odniesieniu do danego produktu, takich jak wycofanie produktu z obrotu.

Artykuł 44

Unijna procedura ochronna

1. Jeżeli w terminie trzech miesięcy od dnia otrzymania informacji, o której mowa w art. 43 ust. 4, państwo członkowskie zgłosi zastrzeżenia dotyczące środka wprowadzonego przez inne państwo członkowskie lub jeżeli Komisja uzna taki środek za sprzeczny z przepisami Unii, Komisja niezwłocznie przystępuje do konsultacji z odpowiednim państwem członkowskim i podmiotem gospodarczym lub podmiotami gospodarczymi i poddaje taki środek krajowy ocenie. Na podstawie wyników tej oceny Komisja podejmuje decyzję, czy środek krajowy jest uzasadniony czy nie, w terminie dziewięciu miesięcy od otrzymania informacji, o której mowa w art. 43 ust. 4, i informuje o tej decyzji dane państwo członkowskie.

2. W przypadku uznania krajowego środka za uzasadniony wszystkie państwa członkowskie wprowadzają środki konieczne do zapewnienia wycofania niezgodnego z przepisami produktu z elementami cyfrowymi ze swoich rynków oraz przekazują Komisji odpowiednie informacje. W przypadku uznania krajowego środka za nieuzasadniony dane państwo członkowskie wycofuje ten środek.

3. W przypadku uznania krajowego środka za uzasadniony i stwierdzenia, że niezgodność produktu z elementami cyfrowymi wynika z niedociągnięć w normach zharmonizowanych, Komisja stosuje procedurę przewidzianą w art. 10 rozporządzenia (UE) nr 1025/2012.

4. W przypadku uznania krajowego środka za uzasadniony i stwierdzenia, że niezgodność produktu z elementami cyfrowymi wynika z niedociągnięć w europejskim programie certyfikacji cyberbezpieczeństwa, o którym mowa w art. 18, Komisja rozważa, czy zmienić lub uchylić akt wykonawczy, o którym mowa w art. 18 ust. 4, określający domniemanie zgodności dotyczące tego programu certyfikacji.

5. W przypadku uznania krajowego środka za uzasadniony i stwierdzenia, że niezgodność produktu z elementami cyfrowymi wynika z niedociągnięć we wspólnych specyfikacjach, o których mowa w art. 19, Komisja rozważa, czy zmienić lub uchylić akt wykonawczy, o którym mowa w art. 19, określający te wspólne specyfikacje.

Artykuł 45

Procedura na szczeblu UE dotycząca produktów z elementami cyfrowymi stwarzających istotne ryzyko w cyberprzestrzeni

1. W przypadku gdy Komisja ma wystarczające powody, aby uznać, w tym na podstawie informacji przekazanych przez ENISA, że produkt z elementami cyfrowymi, który stanowi istotne ryzyko w cyberprzestrzeni, nie spełnia wymagań określonych w niniejszym rozporządzeniu, może zwrócić się do odpowiednich organów nadzoru rynku o przeprowadzenie oceny zgodności i zastosowanie procedur, o których mowa w art. 43.

2. W wyjątkowych okolicznościach, które uzasadniają niezwłoczną interwencję w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego, i jeżeli Komisja ma wystarczające powody, aby uznać, że produkt, o którym mowa w ust. 1, nadal nie spełnia wymogów określonych w niniejszym rozporządzeniu, a odpowiednie organy nadzoru rynku nie wprowadziły żadnych skutecznych środków, Komisja może zwrócić się do ENISA o przeprowadzenie oceny zgodności. Komisja informuje o tym odpowiednie organy nadzoru rynku. Odpowiednie podmioty gospodarcze współpracują w razie konieczności z ENISA.

3. Na podstawie oceny ENISA Komisja może zdecydować, że konieczne jest wprowadzenie środka naprawczego lub ograniczającego na szczeblu Unii. W tym celu Komisja niezwłocznie przeprowadza konsultacje z zainteresowanymi państwami członkowskimi i odpowiednim podmiotem gospodarczym lub podmiotami gospodarczymi.

4. Na podstawie konsultacji, o których mowa w ust. 3, Komisja może przyjąć akty wykonawcze w celu podjęcia decyzji o wprowadzeniu środków naprawczych lub ograniczających na szczeblu Unii, w tym nakazu wycofania produktu z obrotu lub odzyskania go, w rozsądnym terminie, stosownym do charakteru ryzyka. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 51 ust. 2.

5. Komisja niezwłocznie informuje odpowiedni podmiot gospodarczy lub odpowiednie podmioty gospodarcze o podjętej decyzji, o której mowa w ust. 4. Państwo członkowskie niezwłocznie wdraża akty, o których mowa w ust. 4, i informuje o tym Komisję.

6. Przepisy ust. 2–5 mają zastosowanie przez okres trwania wyjątkowej sytuacji, która uzasadnia interwencję Komisji, oraz do czasu zapewnienia zgodności danego produktu z przepisami niniejszego rozporządzenia.

Artykuł 46

Zgodne z przepisami produkty z elementami cyfrowymi, które stwarzają istotne ryzyko w cyberprzestrzeni

1. Jeżeli po przeprowadzeniu oceny zgodnie z art. 43 organ nadzoru rynku państwa członkowskiego stwierdzi, że chociaż produkt z elementami cyfrowymi i procedury wprowadzone przez producenta są zgodne z niniejszym rozporządzeniem, stwarzają one istotne ryzyko w cyberprzestrzeni, a także stwarzają ryzyko dla zdrowia i bezpieczeństwa osób, dla wypełnienia obowiązków wynikających z prawa Unii lub prawa krajowego mających na celu ochronę praw podstawowych, dostępności, autentyczności, integralności lub poufności usług oferowanych przy użyciu elektronicznego systemu informacyjnego przez podmioty niezbędne takie jak podmioty, o których mowa w [załączniku I do dyrektywy XXX / XXXX (dyrektywy NIS 2)], lub dla innych aspektów ochrony interesu publicznego, organ zobowiązuje właściwy podmiot gospodarczy do wprowadzenia wszelkich odpowiednich środków w celu zapewnienia, aby dany produkt z elementami cyfrowymi oraz dane procedury wprowadzone przez producenta po wprowadzeniu do obrotu nie stwarzały już takiego ryzyka, do wycofania produktu z elementami cyfrowymi z obrotu lub odzyskania go w rozsądnym terminie, stosownym do charakteru ryzyka.

2. Producent lub inne właściwe podmioty gospodarcze zapewniają podjęcie działań naprawczych w odniesieniu do odnośnych produktów z elementami cyfrowymi,

które udostępniły na rynku w całej Unii, w terminie wyznaczonym przez organ nadzoru rynku państwa członkowskiego, o którym mowa w ust. 1.

3. Państwo członkowskie niezwłocznie informuje Komisję i pozostałe państwa członkowskie o środkach wprowadzonych na podstawie ust. 1. Informacje te obejmują wszelkie dostępne informacje szczegółowe, w szczególności dane konieczne do identyfikacji odnośnych produktów z elementami cyfrowymi, informacje na temat pochodzenia i łańcucha dostaw tych produktów z elementami cyfrowymi, charakteru występującego ryzyka oraz rodzaju i okresu obowiązywania wprowadzonych środków krajowych.

4. Komisja niezwłocznie rozpoczyna konsultacje z państwami członkowskimi i odpowiednim podmiotem gospodarczym oraz ocenia wprowadzone środki krajowe. Na podstawie wyników tej oceny Komisja decyduje, czy dany środek jest uzasadniony, oraz proponuje odpowiednie środki, o ile są konieczne.

5. Komisja kieruje swoją decyzję do państw członkowskich.

6. W przypadku gdy Komisja ma wystarczające powody, aby uznać, w tym na podstawie informacji przekazanych przez ENISA, że produkt z elementami cyfrowymi, choć zgodny z niniejszym rozporządzeniem, stwarza ryzyko, o którym mowa w ust. 1, może zwrócić się do odpowiedniego organu lub odpowiednich organów nadzoru rynku o przeprowadzenie oceny zgodności i zastosowanie procedur, o których mowa w art. 43 oraz w ust. 1, 2 i 3 niniejszego artykułu.

7. W wyjątkowych okolicznościach, które uzasadniają niezwłoczną interwencję w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego, i jeżeli Komisja ma wystarczające powody, aby uznać, że produkt, o którym mowa w ust. 6, nadal stwarza ryzyko, o którym mowa w ust. 1, a odpowiednie krajowe organy nadzoru rynku nie wprowadziły żadnych skutecznych środków, Komisja może zwrócić się do ENISA o przeprowadzenie oceny ryzyka stwarzanego przez ten produkt i informuje o tym odpowiednie organy nadzoru rynku. Odpowiednie podmioty gospodarcze współpracują w razie konieczności z ENISA.

8. Na podstawie oceny ENISA, o której mowa w ust. 7, Komisja może ustalić, że konieczne jest wprowadzenie środka naprawczego lub ograniczającego na szczeblu Unii. W tym celu Komisja niezwłocznie przeprowadza konsultacje z zainteresowanymi państwami członkowskimi i odpowiednim podmiotem gospodarczym lub odpowiednimi podmiotami gospodarczymi.

9. Na podstawie konsultacji, o których mowa w ust. 8, Komisja może przyjąć akty wykonawcze w celu podjęcia decyzji o wprowadzeniu środków naprawczych lub ograniczających na szczeblu Unii, w tym nakazu wycofania produktu z obrotu lub odzyskania go, w rozsądnym terminie, stosownym do charakteru ryzyka. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 51 ust. 2.

10. Komisja niezwłocznie informuje odpowiedni podmiot gospodarczy lub odpowiednie podmioty gospodarcze o podjętej decyzji, o której mowa w ust. 9. Państwo członkowskie niezwłocznie wprowadza w życie takie akty i informuje o tym Komisję.

11. Przepisy ust. 6–10 mają zastosowanie przez okres trwania wyjątkowej sytuacji, która uzasadnia interwencję Komisji, oraz do czasu, aż dany produkt przestanie stwarzać ryzyko, o którym mowa w ust. 1.

Artykuł 47

Formalna niezgodność z przepisami

1. Jeżeli organ nadzoru rynku państwa członkowskiego dokona jednego z poniższych ustaleń, wymaga od właściwego producenta usunięcia danej niezgodności:

   a) umieszczenie oznakowania zgodności z naruszeniem art. 21 i 22;

   b) nieumieszczenie oznakowania zgodności;

   c) niesporządzenie deklaracji zgodności UE;

   d) nieprawidłowe sporządzenie deklaracji zgodności UE;

   e) nieumieszczenie numeru identyfikacyjnego jednostki notyfikowanej zaangażowanej, w stosownych przypadkach, w procedurę oceny zgodności;

   f) niedostępna albo niekompletna dokumentacja techniczna.

2. W przypadku utrzymywania się niezgodności, o której mowa w ust. 1, dane państwo członkowskie wprowadza wszystkie odpowiednie środki w celu ograniczenia lub zakazania udostępniania danego produktu z elementami cyfrowymi na rynku bądź zapewnienia jego odzyskania lub wycofania z obrotu.

Artykuł 48

Wspólne działania organów nadzoru rynku

1. Organy nadzoru rynku mogą zawierać porozumienia z innymi odpowiednimi organami w sprawie podejmowania wspólnych działań ukierunkowanych na zapewnienie cyberbezpieczeństwa i ochronę konsumentów w odniesieniu do określonych produktów z elementami cyfrowymi wprowadzonych do obrotu lub udostępnionych na rynku, w szczególności produktów często stwarzających ryzyko w cyberprzestrzeni.

2. Komisja lub ENISA mogą zaproponować wspólne działania w zakresie kontroli zgodności z niniejszym rozporządzeniem, które mają być prowadzone przez organy nadzoru rynku, na podstawie wskazań lub informacji dotyczących potencjalnej niezgodności produktów objętych zakresem stosowania niniejszego rozporządzenia z wymogami określonymi w niniejszym rozporządzeniu w szeregu państw członkowskich.

3. Organy nadzoru rynku oraz Komisja, w stosownych przypadkach, zapewniają, aby porozumienie w sprawie wspólnych działań nie prowadziło do nieuczciwej konkurencji między podmiotami gospodarczymi ani nie wpływało negatywnie na obiektywizm, niezależność i bezstronność stron porozumienia.

4. Organ nadzoru rynku może wykorzystywać wszelkie informacje uzyskane w wyniku działań prowadzonych w ramach wszczętego przez ten organ postępowania wyjaśniającego.

5. Dany organ nadzoru rynku oraz Komisja, w stosownych przypadkach, udostępniają publicznie porozumienie w sprawie wspólnych działań, podając nazwy zaangażowanych w nie podmiotów.

Artykuł 49

Akcje kontrolne

1. Organy nadzoru rynku mogą podjąć decyzję o przeprowadzeniu jednoczesnych skoordynowanych działań kontrolnych („akcji kontrolnych”) w odniesieniu do poszczególnych produktów z elementami cyfrowymi lub ich kategorii w celu sprawdzenia zgodności z niniejszym rozporządzeniem lub wykrycia jego naruszeń.

2. O ile zaangażowane organy nadzoru rynku nie uzgodnią inaczej, akcje kontrolne koordynuje Komisja. Koordynator akcji kontrolnej może w stosownych przypadkach podać do publicznej wiadomości zagregowane wyniki.

3. ENISA może określić – w ramach wykonywania swoich zadań, w tym na podstawie zgłoszeń otrzymywanych zgodnie z art. 11 ust. 1 i 2 – kategorie produktów, w odniesieniu do których można zorganizować akcje kontrolne. Wniosek dotyczący akcji kontrolnych przedkłada się potencjalnemu koordynatorowi, o którym mowa w ust. 2, do rozpatrzenia przez organy nadzoru rynku.

4. Prowadząc akcje kontrolne, zaangażowane organy nadzoru rynku mogą korzystać z uprawnień do przeprowadzania postępowania wyjaśniającego określonych w art. 41–47 i wszelkich innych uprawnień nadanych im na mocy przepisów prawa krajowego.

5. Organy nadzoru rynku mogą zapraszać urzędników Komisji i inne osoby towarzyszące upoważnione przez Komisję do udziału w akcjach kontrolnych.

ROZDZIAŁ VI

PRZEKAZANE UPRAWNIENIA I PROCEDURA KOMITETOWA

Artykuł 50

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 2 ust. 4, art. 6 ust. 2, 3 i 5, art. 20 ust. 5 i art. 23 ust. 5, powierza się Komisji.

3. Przekazanie uprawnień, o którym mowa w art. 2 ust. 4, art. 6 ust. 2, 3 i 5, art. 20 ust. 5 i art. 23 ust. 5, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 2 ust. 4, art. 6 ust. 2, 3 i 5, art. 20 ust. 5 i art. 23 ust. 5 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu

Parlamentowi Europejskiemu i Radzie lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 51

Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.
2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.
3. W przypadku gdy opinia komitetu ma zostać uzyskana w drodze procedury pisemnej, procedura ta kończy się bez osiągnięcia rezultatu, gdy – przed upływem terminu na wydanie opinii – zdecyduje o tym przewodniczący komitetu lub wniesie o to członek komitetu.

ROZDZIAŁ VII

POUFNOŚĆ I KARY

Artykuł 52

Poufność

1. Wszystkie strony zaangażowane w stosowanie niniejszego rozporządzenia przestrzegają zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań i swojej działalności w taki sposób, aby chronić w szczególności:
   a) prawa własności intelektualnej oraz poufne informacje handlowe lub tajemnice przedsiębiorstwa osoby fizycznej lub prawnej, w tym kod źródłowy, chyba że zastosowanie mają przypadki określone w art. 5 dyrektywy Parlamentu Europejskiego i Rady 2016/943[24];
   b) skuteczne wdrożenie niniejszego rozporządzenia, w szczególności do celów inspekcji, postępowań wyjaśniających lub audytów;
   c) interesy bezpieczeństwa publicznego i narodowego;
   d) uczciwy przebieg postępowań karnych i administracyjnych.
2. Nie naruszając przepisów ust. 1, informacji wymienianych na zasadzie poufności między organami nadzoru rynku oraz między organami nadzoru rynku a Komisją nie ujawnia się bez uprzedniej zgody organu nadzoru rynku, od którego informacje te pochodzą.
3. Ust. 1 i 2 pozostają bez uszczerbku dla praw i obowiązków Komisji, państw członkowskich i jednostek notyfikowanych w zakresie wymiany informacji

[24] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.U. L 157 z 15.6.2016, s. 1).

i wydawania ostrzeżeń oraz obowiązków zainteresowanych osób w zakresie udzielania informacji zgodnie z prawem karnym państw członkowskich.

4. W stosownych przypadkach Komisja i państwa członkowskie mogą wymieniać informacje szczególnie chronione z odpowiednimi organami państw trzecich, z którymi zawarły dwustronne lub wielostronne porozumienia o poufności gwarantujące odpowiedni stopień ochrony.

Artykuł 53

Kary

1. Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszania przez podmioty gospodarcze przepisów niniejszego rozporządzenia i wdrażają wszystkie środki niezbędne w celu zapewnienia ich wprowadzenia. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.

2. Państwa członkowskie niezwłocznie powiadamiają Komisję o tych przepisach i środkach, a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą.

3. Niezgodność z zasadniczymi wymogami cyberbezpieczeństwa określonymi w załączniku I oraz z obowiązkami określonymi w art. 10 i 11 podlega administracyjnej karze pieniężnej w wysokości do 15 000 000 EUR lub, jeżeli za naruszenie odpowiada przedsiębiorstwo – w wysokości do 2,5 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

4. Niezgodność z wszelkimi innymi obowiązkami wynikającymi z niniejszego rozporządzenia podlega administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR lub, jeżeli za naruszenie odpowiada przedsiębiorstwo – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

5. Przekazywanie informacji nieprawidłowych, niekompletnych lub wprowadzających w błąd jednostkom notyfikowanym i organom nadzoru rynku w odpowiedzi na ich wniosek podlega administracyjnej karze pieniężnej w wysokości do 5 000 000 EUR lub, jeżeli za naruszenie odpowiada przedsiębiorstwo – w wysokości do 1 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

6. Ustalając wysokość administracyjnej kary pieniężnej, w każdym indywidualnym przypadku uwzględnia się wszystkie istotne okoliczności danej sytuacji i zwraca się należytą uwagę na następujące kwestie:

   a) charakter, wagę i czas trwania naruszenia oraz jego konsekwencje;

   b) czy inne organy nadzoru rynku nałożyły już na ten sam podmiot gospodarczy administracyjne kary pieniężne za podobne naruszenie;

   c) wielkość podmiotu gospodarczego dopuszczającego się naruszenia i jego udział w rynku.

7. Organy nadzoru rynku, które stosują administracyjne kary pieniężne, przekazują te informacje organom nadzoru rynku pozostałych państw członkowskich za

pośrednictwem systemu informacyjnego i komunikacyjnego, o którym mowa w art. 34 rozporządzenia (UE) 2019/1020.

8. Każde państwo członkowskie określa, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim.

9. W zależności od systemu prawnego państw członkowskich przepisy dotyczące administracyjnych kar pieniężnych można stosować w taki sposób, że kary nakładają właściwe sądy krajowe lub inne odpowiednie organy zgodnie z kompetencjami ustanowionymi na szczeblu krajowym w tych państwach członkowskich. Stosowanie takich przepisów w tych państwach członkowskich ma skutek równoważny.

10. Administracyjne kary pieniężne można nakładać, w zależności od okoliczności każdego indywidualnego przypadku, oprócz wszelkich innych środków naprawczych lub ograniczających stosowanych przez organy nadzoru rynku w odniesieniu do tego samego naruszenia.

ROZDZIAŁ VIII

PRZEPISY PRZEJŚCIOWE I KOŃCOWE

Artykuł 54

Zmiana w rozporządzeniu (UE) 2019/1020

W załączniku I do rozporządzenia (UE) 2019/1020 dodaje się punkt w brzmieniu:

„71. [Rozporządzenie XXX][akt dotyczący cyberodporności].”

Artykuł 55

Przepisy przejściowe

1. Certyfikaty badania typu UE i decyzje o zatwierdzeniu wydane w odniesieniu do wymogów cyberbezpieczeństwa dotyczących produktów z elementami cyfrowymi, które podlegają innemu unijnemu prawodawstwu harmonizacyjnemu, zachowują ważność do [42 miesięcy od daty wejścia w życie niniejszego rozporządzenia] r., chyba że ich ważność wygasa przed tą datą lub że określono inaczej w innych przepisach Unii, w którym to przypadku zachowują ważność zgodnie z tymi przepisami Unii.

2. Produkty z elementami cyfrowymi, które zostały wprowadzone do obrotu przed [data rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 57] r., podlegają wymogom określonym w niniejszym rozporządzeniu wyłącznie w przypadku, gdy od tej daty nastąpią istotne modyfikacje projektu lub przeznaczenia tych produktów.

3. Na zasadzie odstępstwa od ust. 2 obowiązki określone w art. 11 mają zastosowanie do wszystkich produktów z elementami cyfrowymi objętych zakresem stosowania niniejszego rozporządzenia, które zostały wprowadzone do obrotu przed [data rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 57] r.

Artykuł 56

Ocena i przegląd

Do [36 miesięcy od daty rozpoczęcia stosowania niniejszego rozporządzenia] r., a następnie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia. Sprawozdania te są podawane do wiadomości publicznej.

Artykuł 57

Wejście w życie i stosowanie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie stosuje się od [24 miesiące od wejścia w życie niniejszego rozporządzenia] r. Art. 11 stosuje się jednak od [12 miesięcy od wejścia w życie niniejszego rozporządzenia] r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*

OCEANA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa

1.3. Wniosek/inicjatywa dotyczy:

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

1.4.2. Cel(e) szczegółowy(e)

1.4.3. Oczekiwane wyniki i wpływ

1.4.4. Wskaźniki dotyczące realizacji celów

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

1.5.2. Wartość dodana z tytułu zaangażowania Unii (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii" należy rozumieć jako wartość wynikającą z unijnej interwencji wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

1.6. Czas trwania i wpływ finansowy wniosku/inicjatywy

1.7. Planowane tryby zarządzania

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

2.2.3. Oszacowanie i uzasadnienie opłacalności kontroli (stosunek „kosztów kontroli do wartości zarządzanych funduszy powiązanych") oraz ocena oczekiwanych poziomów ryzyka błędu (przy płatności i w chwili zamknięcia)

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne

3.2.2. Przewidywany produkt finansowany ze środków operacyjnych

3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

3.2.5. Udział osób trzecich w finansowaniu

3.3. Szacunkowy wpływ na dochody

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący rozporządzenia w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi (akt dotyczący cyberodporności)

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa

Sieci komunikacyjne, treści i technologie

1.3. Wniosek/inicjatywa dotyczy:

× **nowego działania**

☐ **nowego działania będącego następstwem projektu pilotażowego/działania przygotowawczego**[37]

☐ **przedłużenia bieżącego działania**

☐ **połączenia lub przekształcenia co najmniej jednego działania pod kątem innego/nowego działania**

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

Zakres wniosku obejmuje dwa główne cele służące zapewnieniu prawidłowego funkcjonowania rynku wewnętrznego: 1) **stworzenie warunków dla rozwoju bezpiecznych produktów z elementami cyfrowymi** przez zapewnienie, aby sprzęt i oprogramowanie były wprowadzane do obrotu z mniejszą liczbą podatności, a także aby producenci poważnie traktowali bezpieczeństwo w całym cyklu życia produktu oraz 2) **stworzenie warunków umożliwiających użytkownikom uwzględnianie cyberbezpieczeństwa przy wyborze produktów z elementami cyfrowymi i korzystaniu z nich**.

1.4.2. Cel(e) szczegółowy(e)

Określono **cztery cele szczegółowe** w odniesieniu do wniosku: (i) zapewnienie, aby producenci poprawiali bezpieczeństwo produktów z elementami cyfrowymi, począwszy od etapu projektowania i opracowywania oraz przez cały cykl życia; (ii) zapewnienie spójnych ram cyberbezpieczeństwa, ułatwiających producentom sprzętu i oprogramowania przestrzeganie przepisów; (iii) zwiększenie przejrzystości zabezpieczeń produktów z elementami cyfrowymi oraz (iv) umożliwienie przedsiębiorstwom i konsumentom bezpiecznego korzystania z produktów z elementami cyfrowymi.

Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupom docelowym.

[37] O którym mowa w art. 58 ust. 2 lit. a) lub b) rozporządzenia finansowego.

Wniosek może przynieść znaczące korzyści dla poszczególnych zainteresowanych stron. W przypadku przedsiębiorstw pozwoli on zapobiec rozbieżnym przepisom dotyczącym bezpieczeństwa produktów z elementami cyfrowymi oraz obniżyć koszty przestrzegania związanych z nimi przepisów dotyczących cyberbezpieczeństwa. Może się on przyczynić do zmniejszenia liczby cyberincydentów, obniżenia kosztów postępowania w przypadku incydentu oraz uniknięcia nadszarpnięcia reputacji. W przypadku całej UE szacuje się, że inicjatywa może doprowadzić do obniżenia kosztów związanych z incydentami dotyczącymi przedsiębiorstw o około 180–290 mld EUR rocznie[38]. Inicjatywa może spowodować wzrost obrotu ze względu na coraz większy popyt na produkty z elementami cyfrowymi. Może poprawić światową reputację przedsiębiorstw, co spowodowałoby wzrost popytu również spoza UE. Jeżeli chodzi o użytkowników, preferowany wariant może zwiększyć przejrzystość zabezpieczeń i ułatwić korzystanie z produktów z elementami cyfrowymi. Konsumenci i obywatele odniosą także korzyść polegającą na lepszej ochronie ich praw podstawowych, takich jak prywatność i ochrona danych.

Jednocześnie wniosek może zwiększyć koszty przestrzegania i egzekwowania przepisów ponoszone przez przedsiębiorstwa, jednostki notyfikowane i organy publiczne, w tym organy ds. akredytacji i organy nadzoru rynku. W przypadku twórców oprogramowania i producentów sprzętu oznaczać to będzie dodatkowe bezpośrednie koszty przestrzegania przepisów w związku z nowymi wymogami bezpieczeństwa, oceną zgodności, obowiązkami w zakresie dokumentacji i zgłaszania incydentów, co spowoduje, że zagregowane koszty przestrzegania przepisów wyniosą około 29 mld EUR przy szacowanej wartości rynkowej obrotu wynoszącej 1 485 mld EUR[39]. Użytkownicy, w tym użytkownicy biznesowi, konsumenci i obywatele mogą doświadczyć wyższych cen produktów z elementami cyfrowymi. Należy je jednak postrzegać w kontekście znaczących korzyści opisanych powyżej.

1.4.3. Wskaźniki dotyczące realizacji celów

Należy określić wskaźniki stosowane do monitorowania postępów i osiągnięć.

Aby sprawdzić, czy producenci zwiększyli bezpieczeństwo produktów z elementami cyfrowymi, począwszy od etapu projektowania i opracowywania oraz przez cały cykl życia tych produktów, można wziąć pod uwagę szereg wskaźników. Mogą to być: liczba istotnych incydentów w Unii spowodowanych podatnościami, udział producentów sprzętu i oprogramowania, którzy stosują cykl życia polegający na systematycznym bezpiecznym opracowywaniu, analiza jakościowa bezpieczeństwa produktów z elementami cyfrowymi, ilościowa i jakościowa ocena baz danych dotyczących podatności, częstotliwość udostępniania przez producentów poprawek zabezpieczeń lub średnia liczba dni między wykryciem podatności a udostępnieniem poprawek zabezpieczeń.

[38] Zob. [dokument roboczy służb Komisji zawierający sprawozdanie z oceny skutków towarzyszący rozporządzeniu w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi].

[39] Zob. [dokument roboczy służb Komisji zawierający sprawozdanie z oceny skutków towarzyszący rozporządzeniu w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi].

Wskaźnikiem dotyczącym spójnych ram cyberbezpieczeństwa może być brak ukierunkowanych krajowych przepisów w zakresie cyberbezpieczeństwa dotyczących konkretnych produktów.

Wskaźnikiem dotyczącym zwiększonej przejrzystości w zakresie zabezpieczeń produktów z elementami cyfrowymi może być udział produktów z elementami cyfrowymi, które są dostarczane z informacjami na temat zabezpieczeń. Ponadto jako wskaźnik tego, czy organizacjom i konsumentom umożliwia się bezpieczne użytkowanie produktów z elementami cyfrowymi, można wykorzystać udział produktów z elementami cyfrowymi, które są dostarczane z instrukcjami dla użytkownika dotyczącymi bezpiecznego użytkowania.

Jeżeli chodzi o monitorowanie wpływu rozporządzenia, w tym celu należałoby rozważyć określone wskaźniki, które Komisja, w stosownych przypadkach przy wsparciu ENISA, miałaby poddawać ocenie. W zależności od celu operacyjnego, który należy osiągnąć, niektóre wskaźniki monitorowania, na podstawie których zostanie ocenione powodzenie horyzontalnych wymogów cyberbezpieczeństwa, są następujące:

W przypadku oceny poziomu cyberbezpieczeństwa produktów z elementami cyfrowymi:

– statystyka i analiza jakościowa dotycząca incydentów mających wpływ na produkty z elementami cyfrowymi oraz sposób postępowania z nimi. Komisja, przy wsparciu ENISA, mogłaby gromadzić te dane i oceniać je;

– rejestry znanych podatności i analizy sposobu postępowania z nimi. ENISA mogłaby przeprowadzić taką analizę w oparciu o europejską bazę danych dotyczących podatności utworzoną na podstawie [dyrektywy XXX/XXXX (NIS 2)];

– badania prowadzone wśród producentów sprzętu i oprogramowania w celu monitorowania postępów.

W przypadku oceny poziomu informacji na temat zabezpieczeń, wsparcia w zakresie zabezpieczeń, wycofania z eksploatacji i należytej staranności: wyniki badań, które przeprowadzi Komisja przy wsparciu ENISA, zarówno wśród użytkowników, jak i przedsiębiorstw.

W przypadku oceny realizacji celem Komisji będzie zapewnienie skutecznego przeprowadzenia ocen zgodności. W tym celu zostanie wydane zlecenie normalizacji, a jego realizacja będzie monitorowana. Komisja sprawdzi również możliwości jednostek notyfikowanych oraz, w stosownych przypadkach, jednostek certyfikujących.

Jeżeli chodzi o stosowanie, za pomocą sprawozdań państw członkowskich Komisja sprawdzi, czy inicjatywy krajowe nie dotyczą aspektów objętych zakresem rozporządzenia.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

Niniejsze rozporządzenie powinno mieć pełne zastosowanie 24 miesiące po jego wejściu w życie. Elementy struktury zarządzania powinny jednak funkcjonować wcześniej. W szczególności państwa członkowskie powinny wyznaczyć istniejące

organy lub ustanowić nowe organy do wykonywania zadań określonych w przepisach.

1.5.2. Wartość dodana z tytułu zaangażowania Unii (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii" należy rozumieć jako wartość wynikającą z unijnej interwencji wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Wyraźnie transgraniczny charakter cyberbezpieczeństwa i coraz częstsze incydenty, których skutki uboczne są odczuwalne w innych krajach oraz dotykają inne sektory i produkty, oznaczają, że państwa członkowskie nie są w stanie skutecznie osiągnąć wspomnianych celów samodzielnie. Biorąc pod uwagę globalny charakter rynków produktów z elementami cyfrowymi, państwa członkowskie stoją w obliczu takiego samego ryzyka w przypadku tego samego produktu z elementami cyfrowymi na swoim terytorium. Pojawiające się niejednolite ramy potencjalnie rozbieżnych przepisów krajowych również mogą zakłócić otwarty i konkurencyjny jednolity rynek produktów z elementami cyfrowymi. Wspólne działanie na szczeblu UE jest zatem konieczne, aby wzbudzić większe zaufanie użytkowników i poprawić atrakcyjność unijnych produktów z elementami cyfrowymi. Przyniosłoby to również korzyści rynkowi wewnętrznemu, gdyż zapewniłoby pewność prawa i równe warunki działania sprzedawcom produktów z elementami cyfrowymi.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Akt dotyczący cyberodporności jest pierwszą tego typu regulacją, w ramach której wprowadza się wymogi cyberbezpieczeństwa w zakresie wprowadzania do obrotu produktów z elementami cyfrowymi. Opiera się on jednak na ustanowieniu nowych ram prawnych oraz na doświadczeniach zdobytych w procesie wdrażania obowiązującego unijnego prawodawstwa harmonizacyjnego dotyczącego różnych produktów, szczególnie w zakresie przygotowania do wdrażania, w tym aspektów takich jak opracowanie norm zharmonizowanych.

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

W rozporządzeniu w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi określono nowe wymogi cyberbezpieczeństwa dla wszystkich produktów z elementami cyfrowymi wprowadzonych do obrotu na rynku UE, których zakres wykracza poza wszelkie wymogi przewidziane w obowiązujących przepisach. Jednocześnie wniosek opiera się na obowiązującej strukturze przepisów nowych ram prawnych. W związku z tym opiera się on na obowiązujących strukturach i procedurach nowych ram prawnych, takich jak współpraca jednostek notyfikowanych i nadzór rynku, moduły oceny zgodności, opracowywanie norm zharmonizowanych. Ponadto nowy wniosek opiera się na niektórych strukturach opracowanych zgodnie z innymi przepisami dotyczącymi cyberbezpieczeństwa, takimi jak dyrektywa (UE) 2016/1148 (dyrektywa w sprawie bezpieczeństwa sieci i informacji), odpowiednio [dyrektywa XXX/XXXX (NIS 2)] lub rozporządzenie (UE) 2019/881 (akt o cyberbezpieczeństwie).

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

Zarządzanie obszarami działania przydzielonymi ENISA odpowiada jej obowiązującemu mandatowi i zadaniom ogólnym. Te obszary działania mogą wymagać określonych profili lub nowych zadań, ale nie będą one znaczące i mogą zostać wchłonięte przez istniejące zasoby ENISA oraz rozwiązane przez realokację lub połączenie różnych zadań. Na przykład jeden z głównych obszarów działania przydzielonych ENISA dotyczy gromadzenia i przetwarzania zgłoszeń od producentów dotyczących wykorzystywanych podatności produktów. W [dyrektywie XXX/XXXX (NIS 2)] powierzono już ENISA zadanie polegające na utworzeniu europejskiej bazy danych dotyczących podatności, w której można ujawniać i rejestrować publicznie znane podatności, na zasadzie dobrowolności, w celu umożliwienia użytkownikom wprowadzenia odpowiednich środków łagodzących. Zasoby przeznaczone na ten cel można również wykorzystać na nowe wyżej wspomniane zadania związane z zawiadomieniami o podatnościach produktów. Mogłoby to zapewnić skuteczne wykorzystanie istniejących zasobów, a także doprowadzić do powstania niezbędnych synergii między takimi zadaniami, które można lepiej wykorzystać w analizach ENISA dotyczących ryzyka i zagrożeń w cyberprzestrzeni.

1.6. Czas trwania i wpływ finansowy wniosku/inicjatywy

☐ **Ograniczony czas trwania**

– ☐ Okres trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

– ☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r. w odniesieniu do środków na zobowiązania oraz od RRRR r. do RRRR r. w odniesieniu do środków na płatności.

× **Nieograniczony czas trwania**

– Wprowadzenie w życie z okresem rozruchu od 2025 r.

– po którym następuje faza operacyjna.

1.7. Planowane tryby zarządzania[40]

☐ **Zarządzanie bezpośrednie** przez Komisję

– × w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;

– ☐ przez agencje wykonawcze

☐ **Zarządzanie dzielone** z państwami członkowskimi

☐ **Zarządzanie pośrednie** poprzez przekazanie zadań związanych z wykonaniem budżetu:

– ☐ państwom trzecim lub organom przez nie wyznaczonym;

– ☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

– ☐ EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

– ☐ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego;

– ☐ organom prawa publicznego;

– ☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile są im zapewnione odpowiednie gwarancje finansowe;

– ☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego i zapewniono odpowiednie gwarancje finansowe;

– ☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie.

– *W przypadku wskazania więcej niż jednego trybu zarządzania należy podać dodatkowe informacje w części „Uwagi”.*

Uwagi

[40] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

W niniejszym rozporządzeniu przypisuje się ENISA określone działania zgodnie z jej obecnym mandatem, a w szczególności z art. 3 ust. 2 rozporządzenia 2019/881 stanowiącym, że ENISA wykonuje zadania powierzone jej na mocy aktów prawnych Unii określających środki zbliżania przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które to przepisy dotyczą cyberbezpieczeństwa. W szczególności do zadań ENISA należy otrzymywanie od producentów zgłoszeń aktywnie wykorzystywanych podatności produktów z elementami cyfrowymi, jak również zgłoszeń incydentów mających wpływ na bezpieczeństwo tych produktów. ENISA powinna także przekazywać te zgłoszenia właściwym CSIRT lub odpowiednio właściwym pojedynczym punktom kontaktowym państw członkowskich wyznaczonym zgodnie z art. [art. X] dyrektywy [dyrektywy XXX/XXXX (NIS 2)], jak również informować o nich właściwe organy nadzoru rynku. Na podstawie gromadzonych informacji ENISA powinna co dwa lata przygotowywać sprawozdanie techniczne na temat pojawiających się tendencji w zakresie ryzyka w cyberprzestrzeni dotyczącego produktów z elementami cyfrowymi oraz przedkładać je grupie współpracy NIS. Ponadto, uwzględniając wiedzę fachową ENISA, zgromadzone informacje i analizy zagrożeń, ENISA może wspierać proces wdrażania niniejszego rozporządzenia, proponując wspólne działania, które miałyby być prowadzone przez krajowe organy nadzoru rynku w oparciu o wskazania lub informacje dotyczące potencjalnej niezgodności z niniejszym rozporządzeniem produktów z elementami cyfrowymi w szeregu państw członkowskich, lub określając kategorie produktów, w odniesieniu do których można zorganizować równoczesne skoordynowane działania kontrolne. W wyjątkowych okolicznościach Komisja może zwrócić się do ENISA o przeprowadzenie oceny określonych produktów z elementami cyfrowymi, które stwarzają istotne ryzyko w cyberprzestrzeni i w przypadku których wymagana jest natychmiastowa interwencja w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego.

Szacuje się, że wszystkie te zadania będą wymagały około 4,5 EPC z istniejących zasobów ENISA, biorąc pod uwagę wiedzę fachową i prace przygotowawcze wykonywane obecnie przez ENISA, między innymi w celu wsparcia zbliżającego się wdrożenia [dyrektywy XXX/XXXX (NIS 2)], na potrzeby którego uzupełniono zasoby ENISA.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Należy określić częstotliwość i warunki.

Do 36 miesięcy od daty rozpoczęcia stosowania niniejszego rozporządzenia, a następnie co cztery lata Komisja przedłoży Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu. Sprawozdania te są podawane do wiadomości publicznej.

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli

W niniejszym rozporządzeniu ustanowiono nową politykę dotyczącą zharmonizowanych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi wprowadzanych do obrotu na rynku wewnętrznym w całym ich cyklu życia. Po przyjęciu aktu prawnego Komisja zwróci się do europejskich organów normalizacyjnych o opracowanie norm. Konieczne jest zapewnienie służbom Komisji odpowiednich zasobów, aby mogły sprostać tym nowym zadaniom. Szacuje się, że egzekwowanie nowego rozporządzenia będzie wymagało 7 EPC (w tym jednego SNE) do realizacji następujących zadań:

- opracowanie zlecenia normalizacji lub wspólnych specyfikacji za pośrednictwem aktów wykonawczych w przypadku braku skutecznego procesu normalizacji;
- opracowanie aktu delegowanego [w terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia] zawierającego definicje produktów krytycznych z elementami cyfrowymi;
- ewentualne opracowanie aktów delegowanych w celu aktualizacji wykazu produktów krytycznych klasy I i II; określenie, czy konieczne jest ograniczenie lub wyłączenie w odniesieniu do produktów z elementami cyfrowymi objętych innymi przepisami unijnymi określającymi wymogi zapewniające taki sam poziom ochrony jak niniejsze rozporządzenie; wprowadzenie obowiązku certyfikacji niektórych produktów wysoce krytycznych z elementami cyfrowymi w oparciu o kryteria określone w niniejszym rozporządzeniu; określenie minimalnego zakresu deklaracji zgodności UE oraz uzupełnienie elementów, które należy uwzględnić w dokumentacji technicznej;
- ewentualne opracowanie aktów wykonawczych w zakresie formatu lub elementów dotyczących obowiązków w zakresie zgłaszania incydentów, zestawienia podstawowych materiałów do produkcji oprogramowania, wspólnych specyfikacji lub umieszczania oznakowania CE;
- ewentualne przygotowanie niezwłocznej interwencji w celu wprowadzenia w wyjątkowych okolicznościach środków naprawczych lub ograniczających w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego, w tym opracowanie aktu wykonawczego;
- organizacja i koordynacja notyfikacji jednostek notyfikowanych przez państwa członkowskie oraz koordynacja jednostek notyfikowanych;

– wspieranie koordynacji organów nadzoru rynku państw członkowskich.

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

W celu zapewnienia wymiany informacji między jednostkami notyfikowanymi i organami nadzoru rynku oraz ich dobrej współpracy Komisja odpowiada za ich koordynację. W celu zapewnienia fachowej wiedzy technicznej i rynkowej utworzona zostanie grupa ekspertów.

2.2.3. Oszacowanie i uzasadnienie opłacalności kontroli (stosunek „kosztów kontroli do wartości zarządzanych funduszy powiązanych") oraz ocena oczekiwanych poziomów ryzyka błędu (przy płatności i w chwili zamknięcia)

2.3. Jeżeli chodzi o wydatki na posiedzenia, biorąc pod uwagę niską wartość pojedynczej transakcji (np. zwrot kosztów podróży dla delegata na posiedzenie), standardowe procedury kontroli wydają się wystarczające. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony, np. ze strategii zwalczania nadużyć finansowych.

Dodatkowe potrzeby w zakresie środków niezbędnych do celów niniejszego rozporządzenia zostaną zaspokojone w ramach istniejących środków zapobiegania nadużyciom finansowym mających zastosowanie do Komisji.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

- Istniejące linie budżetowe

Schemat

- Nowe linie budżetowe, o których utworzenie się wnioskuje

Nie dotyczy

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne

– ☑ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	Numer	

DG: <…….>			Rok **N**[41]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (zob. pkt 1.6)			**OGÓŁEM**
• Środki operacyjne										
Linia budżetowa[42]	Środki na zobowiązania	(1a)								
	Środki na płatności	(2a)								
Linia budżetowa	Środki na zobowiązania	(1b)								
	Środki na płatności	(2b)								
Środki administracyjne finansowane ze środków przydzielonych na określone programy[43]										

[41] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy. „N” należy zastąpić oczekiwanym pierwszym rokiem realizacji (np.: 2021).Tak samo należy postąpić dla kolejnych lat.

[42] Zgodnie z oficjalną nomenklaturą budżetową.

[43] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie realizacji programów lub działań UE (dawne linie „BA”), pośrednie badania naukowe, bezpośrednie badania naukowe.

Linia budżetowa		(3)								
OGÓŁEM środki dla DG <…….>	Środki na zobowiązania	=1a+1b +3								
	Środki na płatności	=2a+2b +3								

• OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)								
	Środki na płatności	(5)								
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy		(6)								
OGÓŁEM środki na DZIAŁ <…> wieloletnich ram finansowych	Środki na zobowiązania	=4+6								
	Środki na płatności	=5+6								

<u>Jeżeli wpływ wniosku/inicjatywy nie ogranicza się do jednego działu operacyjnego, należy powtórzyć powyższą część:</u>

• OGÓŁEM środki operacyjne (wszystkie działy operacyjne)	Środki na zobowiązania	(4)								
	Środki na płatności	(5)								
OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy (wszystkie działy operacyjne)		(6)								
OGÓŁEM środki na DZIAŁY od 1 do 6 wieloletnich ram finansowych (kwota referencyjna)	Środki na zobowiązania	=4+6								
	Środki na płatności	=5+6								

Dział wieloletnich ram finansowych	**7**	„Wydatki administracyjne”

Niniejszą część uzupełnia się przy użyciu „danych budżetowych o charakterze administracyjnym”, które należy najpierw wprowadzić do załącznika do oceny skutków finansowych regulacji (załącznika V do przepisów wewnętrznych), przesyłanego do DECIDE w celu konsultacji pomiędzy służbami.

w mln EUR (do trzech miejsc po przecinku)

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
DG: CNECT						
• Zasoby ludzkie		1,030	1,030	1,030	1,030	**4,120**
• Pozostałe wydatki administracyjne		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
OGÓŁEM DG CNECT	Środki	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

w mln EUR (do trzech miejsc po przecinku)

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
OGÓŁEM środki na DZIAŁY od 1 do 7 wieloletnich ram finansowych	Środki na zobowiązania	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Środki na płatności	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Przewidywany produkt finansowany ze środków operacyjnych

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty ⇩			Rok **N**		Rok **N+1**		Rok **N+2**		Rok **N+3**		Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (zob. pkt 1.6)						**OGÓŁEM**	
	PRODUKTY																	
	Rodzaj[44]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[45]																		
– Produkt																		
– Produkt																		
– Produkt																		
Cel szczegółowy nr 1 – suma cząstkowa																		
CEL SZCZEGÓŁOWY nr 2 ...																		
– Produkt																		
Cel szczegółowy nr 2 – suma cząstkowa																		
OGÓŁEM																		

[44] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np.: liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[45] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	
DZIAŁ 7 wieloletnich ram finansowych					
Zasoby ludzkie	1,030	1,030	1,030	1,030	**4,120**
Pozostałe wydatki administracyjne	0,222	0,222	0,222	0,222	**0,888**
Suma cząstkowa DZIAŁU 7 wieloletnich ram finansowych	1,252	1,252	1,252	1,252	**5,008**

Poza DZIAŁEM 7[46] **wieloletnich ram finansowych**					
Zasoby ludzkie					
Pozostałe wydatki o charakterze administracyjnym					
Suma cząstkowa poza DZIAŁEM 7 wieloletnich ram finansowych					

OGÓŁEM	1,252	1,252	1,252	1,252	**5,008**

Potrzeby w zakresie środków na zasoby ludzkie i inne wydatki o charakterze administracyjnym zostaną pokryte z zasobów dyrekcji generalnej już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

[46] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

3.2.3.1. Szacowane zapotrzebowanie na zasoby ludzkie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich.

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**
20 01 02 01 (w centrali i w biurach przedstawicielstw Komisji)		6	6	6	6
20 01 02 03 (w delegaturach)					
01 01 01 01 (pośrednie badania naukowe)					
01 01 01 11 (bezpośrednie badania naukowe)					
Inne linie budżetowe (określić)					
•Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC)[47]					
20 02 01 (CA, SNE, INT z globalnej koperty finansowej)		1	1	1	1
20 02 03 (CA, LA, SNE, INT i JPD w delegaturach)					
XX 01 xx **yy zz** [48]	– w centrali				
	– w delegaturach				
01 01 01 02 (CA, SNE, INT – pośrednie badania naukowe)					
01 01 01 12 (CA, INT, SNE – bezpośrednie badania naukowe)					
Inne linie budżetowe (określić)					
OGÓŁEM		**7**	**7**	**7**	**7**

XX oznacza odpowiedni obszar polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony 6 EPC x 157 000 EUR/rok = 942 000 EUR	Zgodnie z opisem w pkt 2.2.1: – opracowanie zlecenia normalizacji lub wspólnych specyfikacji za pośrednictwem aktów wykonawczych w przypadku braku skutecznego procesu normalizacji; – opracowanie aktu delegowanego [w terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia] zawierającego definicje produktów krytycznych z elementami cyfrowymi; – ewentualne opracowanie aktów delegowanych w celu aktualizacji wykazu produktów krytycznych klasy I i II; określenie, czy konieczne jest ograniczenie lub wyłączenie w odniesieniu do produktów z elementami cyfrowymi objętych innymi przepisami unijnymi określającymi wymogi zapewniające taki sam poziom ochrony jak niniejsze rozporządzenie; wprowadzanie obowiązku certyfikacji niektórych produktów wysoce krytycznych z elementami cyfrowymi w oparciu o kryteria określone

[47] CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JPD = młodszy specjalista w delegaturze.

[48] W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA”).

	w niniejszym rozporządzeniu; określenie minimalnego zakresu deklaracji zgodności UE oraz uzupełnienie elementów, które należy uwzględnić w dokumentacji technicznej; – ewentualne opracowanie aktów wykonawczych w zakresie formatu lub elementów dotyczących obowiązków w zakresie zgłaszania incydentów, zestawienia podstawowych materiałów do produkcji oprogramowania, wspólnych specyfikacji lub umieszczania oznakowania CE; – ewentualne przygotowanie niezwłocznej interwencji w celu wprowadzenia w wyjątkowych okolicznościach środków naprawczych lub ograniczających w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego, w tym opracowanie aktu wykonawczego; – organizacja i koordynacja notyfikacji jednostek notyfikowanych przez państwa członkowskie oraz koordynacja jednostek notyfikowanych; – wspieranie koordynacji organów nadzoru rynku państw członkowskich.
Personel zewnętrzny 1 SNE x 88 000 EUR/rok	Zgodnie z opisem w pkt 2.2.1: – opracowanie zlecenia normalizacji lub wspólnych specyfikacji za pośrednictwem aktów wykonawczych w przypadku braku skutecznego procesu normalizacji; – opracowanie aktu delegowanego [w terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia] zawierającego definicje produktów krytycznych z elementami cyfrowymi; – ewentualne opracowanie aktów delegowanych w celu aktualizacji wykazu produktów krytycznych klasy I i II; określenie, czy konieczne jest ograniczenie lub wyłączenie w odniesieniu do produktów z elementami cyfrowymi objętych innymi przepisami unijnymi określającymi wymogi zapewniające taki sam poziom ochrony jak niniejsze rozporządzenie; wprowadzanie obowiązku certyfikacji niektórych produktów wysoce krytycznych z elementami cyfrowymi w oparciu o kryteria określone w niniejszym rozporządzeniu; określenie minimalnego zakresu deklaracji zgodności UE oraz uzupełnienie elementów, które należy uwzględnić w dokumentacji technicznej; – ewentualne opracowanie aktów wykonawczych w zakresie formatu lub elementów dotyczących obowiązków w zakresie zgłaszania incydentów, zestawienia podstawowych materiałów do produkcji oprogramowania, wspólnych specyfikacji lub umieszczania oznakowania CE; – ewentualne przygotowanie niezwłocznej interwencji w celu wprowadzenia w wyjątkowych okolicznościach środków naprawczych lub ograniczających w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego, w tym opracowanie aktu wykonawczego; – organizacja i koordynacja notyfikacji jednostek notyfikowanych przez państwa członkowskie oraz koordynacja jednostek notyfikowanych; – wspieranie koordynacji organów nadzoru rynku państw członkowskich.

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

Wniosek/inicjatywa:

– x może zostać w pełni sfinansowany(-a) przez przegrupowanie środków w ramach odpowiedniego działu wieloletnich ram finansowych (WRF).

Przeprogramowanie nie jest wymagane.

– ☐ wymaga zastosowania nieprzydzielonego marginesu środków w ramach odpowiedniego działu WRF lub zastosowania specjalnych instrumentów zdefiniowanych w rozporządzeniu w sprawie WRF.

–

– ☐ wymaga rewizji WRF.

–

3.2.5. Udział osób trzecich w finansowaniu

Wniosek/inicjatywa:

– x nie przewiduje współfinansowania ze strony osób trzecich

– ☐ przewiduje współfinansowanie ze strony osób trzecich szacowane zgodnie z poniższymi szacunkami:

Środki w mln EUR (do trzech miejsc po przecinku)

	Rok **N**[49]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (zob. pkt 1.6)			Ogółem
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

[49] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy. „N” należy zastąpić oczekiwanym pierwszym rokiem realizacji (np.: 2021). Tak samo należy postąpić dla kolejnych lat.

3.3. Szacunkowy wpływ na dochody

– ☐ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

– ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

  – ☐ wpływ na zasoby własne

  – ☐ wpływ na dochody inne

  – Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków ☐

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów:	Środki zapisane w budżecie na bieżący rok obrotowy	Wpływ wniosku/inicjatywy[50]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (zob. pkt 1.6)		
Artykuł …								

W przypadku wpływu na dochody przeznaczone na określony cel należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

Pozostałe uwagi (np. metoda/wzór użyte do obliczenia wpływu na dochody albo inne informacje).

[50] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 20 % na poczet kosztów poboru.