Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2024/2847

20.11.2024

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2024/2847

z dnia 23 października 2024 r.

w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności)

(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],

po konsultacji z Komitetem Regionów,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą [2],

a także mając na uwadze, co następuje:

(1) Cyberbezpieczeństwo jest dla Unii jednym z najpoważniejszych wyzwań. W nadchodzących latach liczba i różnorodność urządzeń podłączonych do internetu będzie gwałtownie rosnąć. Cyberataki stanowią kwestię interesu publicznego, ponieważ mają decydujący wpływ nie tylko na gospodarkę Unii, ale także na system demokratyczny, bezpieczeństwo konsumentów i zdrowie. Należy zatem koniecznie wzmocnić unijne podejście do cyberbezpieczeństwa, zająć się kwestią cyberodporności na poziomie unijnym oraz usprawnić funkcjonowanie rynku wewnętrznego poprzez ustanowienie jednolitych ram regulacyjnych obejmujących zasadnicze wymagania w zakresie cyberbezpieczeństwa dotyczące wprowadzania produktów z elementami cyfrowymi na rynek unijny. Należy rozwiązać dwa główne problemy, które narażają użytkowników i społeczeństwo na wyższe koszty: po pierwsze, niski poziom cyberbezpieczeństwa produktów z elementami cyfrowymi, który przejawia się w powszechnie występujących podatnościach oraz w niewystarczającym i niespójnym dostarczaniu aktualizacji zabezpieczeń w celu wyeliminowania tych podatności, a po drugie, niedostateczne zrozumienie i dostęp do informacji ze strony użytkowników, co uniemożliwia im wybór produktów o odpowiednich właściwościach w zakresie cyberbezpieczeństwa lub korzystanie z nich w bezpieczny sposób.

(2) Niniejsze rozporządzenie ma na celu stworzenie warunków brzegowych dla rozwoju bezpiecznych produktów z elementami cyfrowymi poprzez zadbanie o to, 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 branie pod uwagę cyberbezpieczeństwa przy wyborze produktów z elementami cyfrowymi i przy korzystaniu z nich, na przykład dzięki zwiększeniu przejrzystości w odniesieniu do okresu wsparcia dla produktów z elementami cyfrowymi udostępnionych na rynku.

(3) Odpowiednie obowiązujące prawo Unii obejmuje szereg zbiorów przepisów horyzontalnych, które pod różnym kątem odnoszą się do niektórych aspektów związanych z cyberbezpieczeństwem, w tym poprzez środki mające na celu poprawę bezpieczeństwa cyfrowego łańcucha dostaw. Obowiązujące prawo Unii dotyczące kwestii cyberbezpieczeństwa, w tym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 [3] oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 [4], bezpośrednio nie przewiduje jednak obowiązkowych wymagań w zakresie bezpieczeństwa produktów z elementami cyfrowymi.

---

[1] Dz.U. C 100 z 16.3.2023, s. 101.

[2] Stanowisko Parlamentu Europejskiego z dnia 12 marca 2024 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 10 października 2024 r.

[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] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

(4) Chociaż obowiązujące prawo Unii ma zastosowanie do niektórych produktów z elementami cyfrowymi, nie istnieją horyzontalne unijne ramy regulacyjne ustanawiające wszechstronne wymagania w zakresie cyberbezpieczeństwa dotyczące wszystkich produktów z elementami cyfrowymi. Różne akty przyjęte dotychczas na poziomie unijnym i krajowym oraz różne unijne i krajowe inicjatywy jedynie częściowo rozwiązują zidentyfikowane 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 nałożeniem na przedsiębiorstwa i organizacje niepotrzebnych obciążeń związanych z przestrzeganiem szeregu wymagań i wypełnianiem szeregu obowiązków dotyczących podobnych rodzajów produktów. Cyberbezpieczeństwo tych produktów ma szczególnie wyraźny wymiar transgraniczny, ponieważ produkty z elementami cyfrowymi wytwarzane w jednym państwie członkowskim lub państwie trzecim są często wykorzystywane przez organizacje i konsumentów na całym rynku wewnętrznym. W związku z tym konieczne jest uregulowanie tej kwestii na poziomie Unii, aby zadbać o zharmonizowane ramy regulacyjne i pewność prawa dla użytkowników, organizacji i przedsiębiorstw, w tym mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw zdefiniowanych w załączniku do zalecenia Komisji 2003/361/WE ([5]). Należy zharmonizować unijne otoczenie regulacyjne poprzez wprowadzenie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi. Należy ponadto zagwarantować pewność prawa podmiotom gospodarczym i użytkownikom w całej Unii, a także zapewnić lepszą harmonizację rynku wewnętrznego oraz zagwarantować proporcjonalność mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom, co przełoży się na dogodniejsze warunki dla podmiotów gospodarczych zamierzających wejść na ten rynek.

(5) W odniesieniu do mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, określając kategorię, do której należy dane przedsiębiorstwo, należy w całości stosować przepisy załącznika do zalecenia 2003/361/WE. W związku z tym przy wyliczaniu liczby pracowników i pułapów finansowych definiujących kategorie przedsiębiorstw należy również stosować przepisy art. 6 załącznika do zalecenia 2003/361/WE dotyczące ustalania danych przedsiębiorstwa z uwzględnieniem szczególnych rodzajów przedsiębiorstw, takich jak przedsiębiorstwa partnerskie lub przedsiębiorstwa powiązane.

(6) Komisja powinna wydać wytyczne, aby pomóc podmiotom gospodarczym, w szczególności mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom, w stosowaniu niniejszego rozporządzenia. Takie wytyczne powinny obejmować między innymi zakres niniejszego rozporządzenia, w szczególności zdalne przetwarzanie danych i jego skutki dla twórców wolnego i otwartego oprogramowania, stosowanie kryteriów służących do określania długości okresów wsparcia dla produktów z elementami cyfrowymi, wzajemne powiązania między niniejszym rozporządzeniem a innymi przepisami prawa Unii, a także pojęcie istotnej modyfikacji.

(7) Na poziomie Unii – w różnych dokumentach programowych i politycznych, takich jak wspólny komunikat Komisji i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 16 grudnia 2020 r. pt. „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę", konkluzje Rady z dnia 2 grudnia 2020 r. w sprawie cyberbezpieczeństwa urządzeń podłączonych do internetu oraz z dnia 23 maja 2022 r. w sprawie rozwoju pozycji Unii Europejskiej w cyberprzestrzeni, a także rezolucja Parlamentu Europejskiego z dnia 10 czerwca 2021 r. w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę ([6]) – wezwano do wprowadzenia konkretnych unijnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów cyfrowych lub skomunikowanych, jako że wiele państw trzecich z własnej inicjatywy wprowadziło środki mające na celu zajęcie się tą kwestią. W sprawozdaniu z wyników końcowych Konferencji w sprawie przyszłości Europy obywatele wezwali do zwiększenia roli UE w przeciwdziałaniu zagrożeniom cyberbezpieczeństwa. Aby w dziedzinie cyberbezpieczeństwa Unia mogła odgrywać pierwszoplanową rolę na arenie międzynarodowej, należy ustanowić ambitne ramy regulacyjne.

(8) Aby zwiększyć ogólny poziom cyberbezpieczeństwa wszystkich produktów z elementami cyfrowymi wprowadzanych na rynek wewnętrzny, należy ustanowić stosowane horyzontalnie, ukierunkowane na cel i neutralne technologicznie zasadnicze wymagania w zakresie cyberbezpieczeństwa dotyczące tych produktów.

(9) 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 zapewniać, aby wszystkie produkty z elementami cyfrowymi były projektowane i opracowywane zgodnie z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu. Ten obowiązek dotyczy 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 cyberzagrożenia 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 produktów z elementami cyfrowymi, które są jedynie pośrednio połączone z innymi urządzeniami lub sieciami.

([5]) Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

([6]) Dz.U. C 67 z 8.2.2022, s. 81.

(10) Ustanowienie wymagań w zakresie cyberbezpieczeństwa dotyczących wprowadzania do obrotu produktów z elementami cyfrowymi ma na celu zwiększenie cyberbezpieczeństwa tych produktów, zarówno z myślą o konsumentach, jak i o przedsiębiorstwach. Wymagania te zagwarantują również uwzględnienie cyberbezpieczeństwa w całych łańcuchach dostaw, dzięki czemu produkty końcowe z elementami cyfrowymi i ich komponenty będą bezpieczniejsze. Obejmuje to również wymagania dotyczące wprowadzania do obrotu produktów konsumenckich z elementami cyfrowymi przeznaczonych dla konsumentów podatnych na zagrożenia, na przykład zabawek i elektronicznych niań. Produkty konsumenckie z elementami cyfrowymi sklasyfikowane w niniejszym rozporządzeniu jako ważne produkty z elementami cyfrowymi niosą ze sobą większe ryzyko w cyberprzestrzeni, ponieważ pełnią funkcję, która wiąże się ze znacznym ryzykiem negatywnych skutków pod względem intensywności i zdolności do szkodzenia zdrowiu, bezpieczeństwu lub ochronie użytkowników takich produktów, w związku z czym powinny podlegać bardziej rygorystycznej procedurze oceny zgodności. Dotyczy to takich produktów jak inteligentne urządzenia domowe z funkcjami bezpieczeństwa, w tym inteligentne zamki do drzwi, nianie elektroniczne i systemy alarmowe, zabawki podłączone do internetu oraz technologie medyczne do noszenia na ciele. Ponadto bardziej rygorystyczne procedury oceny zgodności, którym muszą podlegać inne produkty z elementami cyfrowymi sklasyfikowane w niniejszym rozporządzeniu jako ważne lub krytyczne produkty z elementami cyfrowymi, przyczynią się do przeciwdziałania potencjalnym negatywnym skutkom wykorzystywania podatności zagrażającym konsumentom.

(11) Celem niniejszego rozporządzenia jest zapewnienie wysokiego poziomu cyberbezpieczeństwa produktów z elementami cyfrowymi i zintegrowanych z nimi rozwiązań w zakresie zdalnego przetwarzania danych. Takie rozwiązania w zakresie zdalnego przetwarzania danych powinny być zdefiniowane jako przetwarzanie danych na odległość, na potrzeby którego oprogramowanie zostało zaprojektowane i opracowane przez producenta danego produktu z elementami cyfrowymi lub w jego imieniu, a którego brak spowodowałby, że produkt z elementami cyfrowymi nie mógłby pełnić jednej ze swoich funkcji. Podejście to gwarantuje, że takie produkty są w całości odpowiednio zabezpieczone przez producentów, niezależnie od tego, czy dane są przetwarzane lub przechowywane lokalnie na urządzeniu użytkownika, czy zdalnie przez producenta. Jednocześnie zdalne przetwarzanie lub przechowywanie wchodzi w zakres niniejszego rozporządzenia tylko w takim zakresie, w jakim jest to konieczne, aby produkt z elementami cyfrowymi pełnił swoje funkcje. Takie zdalne przetwarzanie lub przechowywanie obejmuje sytuację, w której aplikacja mobilna wymaga dostępu do interfejsu programowania aplikacji lub do bazy danych, dostarczanych w formie usługi oferowanej przez producenta. W takim przypadku usługa ta wchodzi w zakres niniejszego rozporządzenia jako rozwiązanie w zakresie zdalnego przetwarzania danych. Wymagania dotyczące objętych zakresem niniejszego rozporządzenia rozwiązań w zakresie zdalnego przetwarzania danych nie wiążą się zatem ze środkami technicznymi, operacyjnymi ani organizacyjnymi mającymi na celu zarządzanie ryzykiem dla bezpieczeństwa całości sieci i systemów informatycznych producenta.

(12) Rozwiązania w chmurze stanowią rozwiązania w zakresie zdalnego przetwarzania danych w rozumieniu niniejszego rozporządzenia tylko wtedy, gdy są zgodne z definicją zawartą w niniejszym rozporządzeniu. Na przykład w zakres niniejszego rozporządzenia wchodzą funkcjonalności oparte na chmurze zapewniane przez producenta inteligentnych urządzeń domowych, umożliwiające użytkownikom sterowanie urządzeniem na odległość. Natomiast strony internetowe, które nie obsługują funkcjonalności produktów z elementami cyfrowymi, lub usługi w chmurze zaprojektowane i opracowane poza zakresem odpowiedzialności producenta produktu z elementami cyfrowymi, nie są objęte zakresem niniejszego rozporządzenia. Do usług w chmurze i modeli świadczenia usług w chmurze, takich jak oprogramowanie jako usługa (SaaS), platforma jako usługa (PaaS) lub infrastruktura jako usługa (IaaS), ma zastosowanie dyrektywa (UE) 2022/2555. Zakresem stosowania tej dyrektywy są objęte podmioty świadczące w Unii usługi w chmurze, które zgodnie z art. 2 załącznika do zalecenia 2003/361/WE zaliczają się do średnich przedsiębiorstw lub przekraczają pułapy dla średnich przedsiębiorstw przewidziane w ust. 1 tego artykułu.

(13) Zgodnie z celem niniejszego rozporządzenia, jakim jest wyeliminowanie przeszkód w swobodnym przepływie produktów z elementami cyfrowymi, państwa członkowskie nie powinny – w odniesieniu do kwestii objętych zakresem niniejszego rozporządzenia – utrudniać udostępniania na rynku produktów z elementami cyfrowymi spełniających wymagania zawarte w niniejszym rozporządzeniu. W związku z tym w kwestiach zharmonizowanych niniejszym rozporządzeniem państwa członkowskie nie mogą nakładać dodatkowych wymagań w zakresie cyberbezpieczeństwa w związku z udostępnianiem na rynku produktów z elementami cyfrowymi dodatkowymi. Każdy podmiot, publiczny lub prywatny, może jednak ustanowić wymagania dodatkowe w stosunku do wymagań określonych w niniejszym rozporządzeniu w odniesieniu do zamówień na produkty z elementami cyfrowymi lub względem wykorzystywania ich do konkretnych celów, a zatem może zdecydować się na wykorzystywanie produktów z elementami cyfrowymi, które spełniają bardziej rygorystyczne lub bardziej szczegółowe wymagania w zakresie cyberbezpieczeństwa niż wymagania mające zastosowanie do udostępniania na rynku na podstawie niniejszego rozporządzenia. Bez uszczerbku dla dyrektyw Parlamentu Europejskiego i Rady 2014/24/UE ([7]) i 2014/25/UE ([8]) w kontekście udzielania zamówień na produkty z elementami cyfrowymi, które muszą spełniać zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzeniu, w tym wymagania

([7]) Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).

([8]) Dyrektywa Parlamentu Europejskiego i Rady 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca dyrektywę 2004/17/WE (Dz. U. L 94 z 28.3.2014, s. 243).

dotyczące postępowania w przypadku wykrycia podatności, państwa członkowskie powinny zadbać o uwzględnianie takich wymagań w procesie udzielania zamówień oraz o uwzględnianie zdolności producentów do skutecznego stosowania środków z zakresu cyberbezpieczeństwa i zarządzania cyberzagrożeniami. Ponadto w dyrektywie (UE) 2022/2555 określono środki zarządzania ryzykiem w cyberprzestrzeni dla podmiotów kluczowych i ważnych, o których mowa w art. 3 tej dyrektywy, mogące obejmować środki na rzecz bezpieczeństwa łańcucha dostaw wymagające stosowania przez takie podmioty produktów z elementami cyfrowymi spełniających bardziej rygorystyczne wymagania w zakresie cyberbezpieczeństwa niż te określone w niniejszym rozporządzeniu. Zgodnie z dyrektywą (UE) 2022/2555 i określoną w niej zasadą minimalnej harmonizacji państwa członkowskie mogą zatem nakładać dodatkowe wymagania w zakresie cyberbezpieczeństwa dotyczące wykorzystywania produktów technologii informacyjno-komunikacyjnych (ICT) przez podmioty kluczowe lub ważne na podstawie tej dyrektywy, aby zapewnić wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie wymagania będą zgodne z obowiązkami państw członkowskich określonymi w prawie Unii. Kwestie nieobjęte niniejszym rozporządzeniem mogą obejmować czynniki pozatechniczne odnoszące się do produktów z elementami cyfrowymi i ich producentów. Państwa członkowskie mogą zatem ustanowić środki krajowe, w tym ograniczenia dotyczące produktów z elementami cyfrowymi lub dostawców takich produktów, uwzględniające czynniki pozatechniczne. Środki krajowe dotyczące takich czynników muszą być zgodne z prawem Unii.

(14) Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla obowiązków państw członkowskich w zakresie ochrony bezpieczeństwa narodowego zgodnie z prawem Unii. Państwa członkowskie powinny mieć możliwość objęcia produktów z elementami cyfrowymi, które są zamawiane lub wykorzystywane do celów bezpieczeństwa narodowego lub obronności, dodatkowymi środkami, pod warunkiem że takie środki będą zgodne z obowiązkami państw członkowskich określonymi w prawie Unii.

(15) Niniejsze rozporządzenie ma zastosowanie do podmiotów gospodarczych wyłącznie w powiązaniu z produktami z elementami cyfrowymi udostępnianymi na rynku, a zatem dostarczanymi w celu dystrybucji lub w celu wykorzystywania na rynku unijnym w ramach działalności handlowej. Dostarczanie w ramach działalności handlowej może obejmować nie tylko pobieranie zapłaty za produkty z elementami cyfrowymi, ale również pobieranie opłaty za usługi wsparcia technicznego, gdy nie służy to wyłącznie odzyskaniu rzeczywistych kosztów, działanie z zamiarem monetyzacji, np. poprzez udostępnianie platformy oprogramowania, za pośrednictwem której producent zarabia na innych usługach, wymaganie jako warunku wykorzystywania przetwarzania danych osobowych z powodów innych niż tylko poprawa bezpieczeństwa, kompatybilności lub interoperacyjności oprogramowania lub przyjmowanie darowizn przekraczających koszty wynikające z zaprojektowania, opracowania i dostarczenia produktów z elementami cyfrowymi. Przyjmowanie darowizn bez zamiaru osiągnięcia zysku nie powinno być uznawane za działalność handlową.

(16) Dostarczania produktów z elementami cyfrowymi w ramach świadczenia usługi, za którą opłata jest pobierana wyłącznie w celu odzyskania rzeczywistych kosztów bezpośrednio związanych ze świadczeniem tej usługi, na przykład w przypadku niektórych produktów z elementami cyfrowymi dostarczanych przez podmioty administracji publicznej, nie należy uznawać za działalność handlową do celów niniejszego rozporządzenia wyłącznie na tej podstawie. Ponadto opracowywania lub modyfikowania produktów z elementami cyfrowymi przez podmiot administracji publicznej wyłącznie na własny użytek nie należy uznawać za udostępniane na rynku w rozumieniu niniejszego rozporządzenia.

(17) Ogólnodostępne oprogramowanie i dane lub ich zmodyfikowane wersje, do których użytkownicy mogą bezpłatnie uzyskiwać dostęp, z których mogą korzystać i które mogą modyfikować i rozpowszechniać, mogą przyczynić się do badań naukowych i innowacji na rynku. Aby wesprzeć rozwój i rozpowszechnianie wolnego i otwartego oprogramowania, w szczególności przez mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, w tym przedsiębiorstwa typu start-up, osoby fizyczne, organizacje nienastawione na zysk i akademickie organizacje badawcze, zakres stosowania niniejszego rozporządzenia w stosunku do produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie, dostarczanych w ramach działalności handlowej w celu dystrybucji lub wykorzystywania, powinien uwzględniać charakter różnych modeli opracowywania oprogramowania dystrybuowanego i tworzonego z wykorzystaniem licencji na wolne i otwarte oprogramowanie.

(18) Przez wolne i otwarte oprogramowanie rozumie się oprogramowanie, którego kod źródłowy jest ogólnie dostępny i którego licencja zapewnia wszystkim prawo do bezpłatnego dostępu do niego, używania go, modyfikowania i redystrybucji. Wolne i otwarte oprogramowanie jest opracowywane, utrzymywane i dystrybuowane jako ogólnodostępne, w tym za pośrednictwem platform internetowych. W odniesieniu do podmiotów gospodarczych objętych zakresem stosowania niniejszego rozporządzenia zakresem stosowania niniejszego rozporządzenia powinno być objęte wyłącznie wolne i otwarte oprogramowanie udostępniane na rynku, a zatem dostarczane w ramach działalności handlowej w celu dystrybucji lub wykorzystywania. Przy określaniu handlowego lub niehandlowego charakteru działalności nie należy zatem brać pod uwagę samych tylko okoliczności, w jakich produkt z elementami cyfrowymi został opracowany, ani sposobu, w jaki jego opracowanie zostało sfinansowane. Dokładniej rzecz ujmując, do celów niniejszego rozporządzenia i w odniesieniu do podmiotów gospodarczych objętych jego zakresem, aby zapewnić wyraźne rozróżnienie między etapami opracowywania i dostarczania,

dostarczanie produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie, które nie są monetyzowane przez ich producentów, nie powinno być uznawane za działalność handlową. Ponadto dostarczanie produktów z elementami cyfrowymi kwalifikujących się jako komponenty wolnego i otwartego oprogramowania przeznaczone do wbudowania przez innych producentów do ich własnych produktów z elementami cyfrowymi powinno być uznawane za udostępnianie na rynku tylko wtedy, gdy pierwotny producent monetyzuje dany komponent. Na przykład sam fakt, że produkt z elementami cyfrowymi będący otwartym oprogramowaniem jest wspierany finansowo przez producentów lub że producenci uczestniczą w opracowywaniu takiego produktu, nie powinien sam w sobie przesądzać o tym, że działalność ta ma charakter handlowy. Również regularne wydawanie nowych wersji nie powinno samo w sobie prowadzić do wniosku, że produkt z elementami cyfrowymi jest dostarczany w ramach działalności handlowej. Wreszcie do celów niniejszego rozporządzenia opracowywanie przez organizacje nienastawione na zysk produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie nie powinno być uznawane za działalność handlową pod warunkiem że dana organizacja została założona w formie, która gwarantuje wykorzystanie całego zysku po odjęciu kosztów do osiągnięcia celów nienastawionych na zysk. Niniejsze rozporządzenie nie ma zastosowania do osób fizycznych lub prawnych, które tworzą kod źródłowy dla produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie poza ich zakresem odpowiedzialności.

(19) Biorąc pod uwagę, że wiele produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie, które publikuje się, lecz nie udostępnia na rynku w rozumieniu niniejszego rozporządzenia, ma duże znaczenie dla cyberbezpieczeństwa, osoby prawne, które trwale wspierają rozwój takich produktów, które są przeznaczone do celów działalności handlowej, i które to osoby odgrywają główną rolę w gwarantowaniu opłacalności tych produktów (opiekuni otwartego oprogramowania), powinny podlegać mniej restrykcyjnemu i dostosowanemu do potrzeb systemowi regulacyjnemu. Opiekuni otwartego oprogramowania to m.in. niektóre fundacje oraz podmioty, które opracowują i publikują wolne i otwarte oprogramowanie w kontekście biznesowym, w tym podmioty nienastawione na zysk. System regulacyjny powinien uwzględniać ich szczególny charakter i zgodność z rodzajem nakładanych obowiązków. Powinien on obejmować wyłącznie produkty z elementami cyfrowymi kwalifikujące się jako wolne i otwarte oprogramowanie, które ostatecznie są przeznaczone do celów działalności handlowej, np. do wykorzystania w usługach komercyjnych lub w monetyzowanych produktach z elementami cyfrowymi. Do celów tego systemu regulacyjnego zamiar wykorzystania w monetyzowanych produktach z elementami cyfrowymi obejmuje przypadki, w których producenci wbudowujący dany komponent do własnych produktów z elementami cyfrowymi albo regularnie przyczyniają się do rozwoju tego komponentu, albo udzielają regularnego wsparcia finansowego, aby zapewnić ciągłość istnienia oprogramowania. Udzielanie stałego wsparcia na rzecz rozwoju produktu z elementami cyfrowymi obejmuje między innymi hosting platform współpracy, na których opracowywane jest oprogramowanie, i zarządzanie tymi platformami, hosting kodu źródłowego lub oprogramowania, zarządzanie lub gospodarowanie produktami z elementami cyfrowymi kwalifikującymi się jako wolne i otwarte oprogramowanie, a także kierowanie opracowywaniem takich produktów. Biorąc pod uwagę, że mniej restrykcyjny i dostosowany do potrzeb system regulacyjny nie nakłada na tych, którzy działają jak opiekunowie otwartego oprogramowania, takich samych obowiązków jak te, które spoczywają na mocy niniejszego rozporządzenia na tych, którzy działają jak producenci, opiekunom nie należy zezwalać na umieszczanie oznakowania CE na produktach z elementami cyfrowymi, których opracowywanie wspierają.

(20) Hosting produktów z elementami cyfrowymi w otwartych repozytoriach, w tym poprzez systemy zarządzania pakietami lub na platformach współpracy, nie stanowi sam w sobie udostępniania na rynku produktów z elementami cyfrowymi. Dostawców takich usług należy uznawać za dystrybutorów wyłącznie wtedy, gdy udostępniają takie oprogramowanie na rynku, a tym samym w ramach działalności handlowej dostarczają je do dystrybucji lub wykorzystywania na rynku unijnym.

(21) Aby wspierać i ułatwiać należytą staranność producentów, którzy wbudowują do swoich produktów z elementami cyfrowymi komponenty będące wolnym i otwartym oprogramowaniem, a niepodlegające zasadniczym wymaganiom w zakresie cyberbezpieczeństwa określonym w niniejszym rozporządzeniu, Komisja powinna mieć możliwość ustanowienia dobrowolnych programów poświadczania bezpieczeństwa w drodze aktu delegowanego uzupełniającego niniejsze rozporządzenie albo w drodze zwrócenia się na podstawie art. 48 rozporządzenia (UE) 2019/881 z wnioskiem o europejski system certyfikacji cyberbezpieczeństwa, który uwzględni specyfikę modeli opracowywania wolnego i otwartego oprogramowania. Programy poświadczania bezpieczeństwa powinny być opracowane w taki sposób, aby poświadczenie bezpieczeństwa mogły inicjować lub finansować nie tylko osoby fizyczne lub prawne opracowujące lub przyczyniające się do opracowania produktu z elementami cyfrowymi kwalifikującego się jako wolne i otwarte oprogramowanie, ale również osoby trzecie, takie jak producenci, którzy wbudowują takie produkty do własnych produktów z elementami cyfrowymi, użytkownicy lub unijne i krajowe administracje publiczne.

(22) Z uwagi na cele niniejszego rozporządzenia w kwestii cyberbezpieczeństwa publicznego oraz w trosce o zwiększenie orientacji sytuacyjnej państw członkowskich co do zależności Unii od komponentów oprogramowania, a szczególnie od komponentów będących potencjalnie wolnym i otwartym oprogramowaniem, specjalna grupa współpracy administracyjnej (ADCO) ustanowiona niniejszym rozporządzeniem powinna mieć możliwość podjęcia decyzji o wspólnym przeprowadzeniu oceny zależności Unii. Organy nadzoru rynku powinny mieć możliwość zwrócenia się do producentów kategorii produktów z elementami cyfrowymi określonych przez ADCO o przedłożenie zestawień podstawowych materiałów do produkcji oprogramowania, wygenerowanych na podstawie niniejszego rozporządzenia. W trosce o ochronę poufności zestawień podstawowych materiałów do produkcji oprogramowania organy nadzoru rynku powinny przekazywać ADCO istotne informacje o zależności w sposób zanonimizowany i zagregowany.

(23) Skuteczność wdrażania niniejszego rozporządzenia będzie również zależała od dostępności odpowiednich umiejętności w zakresie cyberbezpieczeństwa. Na poziomie Unii w różnych dokumentach programowych i politycznych, w tym w komunikacie Komisji z dnia 18 kwietnia 2023 r. pt. „Wyeliminowanie niedoboru talentów w dziedzinie cyberbezpieczeństwa w celu zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE" oraz w konkluzjach Rady z dnia 22 maja 2023 r. w sprawie polityki UE w zakresie cyberobrony, dostrzeżono brak umiejętności w dziedzinie cyberbezpieczeństwa w Unii oraz potrzebę stawienia czoła takim wyzwaniom w pierwszej kolejności, zarówno w sektorze publicznym, jak i prywatnym. W trosce o skuteczne wdrożenie niniejszego rozporządzenia państwa członkowskie powinny zapewnić dostępność wystarczających zasobów na potrzeby naboru odpowiedniego personelu w organach nadzoru rynku i w jednostkach oceniających zgodność, aby mogły one wykonywać zadania określone w niniejszym rozporządzeniu. Środki te powinny zwiększyć mobilność siły roboczej w dziedzinie cyberbezpieczeństwa i uatrakcyjnić związane z nią ścieżki kariery. Powinny one również sprawić, że siła robocza w dziedzinie cyberbezpieczeństwa będzie bardziej odporna i zróżnicowana, również pod względem płci. Państwa członkowskie powinny zatem podjąć kroki, aby zapewnić, że zadania te będą wykonywane przez odpowiednio wyszkolonych specjalistów posiadających niezbędne umiejętności w dziedzinie cyberbezpieczeństwa. Analogicznie producenci powinni zapewniać, by ich personel posiadał umiejętności niezbędne do wywiązywania się z obowiązków określonych w niniejszym rozporządzeniu. Państwa członkowskie i Komisja, zgodnie ze swoimi prerogatywami i kompetencjami oraz ze szczególnymi zadaniami powierzonymi im na mocy niniejszego rozporządzenia, powinny podjąć środki wspierające producentów, a w szczególności mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, w tym przedsiębiorstwa typu start-up, również w obszarach takich jak rozwój umiejętności, aby mogły wywiązywać się z obowiązków określonych w niniejszym rozporządzeniu. Ponadto, ponieważ dyrektywa (UE) 2022/2555 zobowiązuje państwa członkowskie do przyjęcia w ramach ich krajowych strategii cyberbezpieczeństwa polityk promujących i rozwijających szkolenia w dziedzinie cyberbezpieczeństwa oraz umiejętności z zakresu cyberbezpieczeństwa, przyjmując takie strategie, państwa członkowskie mogą ponadto rozważyć uwzględnienie zapotrzebowania na umiejętności z zakresu cyberbezpieczeństwa wynikające z niniejszego rozporządzenia, w tym potrzeb co do przekwalifikowania i podnoszenia kwalifikacji.

(24) Bezpieczny internet jest niezbędny do funkcjonowania infrastruktury krytycznej i potrzebny całemu społeczeństwu. Celem dyrektywy (UE) 2022/2555 jest zapewnienie wysokiego poziomu cyberbezpieczeństwa usług świadczonych przez podmioty kluczowe i ważne, o których mowa w art. 3 tej dyrektywy, 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 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 (UE) 2022/2555 poprzez zadbanie o to, 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.

(25) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 ([9]) ustanawia przepisy dotyczące wyrobów medycznych, a rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 ([10]) ustanawia przepisy dotyczące wyrobów medycznych do diagnostyki in vitro. Te rozporządzenia dotyczą ryzyka w cyberprzestrzeni i zastosowano w nich szczególne podejścia, do których odniesiono się również w niniejszym rozporządzeniu. Konkretnie w rozporządzeniach (UE) 2017/745 i (UE) 2017/746 określono zasadnicze wymagania 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. Wymagania te zobowiązują producentów do opracowywania i tworzenia produktów z zastosowaniem zasad zarządzania ryzykiem oraz w ramach podejścia obejmującego określenie wymagań dotyczących środków bezpieczeństwa IT, jak również odpowiednich procedur oceny zgodności. Ponadto od grudnia 2019 r. obowiązują szczegółowe wytyczne w zakresie cyberbezpieczeństwa wyrobów medycznych, w których udzielono producentom wyrobów medycznych, w tym wyrobów do diagnostyki in vitro, wskazówek, jak spełnić wszystkie odpowiednie zasadnicze wymagania w odniesieniu do cyberbezpieczeństwa określone w załączniku I do każdego z tych rozporządzeń. Produkty z elementami cyfrowymi, do których zastosowanie ma którekolwiek z tych rozporządzeń, nie powinny zatem podlegać niniejszemu rozporządzeniu.

(26) W zakres niniejszego rozporządzenia nie wchodzą produkty z elementami cyfrowymi opracowane lub zmodyfikowane wyłącznie do celów bezpieczeństwa narodowego lub obronności ani produkty specjalnie zaprojektowane do przetwarzania informacji niejawnych. Zachęca się państwa członkowskie do zapewnienia takiego samego lub wyższego poziomu ochrony tych produktów jak w przypadku produktów objętych zakresem niniejszego rozporządzenia.

([9]) 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).

([10]) 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).

(27) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/2144 ([11]) ustanawia wymogi dotyczące homologacji typu pojazdów oraz ich układów i komponentów, wprowadza pewne wymogi w zakresie 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, w szczególności z Regulaminem ONZ nr 155 – Jednolite przepisy dotyczące homologacji pojazdów w zakresie cyberbezpieczeństwa i systemu zarządzania bezpieczeństwem ([12]), a także przewiduje określone procedury oceny zgodności. W obszarze lotnictwa głównym celem rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 ([13]) 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 ujęto również obowiązki w zakresie ochrony przed zagrożeniami dla bezpieczeństwa informacji. Proces certyfikacji na mocy rozporządzenia (UE) 2018/1139 gwarantuje poziom pewności, który jest również celem niniejszego rozporządzenia. Produkty z elementami cyfrowymi, do których zastosowanie ma rozporządzenie (UE) 2019/2144, oraz produkty certyfikowane zgodnie z rozporządzeniem (UE) 2018/1139 nie powinny zatem podlegać zasadniczym wymaganiom w zakresie cyberbezpieczeństwa i procedurom oceny zgodności określonym w niniejszym rozporządzeniu.

(28) W niniejszym rozporządzeniu ustanawia się horyzontalne przepisy w zakresie cyberbezpieczeństwa, które nie ograniczają się do konkretnych sektorów czy do 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 wymaganiami w zakresie cyberbezpieczeństwa 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 wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu może zostać ograniczone lub podlegać wyłączeniu, jeżeli takie ograniczenie lub wyłączenie jest spójne z ogólnymi ramami regulacyjnymi mającymi zastosowanie do tych produktów i jeżeli przepisy sektorowe zapewniają co najmniej taki sam poziom ochrony jak ten przewidziany w niniejszym rozporządzeniu. Komisja jest uprawniona do przyjmowania aktów delegowanych w celu uzupełnienia niniejszego rozporządzenia poprzez wskazanie takich produktów i przepisów. Niniejsze rozporządzenie zawiera przepisy szczegółowe precyzujące jego powiązania z obowiązującym prawem Unii, do którego należy stosować takie ograniczenia lub wyłączenia.

(29) W trosce o możliwość skutecznej naprawy udostępnionych na rynku produktów z elementami cyfrowymi i przedłużenia ich trwałości należy przewidzieć odstępstwo w zakresie części zamiennych. To odstępstwo powinno dotyczyć zarówno części zamiennych służących do naprawy starszych produktów udostępnionych przed datą rozpoczęcia stosowania niniejszego rozporządzenia, jak i części zamiennych, które zostały już poddane procedurze oceny zgodności na podstawie niniejszego rozporządzenia.

(30) Rozporządzenie delegowane Komisji (UE) 2022/30 ([14]) stanowi, że do niektórych urządzeń radiowych zastosowanie ma szereg zasadniczych wymagań określonych w art. 3 ust. 3 lit. d), e) i f) dyrektywy Parlamentu Europejskiego i Rady 2014/53/UE ([15]), dotyczących niepożądanego wpływu na sieć, wykorzystania zasobów sieciowych w nieodpowiedni sposób, danych osobowych i prywatności oraz oszustw. W decyzji wykonawczej Komisji C (2022) 5637 z dnia 5 sierpnia 2022 r. w sprawie wniosku o normalizację skierowanego do Europejskiego Komitetu Normalizacyjnego oraz do Europejskiego Komitetu Normalizacyjnego Elektrotechniki ustanowiono wymogi dotyczące opracowania konkretnych norm doprecyzowujących sposób, w jaki należy podejść do tych zasadniczych wymagań. Zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzeniu obejmują wszystkie elementy zasadniczych wymagań, o których mowa w art. 3 ust. 3 lit. d), e) i f) dyrektywy

([11]) 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).

([12]) Dz.U. L 82 z 9.3.2021, s. 30.

([13]) 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).

([14]) Rozporządzenie delegowane Komisji (UE) 2022/30 z dnia 29 października 2021 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2014/53/UE w odniesieniu do stosowania zasadniczych wymagań, o których mowa w art. 3 ust. 3 lit. d), e) i f) tej dyrektywy (Dz.U. L 7 z 12.1.2022, s. 6).

([15]) Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.U. L 153 z 22.5.2014, s. 62).

2014/53/UE. Co więcej, zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzeniu są zgodne z celami wymogów dotyczących określonych norm zawartych w tym wniosku o normalizację. Ponadto gdy 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 C(2022) 5637 przy przygotowywaniu i opracowywaniu norm zharmonizowanych w celu ułatwienia wykonania niniejszego rozporządzenia. W okresie przejściowym stosowania niniejszego rozporządzenia Komisja powinna wydać wytyczne dla producentów podlegających niniejszemu rozporządzeniu, którzy podlegają również rozporządzeniu delegowanemu (UE) 2022/30, aby ułatwić im wykazywanie zgodności z tymi dwoma rozporządzeniami.

(31) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/2853 ([16]) ma charakter uzupełniający w stosunku do niniejszego rozporządzenia. W dyrektywie tej określono przepisy dotyczące odpowiedzialności za produkty wadliwe, tak aby osoby poszkodowane mogły dochodzić rekompensaty 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 dostarczania takich aktualizacji zabezpieczeń.

(32) Niniejsze rozporządzenie nie powinno naruszać przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([17]), w tym przepisów dotyczących ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń dotyczących ochrony danych mających świadczyć o zgodności z tym rozporządzeniem prowadzonych przez administratorów i podmioty przetwarzające operacji przetwarzania. Takie operacje mogą być dokonywane w produktach z elementami cyfrowymi. Najważniejsze elementy rozporządzenia (UE) 2016/679 to uwzględnianie ochrony danych w fazie projektowania, domyślna ochrona danych i ogólnie pojęte cyberbezpieczeństwo. Dzięki zapewnieniu ochrony konsumentów i organizacji przed ryzykiem w cyberprzestrzeni ustanowione w niniejszym rozporządzeniu zasadnicze wymagania w zakresie cyberbezpieczeństwa mają się też przyczynić do lepszej ochrony danych osobowych i prywatności osób fizycznych. Należy rozważyć możliwości synergii zarówno w obszarze normalizacji, jak i certyfikacji poszczególnych 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 stosowanie unijnych przepisów o ochronie danych. Te ostatnie powinny także mieć dostęp do informacji istotnych dla realizacji ich zadań.

(33) W zakresie, w jakim ich produkty wchodzą w zakres niniejszego rozporządzenia, dostawcy europejskich portfeli tożsamości cyfrowej, o których mowa w art. 5a ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([18]), powinni przestrzegać zarówno horyzontalnych zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w niniejszym rozporządzeniu, jak i szczególnych wymogów bezpieczeństwa określonych w art. 5a rozporządzenia (UE) nr 910/2014. Aby ułatwić zapewnienie zgodności, dostawcom portfeli należy umożliwić wykazanie zgodności europejskich portfeli tożsamości cyfrowej z wymogami określonymi odpowiednio w niniejszym rozporządzeniu i w rozporządzeniu (UE) nr 910/2014 poprzez certyfikowanie swoich produktów w ramach europejskiego programu certyfikacji cyberbezpieczeństwa ustanowionego na podstawie rozporządzenia (UE) 2019/881, w odniesieniu do którego Komisja określiła w drodze aktów delegowanych domniemanie zgodności z niniejszym rozporządzeniem, w zakresie, w jakim certyfikat lub jego części obejmują te wymogi.

(34) W celu zadbania o to, aby te produkty były projektowane, opracowywane i produkowane zgodnie z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu, wbudowując komponenty pozyskiwane od osób trzecich do produktów z elementami cyfrowymi na etapie projektowania i opracowywania, producenci powinni postępować z należytą starannością w odniesieniu do tych komponentów, w tym komponentów będących wolnym i otwartym oprogramowaniem, które nie zostały udostępnione na rynku.

([16]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/2853 z dnia 23 października 2024 r. w sprawie odpowiedzialności za produkty wadliwe i uchylenia dyrektywy Rady 85/374/EWG (Dz.U. L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) 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).

([18]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. U. L 257 z 28.8.2014, s. 73).

Odpowiedni poziom należytej staranności zależy od charakteru i poziomu ryzyka w cyberprzestrzeni związanego z danym komponentem, w związku z czym powinna ona obejmować co najmniej jedno z następujących działań: sprawdzenie w stosownych przypadkach, czy producent komponentu wykazał zgodność z niniejszym rozporządzeniem, m.in. poprzez sprawdzenie, czy komponent został opatrzony oznakowaniem CE; sprawdzenie, czy komponent podlega regularnej aktualizacji zabezpieczeń, np. poprzez sprawdzenie historii aktualizacji zabezpieczeń; sprawdzenie, czy komponent nie charakteryzuje się podatnościami zarejestrowanymi w europejskiej bazie danych dotyczących podatności utworzonej na podstawie art. 12 ust. 2 dyrektywy (UE) 2022/2555 lub w innych publicznie dostępnych bazach danych dotyczących podatności; lub przeprowadzenie dodatkowych testów bezpieczeństwa. Obowiązki dotyczące postępowania w przypadku wykrycia podatności określone w niniejszym rozporządzeniu, z których producenci muszą się wywiązać przy wprowadzaniu produktu z elementami cyfrowymi do obrotu i w okresie wsparcia, mają zastosowanie do produktów z elementami cyfrowymi w całości, w tym do wszystkich zintegrowanych z nimi komponentów. Gdy w ramach obowiązku należytej staranności producent produktu z elementami cyfrowymi zidentyfikuje podatność w danym komponencie, w tym w komponencie będącym wolnym i otwartym oprogramowaniem, powinien poinformować osobę lub podmiot produkujący lub utrzymujący ten komponent, zbadać podatność i ją usunąć oraz, w stosownych przypadkach, dostarczyć tej osobie lub temu podmiotowi zastosowaną poprawkę zabezpieczeń.

(35) Zaraz po upływie przejściowego okresu stosowania niniejszego rozporządzenia producent produktu z elementami cyfrowymi, który zawiera co najmniej jeden komponent pochodzący od osób trzecich również podlegających niniejszemu rozporządzeniu, może nie być w stanie sprawdzić w ramach obowiązku należytej staranności, czy producenci tych komponentów wykazali zgodność z niniejszym rozporządzeniem, na podstawie sprawdzenia na przykład, czy komponenty te zostały opatrzone oznakowaniem CE. Może tak być w przypadku, gdy komponenty zostały wbudowane, zanim niniejsze rozporządzenie zaczęło mieć zastosowanie do ich producentów. Wtedy producent wbudowujący takie komponenty powinien zachować należytą staranność za pomocą innych środków.

(36) Aby mogły podlegać swobodnemu przepływowi na rynku wewnętrznym, produkty z elementami cyfrowymi powinny być w sposób widoczny, czytelny i nieusuwalny opatrzone oznakowaniem CE, które świadczy o ich zgodności z niniejszym rozporządzeniem. Państwa członkowskie nie powinny bez powodu utrudniać wprowadzania do obrotu produktów z elementami cyfrowymi zgodnych z wymogami określonymi w niniejszym rozporządzeniu i posiadających oznakowanie CE. Ponadto podczas targów, wystaw i pokazów lub podobnych imprez państwa członkowskie nie powinny uniemożliwiać prezentowania lub używania produktu z elementami cyfrowymi, który nie jest zgodny z niniejszym rozporządzeniem, w tym jego prototypów, pod warunkiem że dany produkt ma widoczne oznaczenie, które wskazuje, że nie jest on zgodny z niniejszym rozporządzeniem i nie będzie udostępniany na rynku, zanim nie będzie z nim zgodny.

(37) Aby zapewnić producentom możliwość wydawania oprogramowania do celów testowania przed poddaniem produktów z elementami cyfrowymi ocenie zgodności, państwa członkowskie nie powinny uniemożliwiać udostępniania nieukończonego oprogramowania, takiego jak wersje alfa, wersje beta lub kandydaci do wydania (ang. release candidate), pod warunkiem że takie nieukończone oprogramowanie zostanie udostępnione wyłącznie na okres niezbędny do jego 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 w jak najszerszym zakresie zgodne z wymogami bezpieczeństwa dotyczącymi właściwości produktów z elementami cyfrowymi określonymi w niniejszym rozporządzeniu. Producenci powinni także w 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.

(38) W trosce o to, aby produkty z elementami cyfrowymi po wprowadzeniu ich do obrotu nie stwarzały ryzyka w cyberprzestrzeni dla osób i organizacji, należy określić zasadnicze wymagania w zakresie cyberbezpieczeństwa dotyczące takich produktów. Te zasadnicze wymagania w zakresie cyberbezpieczeństwa, w tym wymagania dotyczące postępowania w przypadku wykrycia podatności, mają zastosowanie do każdego jednostkowego produktu z elementami cyfrowymi wprowadzanego do obrotu, niezależnie od tego, czy produkt z elementami cyfrowymi jest wytwarzany jako pojedynczy egzemplarz, czy seryjnie. Na przykład w przypadku danego rodzaju produktu każdy pojedynczy produkt z elementami cyfrowymi powinien w momencie wprowadzania go do obrotu otrzymywać wszystkie dostępne poprawki lub aktualizacje zabezpieczeń mające na celu rozwiązanie istotnych problemów związanych z bezpieczeństwem. Jeżeli takie produkty z elementami cyfrowymi zostaną następnie zmodyfikowane za pomocą środków fizycznych lub cyfrowych w sposób nieprzewidziany przez producenta w pierwotnej ocenie ryzyka i mogący oznaczać, że nie spełniają one już odpowiednich zasadniczych wymagań w zakresie cyberbezpieczeństwa, taką modyfikację należy uznać za istotną. Na przykład naprawy można uznać za operacje w zakresie utrzymania pod warunkiem że nie modyfikują one produktu z elementami cyfrowymi już wprowadzonego do obrotu w sposób, który może wpływać na jego zgodność z obowiązującymi wymaganiami lub zmienić przeznaczenie, pod kątem którego dokonano oceny produktu.

(39) Podobnie jak w przypadku fizycznych napraw lub modyfikacji produkt z elementami cyfrowymi należy uznać za istotnie zmodyfikowany poprzez zmianę oprogramowania, jeżeli aktualizacja oprogramowania zmienia przeznaczenie produktu, a zmian tych producent nie przewidział w pierwotnej ocenie ryzyka, lub gdy z powodu aktualizacji oprogramowania zmienił się charakter zagrożenia lub wzrósł poziom ryzyka w cyberprzestrzeni,

a zaktualizowana wersja produktu została udostępniona na rynku. Gdy aktualizacje zabezpieczeń, których celem jest zmniejszenie poziomu ryzyka w cyberprzestrzeni produktu z elementami cyfrowymi, nie zmieniają przeznaczenia produktu z elementami cyfrowymi, nie uznaje się ich za istotną modyfikację. Zazwyczaj wliczają się w to sytuacje, w których aktualizacje zabezpieczeń wiążą się jedynie z niewielkimi korektami kodu źródłowego. Może tak być na przykład, gdy aktualizacja zabezpieczeń dotyczy znanej podatności i polega m.in. na modyfikacji funkcji lub wydajności produktu z elementami cyfrowymi, lecz wyłącznie w celu obniżenia poziomu ryzyka w cyberprzestrzeni. Podobnie drobne aktualizacje funkcjonalności, takie jak ulepszenia wizualne lub dodanie nowych piktogramów lub nowych języków do interfejsu użytkownika, zasadniczo nie powinny być uznawane za istotne modyfikacje. Natomiast gdy aktualizacje cech zmieniają pierwotnie zamierzone funkcje, rodzaj lub wydajność produktu z elementami cyfrowymi i spełniają powyższe kryteria, należy je uznać za istotną modyfikację, ponieważ dodanie nowych funkcji zazwyczaj skutkuje szerszą płaszczyzną ataku, zwiększając tym samym ryzyko w cyberprzestrzeni. Może tak być na przykład w razie dodania do aplikacji nowego elementu z danymi wejściowymi, wymagającego od producenta zapewnienia odpowiedniej walidacji danych wejściowych. Przy ocenie, czy aktualizację cech uznaje się za istotną modyfikację, nie ma znaczenia, czy dostarcza się ją jako odrębną aktualizację, czy w połączeniu z aktualizacją zabezpieczeń. Komisja powinna wydać wytyczne, jak stwierdzić, co stanowi istotną modyfikację.

(40) Biorąc pod uwagę iteracyjny charakter rozwoju oprogramowania, producenci, którzy w wyniku późniejszych istotnych modyfikacji danego produktu wprowadzili do obrotu kolejne wersje oprogramowania, powinni mieć możliwość dostarczania aktualizacji zabezpieczeń w okresie wsparcia wyłącznie na potrzeby tej wersji oprogramowania, którą wprowadzili do obrotu jako ostatnią. Powinni mieć taką możliwość tylko wtedy, gdy użytkownicy odnośnych poprzednich wersji produktu mają bezpłatny dostęp do wersji produktu wprowadzonej do obrotu jako ostatnia i nie ponoszą dodatkowych kosztów związanych z dostosowaniem środowiska sprzętu lub oprogramowania, w którym działa ich produkt. Chodzi tu na przykład o przypadek, gdy modernizacja stacjonarnego systemu operacyjnego nie wymaga nowego sprzętu, takiego jak szybsza jednostka centralna lub obszerniejsza pamięć. W okresie wsparcia producent powinien jednak nadal spełniać inne wymogi dotyczące postępowania w przypadku wykrycia podatności, takie jak obowiązek dysponowania strategią skoordynowanego ujawniania podatności lub środkami ułatwiającymi wymianę informacji na temat potencjalnych podatności w odniesieniu do wszystkich późniejszych istotnie zmodyfikowanych wersji oprogramowania wprowadzonego do obrotu. Producenci powinni mieć możliwość dostarczania drobnych aktualizacji zabezpieczeń lub aktualizacji funkcjonalności, które nie stanowią istotnej modyfikacji, jedynie do najnowszej wersji lub podwersji oprogramowania, które nie zostały istotnie zmodyfikowane. Jednocześnie, w razie gdy urządzenie, takie jak smartfon, nie jest kompatybilne z najnowszą wersją systemu operacyjnego, z którą zostało pierwotnie dostarczone, w okresie wsparcia producent powinien stale dostarczać aktualizacje zabezpieczeń co najmniej do najnowszej kompatybilnej wersji systemu operacyjnego.

(41) Zgodnie z powszechnie przyjętą koncepcją istotnej modyfikacji w odniesieniu do produktów objętych unijnym prawodawstwem harmonizacyjnym za każdym razem, gdy następuje istotna modyfikacja, która może wpłynąć na zgodność produktu z elementami cyfrowymi z niniejszym rozporządzeniem, lub gdy zmienia się przeznaczenie produktu, należy sprawdzić 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.

(42) Kiedy produkt z elementami cyfrowymi jest przedmiotem „odnowienia", „konserwacji" i „naprawy", zgodnie z definicjami zawartymi w art. 2 pkt 18, 19 i 20 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1781 ([19]), niekoniecznie skutkuje to istotną modyfikacją produktu, na przykład jeśli nie zmienia przeznaczenia ani funkcji oraz jeśli nie wpływają na poziom ryzyka. Natomiast unowocześnienie produktu z elementami cyfrowymi przez producenta może skutkować zmianami w sposobie projektowania i opracowywania produktu i z tego względu może wpływać na przeznaczenie oraz na zgodność z wymogami określonymi w niniejszym rozporządzeniu.

(43) Produkt z elementami cyfrowymi należy uznać za ważny, jeśli negatywny wpływ wykorzystania potencjalnych podatności w produkcie może być dotkliwy, między innymi z uwagi na funkcję związaną z cyberbezpieczeństwem lub funkcję wiążącą się ze znacznym ryzykiem wystąpienia niekorzystnych skutków pod względem intensywności i zdolności do zakłócenia, kontrolowania lub spowodowania szkód w dużej liczbie innych produktów z elementami cyfrowymi bądź zaszkodzenia zdrowiu, bezpieczeństwu lub ochronie użytkowników przez bezpośrednią manipulację, takie jak funkcja systemu centralnego, w tym funkcja zarządzania siecią, kontroli konfiguracji, wirtualizacji lub przetwarzania danych osobowych. W szczególności podatności w produktach z elementami cyfrowymi posiadających funkcje związane z cyberbezpieczeństwem, takie jak menedżer uruchamiania systemu, mogą prowadzić do rozprzestrzeniania się problemów z bezpieczeństwem w całym łańcuchu dostaw. Dotkliwość

([19]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1781 z dnia 13 czerwca 2024 r. w sprawie ustanowienia ram ustalania wymogów ekoprojektu w odniesieniu do zrównoważonych produktów oraz zmiany dyrektywy (UE) 2020/1828 i rozporządzenia (UE) 2023/1542 i uchylenia dyrektywy 2009/125/WE (Dz.U. L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

wpływu incydentu może wzrosnąć także wówczas, gdy produkt głównie pełni funkcję systemu centralnego, w tym funkcję zarządzania siecią, kontroli konfiguracji, wirtualizacji lub przetwarzania danych osobowych.

(44) Niektóre kategorie produktów z elementami cyfrowymi należy poddać bardziej rygorystycznym procedurom oceny zgodności przy jednoczesnym zachowaniu proporcjonalnego podejścia. W tym celu ważne produkty z elementami cyfrowymi należy podzielić na dwie klasy, odzwierciedlające poziom ryzyka w cyberprzestrzeni powiązanego z tymi kategoriami produktów. Incydent z udziałem ważnych produktów z elementami cyfrowymi, które należą do klasy II, może prowadzić do poważniejszych negatywnych skutków niż incydent z udziałem ważnych produktów z elementami cyfrowymi, które należą do klasy I, na przykład ze względu na charakter ich funkcji związanej z cyberbezpieczeństwem lub ze względu na działanie innej funkcji, która wiąże się ze znacznym ryzykiem wystąpienia niekorzystnych skutków. Na takie poważniejsze skutki produktów z elementami cyfrowymi, które należą do klasy II, może wskazywać funkcja związana z cyberbezpieczeństwem lub inna funkcja, która wiąże się ze znacznym ryzykiem wystąpienia niekorzystnych skutków znacznie poważniejszych niż w przypadku produktów zaliczonych do klasy I, albo obie takie funkcje. Ważne produkty z elementami cyfrowymi należące do klasy II powinny zatem podlegać bardziej rygorystycznej procedurze oceny zgodności.

(45) Ważne produkty z elementami cyfrowymi, o których mowa w niniejszym rozporządzeniu, należy rozumieć jako produkty, które posiadają podstawową funkcjonalność kategorii ważnych produktów z elementami cyfrowymi określonej w niniejszym rozporządzeniu. Na przykład w niniejszym rozporządzeniu określono kategorie ważnych produktów z elementami cyfrowymi, które na podstawie ich podstawowej funkcjonalności zdefiniowano jako zapory sieciowe lub systemy wykrywania włamań lub zapobiegania włamaniom należące do klasy II. W związku z tym zapory sieciowe lub systemy wykrywania włamań lub zapobiegania włamaniom podlegają obowiązkowej ocenie zgodności przez stronę trzecią. Nie dotyczy to innych produktów z elementami cyfrowymi niesklasyfikowanych jako ważne produkty z elementami cyfrowymi, które mogą obejmować zapory sieciowe lub systemy wykrywania włamań lub zapobiegania włamaniom. Komisja powinna przyjąć akt wykonawczy w celu stworzenia opisu technicznego kategorii ważnych produktów z elementami cyfrowymi, które należą do klas I i II określonych w niniejszym rozporządzeniu.

(46) Kategorie produktów krytycznych z elementami cyfrowymi określone w niniejszym rozporządzeniu posiadają funkcję związaną z cyberbezpieczeństwem i wypełniają funkcję, która wiąże się ze znacznym ryzykiem negatywnych skutków pod względem intensywności i zdolności do zakłócenia, kontrolowania lub spowodowania szkód w dużej liczbie innych produktów z elementami cyfrowymi przez bezpośrednią manipulację. Ponadto te kategorie produktów z elementami cyfrowymi uznaje się za krytyczne zależności dla podmiotów kluczowych, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555. Kategorie produktów krytycznych z elementami cyfrowymi określone w załączniku do niniejszego rozporządzenia już powszechnie podlegają, ze względu na ich krytyczność, różnym formom certyfikacji i są również objęte europejskim systemem certyfikacji cyberbezpieczeństwa opartym na wspólnych kryteriach (EUCC) określonym w rozporządzeniu wykonawczym Komisji (UE) 2024/482 ([20]). Dlatego też aby zapewnić odpowiednią wspólną ochronę cyberbezpieczeństwa produktów krytycznych z elementami cyfrowymi w Unii, właściwe i proporcjonalne byłoby objęcie takich kategorii produktów obowiązkowym europejskim certyfikatem cyberbezpieczeństwa w drodze aktu delegowanego, jeżeli istnieje już odpowiedni europejski system certyfikacji cyberbezpieczeństwa obejmujący te produkty, a Komisja przeprowadziła już ocenę potencjalnego wpływu planowanej obowiązkowej certyfikacji na rynek. W tej ocenie należy wziąć pod uwagę zarówno podaż, jak i popyt – w tym to, czy popyt na produkty z elementami cyfrowymi zarówno po stronie państw członkowskich, jak i użytkowników jest dostatecznie duży, by wymagać obowiązkowej europejskiej certyfikacji cyberbezpieczeństwa – a także przeznaczenie produktów z elementami cyfrowymi, w tym krytyczne zależności podmiotów kluczowych od nich, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555. W ocenie należy również przeanalizować potencjalny wpływ obowiązkowej certyfikacji na dostępność tych produktów na rynku wewnętrznym oraz na zdolność i gotowość państw członkowskich do wdrożenia odpowiednich europejskich systemów certyfikacji cyberbezpieczeństwa.

(47) Akty delegowane wprowadzające wymóg obowiązkowej europejskiej certyfikacji cyberbezpieczeństwa powinny określać, które produkty z elementami cyfrowymi posiadające podstawową funkcjonalność kategorii produktów krytycznych z elementami cyfrowymi określonej w niniejszym rozporządzeniu mają podlegać obowiązkowej certyfikacji, a także wskazywać wymagany poziom uzasadnienia zaufania, który powinien być co najmniej „istotny". Wymagany poziom uzasadnienia zaufania powinien być proporcjonalny do poziomu ryzyka w cyberprzestrzeni, jakie niesie ze sobą produkt z elementami cyfrowymi. Na przykład jeżeli produkt z elementami cyfrowymi posiada podstawową funkcjonalność kategorii produktów krytycznych z elementami cyfrowymi określonej w niniejszym

([20]) Rozporządzenie wykonawcze Komisji (UE) 2024/482 z dnia 31 stycznia 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC) (Dz.U. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

rozporządzeniu i jest przeznaczony do stosowania w środowisku wrażliwym lub krytycznym, tak jak w przypadku produktów przeznaczonych do użytku przez podmioty kluczowe, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555, może on wymagać najwyższego poziomu uzasadnienia zaufania.

(48) Aby zapewnić w Unii odpowiednią wspólną ochronę cyberbezpieczeństwa produktów z elementami cyfrowymi, których podstawowe funkcje pozwalają zaliczyć je do kategorii produktów krytycznych z elementami cyfrowymi określonej w niniejszym rozporządzeniu, Komisja powinna być również uprawniona do przyjmowania aktów delegowanych w celu zmiany niniejszego rozporządzenia poprzez dodanie lub wycofanie kategorii produktów krytycznych z elementami cyfrowymi, w odniesieniu do których producenci mogliby być zobowiązani do uzyskania europejskiego certyfikatu cyberbezpieczeństwa w ramach europejskiego programu certyfikacji cyberbezpieczeństwa na podstawie rozporządzenia (UE) 2019/881 w celu wykazania zgodności z niniejszym rozporządzeniem. Do kategorii tych można dodać nową kategorię produktów krytycznych z elementami cyfrowymi, jeżeli podmioty kluczowe, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555, są od niej w istotny sposób zależne, jeżeli występują w nich incydenty lub wykorzystywane podatności, co może prowadzić do zakłóceń w krytycznych łańcuchach dostaw. Oceniając potrzebę dodania lub wycofania kategorii produktów krytycznych z elementami cyfrowymi w drodze aktu delegowanego, Komisja powinna mieć możliwość uwzględnienia, czy państwa członkowskie zidentyfikowały na poziomie krajowym produkty z elementami cyfrowymi, które mają podstawowe znaczenie dla odporności podmiotów kluczowych, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555 i coraz częściej są celem cyberataków w łańcuchu dostaw o potencjalnie poważnych skutkach zakłócających. Ponadto Komisja powinna móc uwzględnić wyniki skoordynowanego na poziomie Unii szacowania ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzonego zgodnie z art. 22 dyrektywy (UE) 2022/2555.

(49) Przygotowując środki służące wdrożeniu niniejszego rozporządzenia, Komisja powinna zadbać o usystematyzowane i regularne konsultacje z szerokim gronem interesariuszy. Powinny one mieć miejsce w szczególności w przypadku, gdy Komisja ocenia potrzebę ewentualnych aktualizacji wykazów kategorii ważnych lub krytycznych produktów z elementami cyfrowymi, ponieważ przy tej ocenie należy skonsultować się z odpowiednimi producentami i uwzględnić ich opinie, aby przeanalizować ryzyko w cyberprzestrzeni, a także bilans kosztów i korzyści związanych z uznaniem takich kategorii produktów za ważne lub krytyczne.

(50) 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 zawsze jest związane z cyberbezpieczeństwem, lecz może być konsekwencją naruszenia bezpieczeństwa. Takie rodzaje ryzyka powinny nadal być uregulowane przez właściwe unijne prawodawstwo harmonizacyjne inne niż niniejsze rozporządzenie. W przypadku braku mającego zastosowanie unijnego prawodawstwa harmonizacyjnego innego niż niniejsze rozporządzenie te rodzaje ryzyka powinny podlegać rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2023/988 ([21]). Z tego względu, w świetle ukierunkowanego charakteru niniejszego rozporządzenia, na zasadzie odstępstwa od art. 2 ust. 1 akapit trzeci lit. b) rozporządzenia (UE) 2023/988, do produktów z elementami cyfrowymi, jeżeli nie podlegają one szczegółowym wymogom nałożonym przez inne niż niniejsze rozporządzenie unijne prawodawstwo harmonizacyjne w rozumieniu art. 3 pkt 27 rozporządzenia (UE) 2023/988, w odniesieniu do ryzyka w zakresie bezpieczeństwa nieobjętego niniejszym rozporządzeniem zastosowanie powinny mieć rozdział III sekcja 1, rozdziały V i VII oraz rozdziały IX–XI rozporządzenia (UE) 2023/988.

(51) Produkty z elementami cyfrowymi sklasyfikowane jako systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. 6 rozporządzenia (UE) 2024/1689 Parlamentu Europejskiego i Rady ([22]), wchodzące w zakres niniejszego rozporządzenia, powinny spełniać zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzeniu. Jeżeli te systemy sztucznej inteligencji wysokiego ryzyka spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzeniu, należy je uznać za zgodne z wymogami w zakresie cyberbezpieczeństwa określonymi w art. 15 rozporządzenia (UE) 2024/1689 w takim zakresie, w jakim wymogi te są objęte deklaracją zgodności UE lub jej częściami wydanymi na podstawie niniejszego rozporządzenia. W tym celu ocena ryzyka w cyberprzestrzeni związanego z produktem z elementami cyfrowymi sklasyfikowanym jako system sztucznej inteligencji wysokiego ryzyka zgodnie z rozporządzeniem (UE) 2024/1689, które należy uwzględnić na etapie planowania, projektowania, opracowywania, produkcji, dostarczania i utrzymania takiego produktu zgodnie z wymogami niniejszego rozporządzenia, powinna uwzględniać ryzyko dla cyberodporności systemu sztucznej inteligencji w związku z dokonywanymi przez osoby trzecie próbami zmiany sposobu jego użycia, zachowania lub efektywności, w tym z podatnościami charakterystycznymi dla systemów sztucznej

([21]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z dnia 10 maja 2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG (Dz.U. L 135 z 23.5.2023, s. 1).

([22]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

inteligencji, takimi jak zatruwanie danych lub ataki polegające na wprowadzeniu do modelu złośliwych danych w celu spowodowania niezamierzonego działania systemu, a także, w stosownych przypadkach, ryzyko dla praw podstawowych zgodnie z rozporządzeniem (UE) 2024/1689. Jeśli chodzi o procedury oceny zgodności dotyczące zasadniczych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktu z elementami cyfrowymi, który wchodzi w zakres niniejszego rozporządzenia i jest sklasyfikowany jako system sztucznej inteligencji wysokiego ryzyka, co do zasady zastosowanie powinny mieć nie odpowiednie przepisy niniejszego rozporządzenia, ale art. 43 rozporządzenia (UE) 2024/1689. Zasada ta nie powinna jednak powodować zmniejszenia niezbędnego poziomu bezpieczeństwa w odniesieniu do ważnych lub krytycznych produktów z elementami cyfrowymi, o których mowa w niniejszym rozporządzeniu. Z tego względu, na zasadzie odstępstwa od tej zasady, systemy sztucznej inteligencji wysokiego ryzyka, które wchodzą w zakres rozporządzenia (UE) 2024/1689 i są również ważnymi lub krytycznymi produktami z elementami cyfrowymi, o których mowa w niniejszym rozporządzeniu, oraz do których zastosowanie ma procedura oceny zgodności opierająca się na kontroli wewnętrznej, o której mowa w załączniku VI do rozporządzenia (UE) 2024/1689, powinny podlegać przewidzianym w niniejszym rozporządzeniu procedurom oceny zgodności w zakresie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w niniejszym rozporządzeniu. W takim przypadku do wszystkich pozostałych aspektów objętych rozporządzeniem (UE) 2024/1689 należy stosować odpowiednie przepisy dotyczące oceny zgodności opierającej się na kontroli wewnętrznej określone w załączniku VI do tego rozporządzenia.

(52) W celu poprawy bezpieczeństwa produktów z elementami cyfrowymi wprowadzanych na rynek wewnętrzny niezbędne jest określenie zasadniczych wymagań w zakresie cyberbezpieczeństwa mających zastosowanie do takich produktów. Zasadnicze wymagania w zakresie cyberbezpieczeństwa powinny pozostawać bez uszczerbku dla skoordynowanego na poziomie Unii szacowania ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw, o którym mowa w art. 22 dyrektywy (UE) 2022/2555, które uwzględnia 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 uprawnienia państw członkowskich do określania dodatkowych wymogów, które uwzględniają czynniki pozatechniczne w celu zapewnienia wysokiego poziomu odporności, w tym te określone w zaleceniu Komisji (UE) 2019/534 ([23]), w unijnej skoordynowanej ocenie ryzyka w zakresie cyberbezpieczeństwa sieci 5G oraz w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G uzgodnionym przez Grupę Współpracy ustanowioną w art. 14 dyrektywy (UE) 2022/2555.

(53) Producenci produktów objętych zakresem rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1230 ([24]), które są również produktami z elementami cyfrowymi zdefiniowanymi w niniejszym rozporządzeniu, powinni spełniać zarówno zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzeniu, jak i zasadnicze wymogi w zakresie zdrowia i bezpieczeństwa określone w rozporządzeniu (UE) 2023/1230. Zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzeniu oraz niektóre zasadnicze wymagania określone w rozporządzeniu (UE) 2023/1230 mogą dotyczyć podobnych rodzajów ryzyka w cyberprzestrzeni. W związku z tym zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu mogłaby ułatwić spełnienie określonych w rozporządzeniu (UE) 2023/1230 zasadniczych wymagań, które obejmują również niektóre rodzaje ryzyka w cyberprzestrzeni, w szczególności tych dotyczących zabezpieczenia przed uszkodzeniem oraz bezpieczeństwa i niezawodności układów sterowania, określonymi w sekcjach 1.1.9 i 1.2.1 załącznika III do tego rozporządzenia. Producent musi wykazać taką synergię, stosując na przykład, w miarę dostępności, normy zharmonizowane lub inne specyfikacje techniczne uwzględniające odpowiednie zasadnicze wymagania w zakresie cyberbezpieczeństwa zgodnie z oceną ryzyka obejmującą te rodzaje ryzyka w cyberprzestrzeni. Producent powinien również przestrzegać obowiązujących procedur oceny zgodności określonych w niniejszym rozporządzeniu i w rozporządzeniu (UE) 2023/1230. W pracach przygotowawczych wspierających wdrożenie niniejszego rozporządzenia i rozporządzenia (UE) 2023/1230 oraz w powiązanych procesach normalizacyjnych Komisja i europejskie organizacje normalizacyjne powinny promować spójne metody oceny ryzyka w cyberprzestrzeni oraz uwzględniania tego ryzyka w normach zharmonizowanych w odniesieniu do odpowiednich zasadniczych wymagań. W szczególności Komisja i europejskie organizacje normalizacyjne powinny uwzględnić niniejsze rozporządzenie przy przygotowywaniu i opracowywaniu norm zharmonizowanych, aby ułatwić wdrożenie rozporządzenia (UE) 2023/1230, w szczególności w odniesieniu do aspektów cyberbezpieczeństwa związanych z elementami, o których mowa w sekcjach 1.1.9 i 1.2.1 załącznika III do tego rozporządzenia, czyli z zabezpieczeniem przed uszkodzeniem oraz z bezpieczeństwem i niezawodnością układów sterowania. Komisja powinna zapewnić wytyczne, aby wesprzeć producentów, którzy podlegają zarówno niniejszemu rozporządzeniu, jak i rozporządzeniu (UE) 2023/1230, a w szczególności ułatwić wykazanie zgodności z odpowiednimi zasadniczymi wymaganiami określonymi w niniejszym rozporządzeniu i w rozporządzeniu (UE) 2023/1230.

(54) W celu zapewnienia, aby produkty z elementami cyfrowymi były bezpieczne zarówno w momencie wprowadzenia ich do obrotu, jak i przez cały czas oczekiwanego użytkowania produktu z elementami cyfrowymi, konieczne jest określenie zasadniczych wymagań w zakresie cyberbezpieczeństwa dotyczących postępowania w przypadku wykrycia podatności oraz zasadniczych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do właściwości produktów z elementami cyfrowymi. Chociaż producenci powinni przestrzegać wszystkich zasadniczych wymagań

([23]) Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. w sprawie cyberbezpieczeństwa sieci 5G (Dz.U. L 88 z 29.3.2019, s. 42).
([24]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1230 z dnia 14 czerwca 2023 r. w sprawie maszyn oraz w sprawie uchylenia dyrektywy 2006/42/WE Parlamentu Europejskiego i Rady i dyrektywy Rady 73/361/EWG (Dz.U. L 165 z 29.6.2023, s. 1).

w zakresie cyberbezpieczeństwa dotyczących postępowania w przypadku wykrycia podatności w całym okresie wsparcia, powinni oni określić, jakie inne zasadnicze wymagania w zakresie cyberbezpieczeństwa dotyczące właściwości produktu są istotne dla danego rodzaju produktu z elementami cyfrowymi. W tym celu producenci powinni przeprowadzić ocenę ryzyka w cyberprzestrzeni związanego z produktem z elementami cyfrowymi, aby zidentyfikować istotne ryzyko oraz wskazać istotne zasadnicze wymagania w zakresie cyberbezpieczeństwa, jak również aby udostępniać swoje produkty bez znanych i możliwych do wykorzystania podatności, które mogłyby mieć wpływ na bezpieczeństwo tych produktów, oraz właściwie zastosować odpowiednie normy zharmonizowane, wspólne specyfikacje lub normy europejskie lub międzynarodowe.

(55) Jeżeli niektóre zasadnicze wymagania w zakresie cyberbezpieczeństwa nie mają zastosowania do danego produktu z elementami cyfrowymi, producent powinien przedstawić jasne uzasadnienie tego faktu w ocenie ryzyka w cyberprzestrzeni zawartej w dokumentacji technicznej. Taka sytuacja może zaistnieć w przypadku, gdy zasadnicze wymaganie w zakresie cyberbezpieczeństwa jest niezgodne z charakterem danego produktu z elementami cyfrowymi. Na przykład przeznaczenie produktu z elementami cyfrowymi może wymagać od producenta przestrzegania powszechnie uznanych norm interoperacyjności, nawet jeżeli jego zabezpieczenia nie są już uznawane za najnowocześniejsze. Podobnie inne przepisy prawa Unii nakładają na producentów obowiązek stosowania szczególnych wymogów w zakresie interoperacyjności. W przypadku gdy zasadnicze wymaganie w zakresie cyberbezpieczeństwa nie ma zastosowania do produktu z elementami cyfrowymi, ale producent zidentyfikował ryzyko w cyberprzestrzeni w odniesieniu do tego zasadniczego wymagania w zakresie cyberbezpieczeństwa, powinien on wprowadzić środki w celu wyeliminowania tego ryzyka innymi sposobami, na przykład poprzez ograniczenie przeznaczenia produktu do zaufanego środowiska lub poprzez poinformowanie użytkowników o tym ryzyku.

(56) Jednym z najważniejszych środków, które użytkownicy powinni zastosować w celu ochrony swoich produktów z elementami cyfrowymi przed cyberatakami, jest jak najszybsza instalacja najnowszych dostępnych aktualizacji zabezpieczeń. Producenci powinni zatem tak projektować swoje produkty i wprowadzać takie procedury, aby produkty z elementami cyfrowymi zawierały funkcje, które umożliwiają automatyczne powiadamianie o aktualizacjach zabezpieczeń, ich dystrybucję, pobieranie i instalację, zwłaszcza w przypadku towarów konsumenckich. Powinni oni również zapewniać możliwość zatwierdzania pobierania i instalowania aktualizacji zabezpieczeń na ostatnim etapie. Użytkownicy powinni zachować możliwość dezaktywacji automatycznych aktualizacji za pomocą jasnego i łatwego w użyciu mechanizmu, popartego jasnymi instrukcjami dotyczącymi sposobu, w jaki użytkownicy mogą to uczynić. Wymogi dotyczące automatycznych aktualizacji określone w załączniku do niniejszego rozporządzenia nie mają zastosowania do produktów z elementami cyfrowymi, które w pierwszej kolejności mają stanowić komponenty innych produktów. Nie mają one również zastosowania do produktów z elementami cyfrowymi, w przypadku których użytkownicy z zasady nie spodziewaliby się automatycznych aktualizacji, w tym produktów z elementami cyfrowymi przeznaczonych do wykorzystania w profesjonalnych sieciach ICT, a zwłaszcza w krytycznych i przemysłowych środowiskach, w których automatyczna aktualizacja mogłaby spowodować ingerencję w operacje. Niezależnie od tego, czy produkt z elementami cyfrowymi jest zaprojektowany w sposób zakładający automatyczne aktualizacje, czy też nie, jego producent powinien informować użytkowników o podatnościach i niezwłocznie udostępniać aktualizacje zabezpieczeń. W przypadku gdy produkt z elementami cyfrowymi posiada interfejs użytkownika lub podobne środki techniczne umożliwiające bezpośrednią interakcję z użytkownikami, producent powinien korzystać z takich funkcji w celu poinformowania użytkowników, że okres wsparcia ich produktu z elementami cyfrowymi zakończył się. Komunikaty powinny ograniczać się do tego, co jest konieczne do zapewnienia skutecznego odbioru tych informacji, i nie powinny mieć negatywnego wpływu na użytkowanie produktu z elementami cyfrowymi.

(57) Aby zwiększyć przejrzystość procedur postępowania w przypadku wykrycia podatności oraz zadbać o to, aby użytkownicy nie byli zobowiązani do instalowania nowych aktualizacji funkcji tylko po to, aby uzyskać najnowsze aktualizacje zabezpieczeń, producenci powinni zapewnić, jeżeli jest to technicznie wykonalne, aby nowe aktualizacje zabezpieczeń były dostarczane oddzielnie od aktualizacji funkcji.

(58) We wspólnym komunikacie Komisji i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 20 czerwca 2023 r. zatytułowanym „Europejska strategia bezpieczeństwa gospodarczego" stwierdzono, że Unia musi zmaksymalizować korzyści płynące z jej otwartości gospodarczej, a jednocześnie zminimalizować ryzyko związane z zależnościami gospodarczymi od dostawców wysokiego ryzyka za pomocą wspólnych ram strategicznych na rzecz bezpieczeństwa gospodarczego Unii. W przypadku produktów z elementami cyfrowymi zależność od dostawców wysokiego ryzyka może stanowić ryzyko strategiczne, które należy wyeliminować na poziomie Unii, zwłaszcza gdy produkty z elementami cyfrowymi są przeznaczone do użytku przez podmioty kluczowe, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555. Ryzyko takie może być związane między innymi z jurysdykcją mającą zastosowanie do producenta, charakterystyką jego struktury własnościowej oraz powiązaniami kontrolnymi z rządem państwa trzeciego, w którym ma on siedzibę, w szczególności jeżeli dane państwo trzecie uczestniczy w szpiegostwie gospodarczym lub nieodpowiedzialnych zachowaniach w cyberprzestrzeni, a jego ustawodawstwo umożliwia arbitralny dostęp do wszelkiego rodzaju operacji lub danych przedsiębiorstwa, w tym szczególnie chronionych danych handlowych, i może nakładać obowiązki do celów wywiadowczych bez demokratycznych mechanizmów kontroli i równowagi, mechanizmu nadzoru, sprawiedliwości proceduralnej lub prawa do odwołania się do niezależnego sądu lub trybunału. Określając powagę ryzyka w cyberprzestrzeni w rozumieniu niniejszego rozporządzenia, Komisja i organy nadzoru rynku, w zakresie swoich kompetencji określonych w niniejszym rozporządzeniu, powinny również uwzględnić

pozatechniczne czynniki ryzyka, w szczególności te ustalone w wyniku skoordynowanego na poziomie Unii szacowania ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw, przeprowadzonego zgodnie z art. 22 dyrektywy (UE) 2022/2555.

(59) Aby zapewnić bezpieczeństwo produktów z elementami cyfrowymi po ich wprowadzeniu do obrotu, producenci powinni zdefiniować okres wsparcia, który powinien odzwierciedlać przewidywany czas użytkowania danego produktu z elementami cyfrowymi. Definiując okres wsparcia, producent powinien wziąć pod uwagę w szczególności uzasadnione oczekiwania użytkowników, charakter produktu, a także odpowiednie prawo Unii określające cykl życia produktów z elementami cyfrowymi. Producenci powinni mieć również możliwość uwzględnienia innych istotnych czynników. Kryteria powinny być stosowane w sposób zapewniający proporcjonalność przy definiowaniu okresu wsparcia. Na żądanie producent powinien przekazać organom nadzoru rynku informacje, które zostały uwzględnione przy definiowaniu okresu wsparcia produktu z elementami cyfrowymi.

(60) Okres wsparcia, w którym producent zapewnia skuteczną obsługę podatności, powinien wynosić co najmniej pięć lat, chyba że okres użytkowania produktu z elementami cyfrowymi jest krótszy niż pięć lat – wówczas producent powinien zapewnić obsługę podatności przez ten okres. Jeżeli można racjonalnie oczekiwać, że dany produkt z elementami cyfrowymi będzie użytkowany dłużej niż pięć lat, jak często ma to miejsce w przypadku komponentów sprzętowych, takich jak płyty główne lub mikroprocesory, urządzeń sieciowych, takich jak routery, modemy lub przełączniki sieciowe, a także oprogramowania, np. systemów operacyjnych lub narzędzi do edycji wideo, producenci powinni odpowiednio zapewnić dłuższe okresy wsparcia. W szczególności produkty z elementami cyfrowymi przeznaczone do użytku w środowisku przemysłowym, takie jak systemy kontroli przemysłowej, są często użytkowane przez znacznie dłuższe okresy. Producent powinien móc zdefiniować okres wsparcia krótszy niż pięć lat tylko wtedy, gdy jest to uzasadnione charakterem danego produktu z elementami cyfrowymi i gdy oczekuje się, że produkt ten będzie użytkowany krócej niż pięć lat, w którym to przypadku okres wsparcia powinien odpowiadać przewidywanemu okresowi użytkowania. Na przykład okres użytkowania aplikacji do ustalania kontaktów zakaźnych przeznaczonej na czas pandemii może być ograniczony do czasu trwania pandemii. Ponadto niektóre aplikacje z natury mogą być udostępniane wyłącznie na zasadzie subskrypcji, w szczególności w przypadku, gdy po wygaśnięciu subskrypcji aplikacja staje się niedostępna dla użytkownika i w związku z tym nie jest już używana.

(61) Aby zapewnić obsługę podatności po zakończeniu okresów wsparcia produktów z elementami cyfrowymi, producenci powinni rozważyć udostępnienie kodu źródłowego takich produktów z elementami cyfrowymi albo innym przedsiębiorstwom, które zobowiążą się do dalszego świadczenia usług w zakresie obsługi podatności, albo do wiadomości publicznej. W przypadku gdy producenci udostępniają kod źródłowy innym przedsiębiorstwom, powinni móc chronić własność produktu z elementami cyfrowymi i zapobiegać publicznemu rozpowszechnianiu kodu źródłowego, na przykład w drodze ustaleń umownych.

(62) W celu zadbania o to, aby producenci w całej Unii określali podobne okresy wsparcia dla porównywalnych produktów z elementami cyfrowymi, grupa ADCO powinna publikować statystyki dotyczące średnich okresów wsparcia zdefiniowanych przez producentów dla poszczególnych kategorii produktów z elementami cyfrowymi oraz wydawać wytyczne wskazujące odpowiednie okresy wsparcia dla takich kategorii. Ponadto aby zapewnić zharmonizowane podejście na całym rynku wewnętrznym, Komisja powinna mieć możliwość przyjmowania aktów delegowanych w celu zdefiniowania minimalnych okresów wsparcia dla konkretnych kategorii produktów, jeżeli z danych dostarczonych przez organy nadzoru rynku wynika, że okresy wsparcia zdefiniowane przez producentów są systematycznie niezgodne z kryteriami definiowania okresów wsparcia przewidzianymi w niniejszym rozporządzeniu lub że producenci w różnych państwach członkowskich w nieuzasadniony sposób definiują różne okresy wsparcia.

(63) Producenci powinni utworzyć pojedynczy punkt kontaktowy, który umożliwi użytkownikom łatwą komunikację z nimi, w tym w celu zgłaszania podatności produktu z elementem cyfrowym i otrzymywania informacji o takich podatnościach. Powinni oni zapewnić użytkownikom łatwy dostęp do takiego pojedynczego punktu kontaktowego i wyraźnie informować o jego dostępności oraz dbać o to, by informacje te były aktualizowane. Jeżeli producenci postanowią oferować narzędzia zautomatyzowane, np. czatboty, powinni również podawać numer telefonu lub inne cyfrowe możliwości kontaktu, takie jak adres e-mail lub formularz kontaktowy. Pojedynczy punkt kontaktowy nie powinien opierać się wyłącznie na zautomatyzowanych narzędziach.

(64) Producenci powinni udostępniać na rynku swoje produkty z elementami cyfrowymi w bezpiecznej domyślnej konfiguracji i bezpłatnie dostarczać użytkownikom aktualizacje zabezpieczeń. Producenci powinni mieć możliwość odstąpienia od tych zasadniczych wymagań w zakresie cyberbezpieczeństwa wyłącznie w przypadku produktów dostosowanych do indywidualnych potrzeb, które są montowane w konkretnym celu dla konkretnego użytkownika biznesowego, i wyłącznie wówczas, gdy zarówno producent, jak i użytkownik wyraźnie zgodzili się na inny zestaw warunków umownych.

(65) Producenci powinni jednocześnie powiadamiać za pośrednictwem pojedynczej platformy sprawozdawczej zarówno zespół reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) wyznaczony na koordynatora, jak i ENISA o aktywnie wykorzystywanych podatnościach obecnych w produktach z elementami cyfrowymi, a także o poważnych incydentach mających wpływ na bezpieczeństwo tych produktów. Powiadomienia te powinny być przekazywane z wykorzystaniem punktu zgłoszeń elektronicznych CSIRT wyznaczonego na koordynatora i powinny być jednocześnie dostępne dla ENISA.

(66) Producenci powinni zgłaszać aktywnie wykorzystywane podatności w celu zadbania o to, aby CSIRT-y wyznaczone na koordynatorów i ENISA posiadały odpowiedni przegląd takich podatności i otrzymywały informacje niezbędne do realizacji swoich zadań określonych w dyrektywie (UE) 2022/2555, a także w celu podniesienia ogólnego poziomu cyberbezpieczeństwa podmiotów kluczowych i ważnych, o których mowa w art. 3 tej dyrektywy, oraz zapewnienia skutecznego funkcjonowania organów nadzoru rynku. Ponieważ większość produktów z elementami cyfrowymi jest wprowadzana do obrotu na całym rynku wewnętrznym, każdą podatność wykorzystywaną w produkcie z elementami cyfrowymi należy uznać za zagrożenie dla funkcjonowania rynku wewnętrznego. ENISA powinna, w porozumieniu z producentem, ujawniać naprawione podatności w europejskiej bazie danych dotyczących podatności utworzonej na podstawie art. 12 ust. 2 dyrektywy (UE) 2022/2555. Europejska baza danych dotyczących podatności będzie pomagać producentom w wykrywaniu znanych możliwych do wykorzystania podatności w ich produktach, aby zapewnić wprowadzanie do obrotu bezpiecznych produktów.

(67) Producenci powinni także zgłaszać do CSIRT-u wyznaczonego na koordynatora oraz do ENISA wszelkie poważne incydenty wpływające na bezpieczeństwo produktu z elementami cyfrowymi. Aby zapewnić użytkownikom możliwość szybkiego reagowania na poważne 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 w cyberprzestrzeni, docierając bezpośrednio do użytkowników.

(68) Aktywnie wykorzystywane podatności dotyczą przypadków, w których producent ustali, że naruszenie bezpieczeństwa mające wpływ na jego użytkowników lub jakiekolwiek inne osoby fizyczne lub prawne był wynikiem wykorzystania przez podmiot działający w złej wierze wady w jednym z produktów z elementami cyfrowymi udostępnionych na rynku przez producenta. Przykładami takich podatności mogą być niedociągnięcia w funkcjach identyfikacji i uwierzytelniania produktu. Podatności wykrywane bez złych zamiarów do celów testowania w dobrej wierze, analizy, korekty lub ujawniania z myślą o wsparciu bezpieczeństwa lub ochrony właściciela systemu i jego użytkowników nie powinny podlegać obowiązkowi zgłaszania. Z kolei poważne incydenty mające wpływ na bezpieczeństwo produktu z elementami cyfrowymi dotyczą sytuacji, w których incydent cyberbezpieczeństwa wpływa na realizowane przez producenta procesy opracowywania, produkcji lub utrzymania w taki sposób, że mógłby spowodować zwiększone ryzyko w cyberprzestrzeni dla użytkowników lub innych osób. Takim poważnym incydentem może być sytuacja, w której atakujący skutecznie wprowadził złośliwy kod do kanału, za pośrednictwem którego producent udostępnia użytkownikom aktualizacje zabezpieczeń.

(69) Aby zapewnić możliwość szybkiego rozpowszechniania zgłoszeń wśród wszystkich odpowiednich CSIRT-ów wyznaczonych na koordynatorów oraz aby umożliwić producentom składanie jednego zgłoszenia na każdym etapie procesu zgłaszania, ENISA powinna ustanowić pojedynczą platformę sprawozdawczą z krajowymi punktami zgłoszeń elektronicznych. Za bieżące funkcjonowanie pojedynczej platformy sprawozdawczej powinna odpowiadać ENISA. CSIRT-y wyznaczone na koordynatorów powinny informować swoje odpowiednie organy nadzoru rynku o zgłoszonych podatnościach lub incydentach. Pojedyncza platforma sprawozdawcza powinna być zaprojektowana w taki sposób, aby zapewniała poufność zgłoszeń, w szczególności w odniesieniu do podatności, dla których nie jest jeszcze dostępna aktualizacja zabezpieczeń. Ponadto ENISA powinna wprowadzić procedury bezpiecznego i poufnego postępowania z informacjami. Na podstawie zgromadzonych przez siebie informacji ENISA powinna co dwa lata przygotowywać sprawozdanie techniczne na temat nowych tendencji w zakresie ryzyka w cyberprzestrzeni dotyczącego produktów z elementami cyfrowymi oraz przedkładać je Grupie Współpracy ustanowionej zgodnie z art. 14 dyrektywy (UE) 2022/2555.

(70) W wyjątkowych okolicznościach, w szczególności na wniosek producenta, CSIRT wyznaczony na koordynatora, który jako pierwszy otrzymuje zgłoszenie, powinien móc podjąć decyzję o opóźnieniu jego przekazania innym odpowiednim CSIRT-om wyznaczonym na koordynatorów za pośrednictwem pojedynczej platformy sprawozdawczej, jeżeli jest to uzasadnione względami związanymi z cyberbezpieczeństwem i na okres absolutnie niezbędny. CSIRT wyznaczony na koordynatora powinien niezwłocznie poinformować ENISA o decyzji o opóźnieniu i jej powodach, a także o tym, kiedy zamierza dalej rozpowszechniać informacje. Komisja powinna opracować, w drodze aktu delegowanego, specyfikacje dotyczące warunków, w jakich można powołać się na powiązane z cyberbezpieczeństwem podstawy, i powinna współpracować z siecią CSIRT ustanowioną na podstawie art. 15 dyrektywy (UE) 2022/2555 oraz z ENISA przy przygotowywaniu projektu aktu delegowanego. Przykłady powiązanych z cyberbezpieczeństwem podstaw obejmują trwającą procedurę skoordynowanego ujawniania podatności lub sytuacje, w których oczekuje się, że producent wkrótce przedstawi środek łagodzący, a ryzyko w cyberprzestrzeni wynikające z natychmiastowego rozpowszechniania za pośrednictwem pojedynczej platformy sprawozdawczej przewyższa korzyści płynące z takiego działania. Na wniosek CSIRT-u wyznaczonego na koordynatora ENISA

powinna mieć możliwość wspierania tego CSIRT-u w powoływaniu się na powiązane z cyberbezpieczeństwem podstawy w odniesieniu do opóźnienia w rozpowszechnianiu zgłoszenia na podstawie informacji, które ENISA otrzymała od tego CSIRT-u na temat decyzji o wstrzymaniu zgłoszenia z powodu tych względów związanych z cyberbezpieczeństwem. Ponadto w szczególnie wyjątkowych okolicznościach ENISA nie powinna jednocześnie otrzymywać wszystkich szczegółów zgłoszenia dotyczącego aktywnie wykorzystywanej podatności. Dotyczy to przypadku, gdy producent zaznacza w swoim zgłoszeniu, że zgłoszona podatność została aktywnie wykorzystana przez podmiot działający w złej wierze i że zgodnie z dostępnymi informacjami nie została ona wykorzystana w żadnym innym państwie członkowskim niż w państwie CSIRT-u wyznaczonego na koordynatora, któremu producent zgłosił podatność, jeżeli jakiekolwiek natychmiastowe dalsze rozpowszechnienie zgłoszonej podatności prawdopodobnie doprowadziłoby do dostarczenia informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami tego państwa członkowskiego, lub jeżeli zgłoszona podatność stwarza bezpośrednie wysokie ryzyko dla cyberbezpieczeństwa wynikające z dalszego rozpowszechniania. W takich przypadkach ENISA uzyska jedynie równoczesny dostęp do informacji o tym, że producent dokonał zgłoszenia, ogólnych informacji na temat danego produktu z elementami cyfrowymi, informacji o ogólnym charakterze wykorzystania podatności oraz informacji o tym, że producent powołał się na te względy bezpieczeństwa, a zatem wstrzymano przekazanie pełnej treści zgłoszenia. Pełne zgłoszenie powinno następnie zostać udostępnione ENISA i innym odpowiednim CSIRT-om wyznaczonym na koordynatorów, jeżeli CSIRT wyznaczony na koordynatora, który jako pierwszy otrzymał zgłoszenie, stwierdzi, że te względy bezpieczeństwa, odzwierciedlające szczególnie wyjątkowe okoliczności określone w niniejszym rozporządzeniu, przestają istnieć. Jeżeli na podstawie dostępnych informacji ENISA uzna, że istnieje ryzyko systemowe mające wpływ na bezpieczeństwo rynku wewnętrznego, ENISA powinna zalecić CSIRT-owi odbierającemu zgłoszenie, aby przekazał pełne zgłoszenie pozostałym CSIRT-om wyznaczonym na koordynatorów oraz samej ENISA.

(71) Zgłaszając aktywnie wykorzystywaną podatność lub poważny incydent mający wpływ na bezpieczeństwo produktu z elementami cyfrowymi, producenci powinni wskazać, jak wrażliwe ich zdaniem są zgłoszone informacje. CSIRT wyznaczony na koordynatora, który jako pierwszy otrzymał zgłoszenie, powinien uwzględnić te informacje przy ocenie, czy zgłoszenie powoduje wystąpienie wyjątkowych okoliczności, które uzasadniają opóźnienie w przekazaniu zgłoszenia innym odpowiednim CSIRT-om wyznaczonym na koordynatorów z uzasadnionych względów związanych z cyberbezpieczeństwem. Powinien on również uwzględnić te informacje przy ocenie, czy zgłoszenie aktywnie wykorzystywanej podatności powoduje wystąpienie szczególnie wyjątkowych okoliczności, które uzasadniają nieudostępnianie ENISA od razu pełnego zgłoszenia. Ponadto CSIRT-y wyznaczone na koordynatorów powinny mieć możliwość uwzględnienia tych informacji przy określaniu odpowiednich środków mających na celu ograniczenie ryzyka wynikającego z takich podatności i incydentów.

(72) Aby uprościć przekazywanie informacji wymaganych na mocy niniejszego rozporządzenia, z uwzględnieniem innych uzupełniających wymogów sprawozdawczych określonych w przepisach prawa Unii, takich jak rozporządzenie (UE) 2016/679, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 ([25]), dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([26]) i dyrektywa (UE) 2022/2555, a także aby zmniejszyć obciążenia administracyjne dla podmiotów, zachęca się państwa członkowskie, aby rozważyły ustanowienie na poziomie krajowym pojedynczych punktów kontaktowych na potrzeby takich wymogów sprawozdawczych. Wykorzystywanie takich krajowych pojedynczych punktów kontaktowych do zgłaszania incydentów bezpieczeństwa na podstawie rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE nie powinno mieć wpływu na stosowanie przepisów rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE, w szczególności przepisów dotyczących niezależności organów, o których mowa w tych aktach. Ustanawiając pojedynczą platformę sprawozdawczą, o której mowa w niniejszym rozporządzeniu, ENISA powinna uwzględnić możliwość włączenia krajowych punktów zgłoszeń elektronicznych, o których mowa w niniejszym rozporządzeniu, do krajowych pojedynczych punktów kontaktowych, które mogą również przyjmować inne zgłoszenia wymagane na mocy prawa Unii.

(73) Ustanawiając pojedynczą platformę sprawozdawczą, o której mowa w niniejszym rozporządzeniu, oraz aby skorzystać z dotychczasowych doświadczeń, ENISA powinna konsultować się z innymi instytucjami lub agencjami Unii, które zarządzają platformami lub bazami danych podlegającymi rygorystycznym wymogom bezpieczeństwa, takimi jak Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA). ENISA powinna również przeanalizować potencjalną komplementarność z europejską bazą danych dotyczącą podatności utworzoną na podstawie art. 12 ust. 2 dyrektywy (UE) 2022/2555.

(74) Producenci i inne osoby fizyczne i prawne powinni mieć możliwość dobrowolnego zgłaszania CSIRT-owi wyznaczonemu na koordynatora lub ENISA wszelkich podatności zawartych w produkcie z elementami cyfrowymi,

([25]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).

([26]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.U. L 201 z 31.7.2002, s. 37).

cyberzagrożeń, które mogłyby mieć wpływ na profil ryzyka produktu z elementami cyfrowymi, wszelkich incydentów mających wpływ na bezpieczeństwo produktu z elementami cyfrowymi, a także potencjalnych zdarzeń dla cyberbezpieczeństwa, które mogłyby doprowadzić do takiego incydentu.

(75) Państwa członkowskie powinny w miarę możliwości dążyć do wyeliminowania problemów, z którymi mierzą się osoby wyszukujące podatności, w tym ich potencjalnego narażenia na odpowiedzialność karną, zgodnie z prawem krajowym. W związku z tym, że osoby fizyczne i prawne wyszukujące podatności mogą w niektórych państwach członkowskich być narażone na odpowiedzialność karną i cywilną, zachęca się państwa członkowskie do przyjęcia wytycznych przewidujących odstąpienie od postępowania cywilnego lub karnego wobec osób wyszukujących podatności w obszarze bezpieczeństwa informacji oraz zwolnienie ich z odpowiedzialności cywilnej lub karnej za te działania.

(76) Producenci produktów z elementami cyfrowymi powinni wdrożyć politykę skoordynowanego ujawniania podatności, aby ułatwić zgłaszanie podatności przez osoby lub podmioty bezpośrednio producentowi lub pośrednio, a na żądanie anonimowo, za pośrednictwem CSIRT-ów wyznaczonych na koordynatorów do celów skoordynowanego ujawniania podatności zgodnie z art. 12 ust. 1 dyrektywy (UE) 2022/2555. W polityce producentów dotyczącej skoordynowanego ujawniania podatności należy określić ustrukturyzowany proces, w ramach którego podatności zgłaszane są producentowi w sposób umożliwiający mu zdiagnozowanie i wyeliminowanie takich podatności, zanim szczegółowe informacje dotyczące podatności zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej. Ponadto producenci powinni również rozważyć publikację swojej polityki bezpieczeństwa w formacie nadającym się do odczytu maszynowego. 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. Są to tak zwane „programy bug bounty".

(77) 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 w cyberprzestrzeni. Szczególnie istotne jest zapewnienie przez producentów, aby ich produkty z elementami cyfrowymi nie zawierały opracowanych przez strony trzecie komponentów, w których mogą występować podatności. Producenci nie powinni być zobowiązani do upubliczniania zestawieniu podstawowych materiałów do produkcji oprogramowania.

(78) W nowych złożonych modelach biznesowych związanych ze sprzedażą przez internet firma działająca online może świadczyć różnorodne usługi. W zależności od charakteru usług świadczonych w odniesieniu do danego produktu z elementami cyfrowymi ten sam podmiot może należeć do różnych kategorii modeli biznesowych lub podmiotów gospodarczych. Jeżeli podmiot świadczy tylko usługi pośrednictwa internetowego w odniesieniu do danego produktu z elementami cyfrowymi i jest jedynie dostawcą internetowej platformy handlowej, zgodnie z definicją zawartą w art. 3 pkt 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/988, nie kwalifikuje się on jako jeden z rodzajów podmiotów gospodarczych w rozumieniu niniejszego rozporządzenia. Jeżeli ten sam podmiot jest dostawcą internetowej platformy handlowej i działa również jako podmiot gospodarczy zdefiniowany w niniejszym rozporządzeniu w odniesieniu do sprzedaży określonych produktów z elementami cyfrowymi, powinien on podlegać obowiązkom określonym w niniejszym rozporządzeniu dla tego rodzaju podmiotu gospodarczego. Na przykład jeżeli dostawca internetowej platformy handlowej również dystrybuuje produkt z elementami cyfrowymi, wówczas w odniesieniu do sprzedaży dystrybuowanego produktu zostałby uznany za dystrybutora. Podobnie jeżeli dany podmiot sprzedaje produkty z elementami cyfrowymi pod własną marką, uznawany byłby za producenta, a zatem musiałby spełniać wymagania mające zastosowanie do producentów. Ponadto niektóre podmioty mogą być uznawane za dostawców usług realizacji zamówień w rozumieniu art. 3 pkt 11 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 ([27]), jeżeli oferują takie usługi. Takie przypadki wymagałyby oceny indywidualnej. Biorąc pod uwagę znaczącą rolę, jaką internetowe platformy handlowe odgrywają w umożliwianiu handlu elektronicznego, powinny one dążyć do współpracy z organami nadzoru rynku państw członkowskich, aby pomóc zapewnić zgodność produktów z elementami cyfrowymi nabywanych za pośrednictwem internetowych platform handlowych z wymogami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu.

(79) 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 wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzenia przełożono na szczegółowe specyfikacje techniczne oraz które przyjęto zgodnie z rozporządzeniem Parlamentu

([27]) 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).

Europejskiego i Rady (UE) nr 1025/2012 ([28]). W rozporządzeniu tym przewidziano procedurę sprzeciwu wobec norm zharmonizowanych, w przypadku gdy normy takie nie spełniają w pełni wymogów określonych w niniejszym rozporządzeniu. Proces normalizacji powinien zapewniać zrównoważoną reprezentację interesów i faktyczny udział zainteresowanych stron ze społeczeństwa obywatelskiego, w tym organizacji konsumenckich. Należy również uwzględnić normy międzynarodowe zgodne z poziomem ochrony cyberbezpieczeństwa przewidzianym w zasadniczych wymaganiach w zakresie cyberbezpieczeństwa określonych w niniejszym rozporządzeniu, aby ułatwić opracowywanie norm zharmonizowanych i wdrażanie niniejszego rozporządzenia, a także ułatwić przestrzeganie przepisów przedsiębiorstwom, w szczególności mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom, a także przedsiębiorstwom działającym na rynku globalnym.

(80) Terminowe opracowanie norm zharmonizowanych w okresie przejściowym stosowania niniejszego rozporządzenia oraz ich dostępność przed datą rozpoczęcia stosowania niniejszego rozporządzenia będą miały szczególne znaczenie dla jego skutecznego wdrożenia. Dotyczy to w szczególności ważnych produktów z elementami cyfrowymi należących do klasy I. Dostępność norm zharmonizowanych umożliwi producentom takich produktów przeprowadzanie ocen zgodności za pomocą procedury kontroli wewnętrznej, co pozwoli uniknąć zatorów i opóźnień w działaniach jednostek oceniających zgodność.

(81) W rozporządzeniu (UE) 2019/881 ustanowiono europejskie ramy dobrowolnej certyfikacji cyberbezpieczeństwa dotyczącej produktów ICT, procesów ICT i usług ICT. Europejskie programy certyfikacji cyberbezpieczeństwa zapewniają wspólne ramy zaufania dla użytkowników korzystających z produktów z elementami cyfrowymi, które wchodzą w zakres niniejszego rozporządzenia. Niniejsze rozporządzenie powinno zatem 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 europejskiego programu certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881, co zostało określone przez Komisję w akcie wykonawczym, uznaje się za zgodne z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu w zakresie, w jakim europejski certyfikat cyberbezpieczeństwa bądź deklaracja zgodności lub ich części obejmują te wymogi. W świetle niniejszego rozporządzenia, w tym przy przygotowywaniu unijnego kroczącego programu prac zgodnie z rozporządzeniem (UE) 2019/881, należy ocenić potrzebę nowych europejskich programów certyfikacji cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi. W przypadku gdy potrzebny jest nowy program obejmujący produkty z elementami cyfrowymi, na przykład aby ułatwić przestrzeganie niniejszego rozporządzenia, Komisja może zwrócić się do ENISA o przygotowanie propozycji programu zgodnie z art. 48 rozporządzenia (UE) 2019/881. W takich przyszłych europejskich programach certyfikacji cyberbezpieczeństwa obejmujących produkty z elementami cyfrowymi należy uwzględnić zasadnicze wymagania w zakresie cyberbezpieczeństwa i procedury oceny zgodności określone w niniejszym rozporządzeniu oraz ułatwiać zapewnienie zgodności z niniejszym rozporządzeniem. W przypadku europejskich programów certyfikacji cyberbezpieczeństwa, które wejdą w życie przed wejściem w życie niniejszego rozporządzenia, konieczne może być doprecyzowanie szczegółowych aspektów stosowania domniemania zgodności. Komisja powinna być uprawniona do określania, w drodze aktów delegowanych, na jakich warunkach można stosować europejskie programy certyfikacji cyberbezpieczeństwa w celu wykazania zgodności z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu. Co więcej, aby uniknąć nadmiernych obciążeń administracyjnych, na producentach nie powinien spoczywać obowiązek przeprowadzenia oceny zgodności przez stronę trzecią, jak przewidziano w niniejszym rozporządzeniu w odniesieniu do odpowiednich wymogów, jeżeli w ramach takich europejskich programów certyfikacji cyberbezpieczeństwa wydano europejski certyfikat cyberbezpieczeństwa przynajmniej na poziomie „istotny".

(82) Po wejściu w życie rozporządzenia wykonawczego (UE) 2024/482, który dotyczy produktów wchodzących w zakres niniejszego rozporządzenia, takich jak sprzętowe moduły bezpieczeństwa i mikroprocesory, Komisja powinna móc określić, w drodze aktu delegowanego, w jaki sposób EUCC zapewnia domniemanie zgodności z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu lub jego części. Co więcej, w takim akcie delegowanym można określić, w jaki sposób certyfikat wydany w ramach EUCC zwalnia producentów z obowiązku przeprowadzenia oceny przez stronę trzecią, wymaganej na podstawie niniejszego rozporządzenia w odniesieniu do odpowiednich wymogów.

(83) Obecne europejskie ramy normalizacyjne, które opierają się na zasadach nowego podejścia określonych w rezolucji Rady z dnia 7 maja 1985 r. w sprawie nowego podejścia do harmonizacji i norm technicznych oraz na rozporządzeniu (UE) nr 1025/2012, stanowią domyślnie ramy opracowywania norm przewidujących domniemanie zgodności z odpowiednimi zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu. Normy europejskie powinny być oparte na zasadach rynkowych i uwzględniać interes publiczny, a także cele polityki jasno określone we wniosku Komisji skierowanym do co najmniej jednej europejskiej organizacji normalizacyjnej o opracowanie norm zharmonizowanych w ustalonym terminie, a ich podstawą powinien być konsensus. Jednakże w razie braku odpowiednich odniesień do norm zharmonizowanych Komisja

([28]) 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).

powinna mieć możliwość przyjęcia aktów wykonawczych ustanawiających wspólne specyfikacje dotyczące zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w niniejszym rozporządzeniu, pod warunkiem że dzieje się to z należytym poszanowaniem roli i funkcji europejskich organizacji normalizacyjnych, jako wyjątkowe rozwiązanie awaryjne ułatwiające producentowi spełnienie tych zasadniczych wymagań w zakresie cyberbezpieczeństwa w przypadku zablokowania procesu normalizacji lub w przypadku opóźnień w określeniu odpowiednich norm zharmonizowanych. Jeżeli takie opóźnienie wynika ze złożoności technicznej danej normy, Komisja powinna wziąć tę kwestię pod uwagę przed podjęciem decyzji o ustanowieniu wspólnych specyfikacji.

(84) Aby jak najskuteczniej ustanowić wspólne specyfikacje obejmujące zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzeniu, Komisja powinna zaangażować w ten proces odpowiednie zainteresowane strony.

(85) Rozsądny termin oznacza – w kontekście publikacji odniesienia do norm zharmonizowanych w *Dzienniku Urzędowym Unii Europejskiej* zgodnie z rozporządzeniem (UE) nr 1025/2012 – termin, w którym oczekuje się publikacji w *Dzienniku Urzędowym Unii Europejskiej* odniesienia do normy, jej sprostowania lub zmiany i który nie powinien przekraczać jednego roku po terminie opracowania normy europejskiej określonym zgodnie z rozporządzeniem (UE) nr 1025/2012.

(86) Aby ułatwić ocenę zgodności z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa 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.

(87) Stosowanie norm zharmonizowanych, wspólnych specyfikacji lub europejskich programów certyfikacji cyberbezpieczeństwa przyjętych na podstawie rozporządzenia (UE) 2019/881, zapewniających domniemanie zgodności w odniesieniu do zasadniczych wymagań w zakresie cyberbezpieczeństwa mających zastosowanie do produktów z elementami cyfrowymi, ułatwi producentom ocenę zgodności. Jeżeli producent zdecyduje się nie stosować takich środków w odniesieniu do niektórych wymogów, musi wskazać w swojej dokumentacji technicznej, w jaki inny sposób osiągnięto zgodność. Ponadto stosowanie przez producentów norm zharmonizowanych, wspólnych specyfikacji lub europejskich programów certyfikacji cyberbezpieczeństwa przyjętych na podstawie rozporządzenia (UE) 2019/881, zapewniających domniemanie zgodności ze strony producentów, ułatwiłoby organom nadzoru rynku kontrolę zgodności produktów z elementami cyfrowymi. W związku z tym producentów produktów z elementami cyfrowymi zachęca się do stosowania takich norm zharmonizowanych, wspólnych specyfikacji lub europejskich programów certyfikacji cyberbezpieczeństwa.

(88) Producenci powinni sporządzić deklarację zgodności UE zawierającą wymagane na podstawie niniejszego rozporządzenia informacje na temat zgodności produktów z elementami cyfrowymi z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu oraz, w stosownych przypadkach, w innym właściwym unijnym prawodawstwie harmonizacyjnym, którym objęty jest produkt z elementami cyfrowymi. Inne akty prawne 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 prawnymi 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.

(89) 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 ([29]). 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 określone w niniejszym rozporządzeniu.

(90) Aby podmioty gospodarcze mogły wykazać zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa 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

([29]) 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).

zgodności. Decyzją Parlamentu Europejskiego i Rady nr 768/2008/WE ([30]) 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 należy oprzeć procedury oceny zgodności odpowiednie do celów weryfikacji zgodności produktów z elementami cyfrowymi z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa 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 z elementami cyfrowymi.

(91) Ocena zgodności produktów z elementami cyfrowymi, które w niniejszym rozporządzeniu nie są wymienione jako ważne lub krytyczne produkty z elementami cyfrowymi, może być przeprowadzana przez producenta na własną odpowiedzialność zgodnie z procedurą kontroli wewnętrznej na podstawie modułu A określonego w decyzji 768/2008/WE zgodnie z niniejszym rozporządzeniem. Dotyczy to również przypadków, w których producent zdecyduje się nie stosować w całości lub w części obowiązującej normy zharmonizowanej, wspólnej specyfikacji lub europejskiego programu certyfikacji cyberbezpieczeństwa. Producent zachowuje elastyczność co do możliwości wyboru bardziej rygorystycznej procedury oceny zgodności z udziałem strony trzeciej. W ramach procedury oceny zgodności w kontekście kontroli wewnętrznej producent zapewnia i oświadcza, na swoją wyłączną odpowiedzialność, że produkt z elementami cyfrowymi i procesy producenta spełniają obowiązujące zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w niniejszym rozporządzeniu. Jeżeli ważny produkt z elementami cyfrowymi należy do klasy I, niezbędny jest zwiększony poziom pewności w celu wykazania zgodności z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu. Jeśli producent chce przeprowadzić ocenę zgodności na własną odpowiedzialność (moduł A), powinien stosować normy zharmonizowane, wspólne specyfikacje lub europejskie programy certyfikacji cyberbezpieczeństwa przyjęte na podstawie rozporządzenia (UE) 2019/881 wskazane przez Komisję w akcie wykonawczym. Jeśli producent nie stosuje takich norm zharmonizowanych, wspólnych specyfikacji ani europejskich programów certyfikacji cyberbezpieczeństwa, powinien przeprowadzić ocenę zgodności z udziałem strony trzeciej (w oparciu o moduły B i C lub moduł H). 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 na modułach B i C lub module H określonych w decyzji 768/2008/WE jako najbardziej odpowiednie do celów przeprowadzenia oceny zgodności ważnych produktów 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 użytkowaniem ważnych produktów z elementami cyfrowymi należących do klasy II, ocena zgodności powinna zawsze obejmować stronę trzecią, nawet jeżeli produkt jest w pełni lub częściowo zgodny z normami zharmonizowanymi, wspólnymi specyfikacjami lub europejskimi programami certyfikacji cyberbezpieczeństwa. Producenci ważnych produktów z elementami cyfrowymi sklasyfikowanych jako wolne i otwarte oprogramowanie powinni mieć możliwość stosowania procedury kontroli wewnętrznej opartej na module A, pod warunkiem że udostępnią publicznie dokumentację techniczną.

(92) O ile tworzenie materialnych produktów z elementami cyfrowymi zazwyczaj wymaga od producentów podejmowania istotnych starań na etapach projektowania, opracowywania i produkcji, o tyle 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 należy jeszcze 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 w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu na etapach projektowania, opracowywania i produkcji.

(93) Aby zapewnić proporcjonalność, w przypadku mikroprzedsiębiorstw i małych przedsiębiorstw należy zmniejszyć koszty administracyjne bez wpływu na poziom ochrony cyberbezpieczeństwa produktów z elementami cyfrowymi, które są objęte zakresem stosowania niniejszego rozporządzenia, ani na równe warunki działania dla producentów. Komisja powinna zatem opracować uproszczony formularz dokumentacji technicznej na potrzeby mikroprzedsiębiorstw i małych przedsiębiorstw. Uproszczony formularz dokumentacji technicznej przyjęty przez Komisję powinien zawierać wszystkie obowiązkowe elementy związane z dokumentacją techniczną przewidziane w niniejszym rozporządzeniu oraz określać, w jaki sposób mikroprzedsiębiorstwo lub małe przedsiębiorstwo może zwięźle przedstawić wymagane elementy, takie jak opis projektowania, opracowania i produkcji produktu z elementami cyfrowymi. Formularz taki przyczyniłby się tym samym do zmniejszenia obciążeń administracyjnych związanych z przestrzeganiem przepisów poprzez zapewnienie zainteresowanym przedsiębiorstwom pewności prawnej co do zakresu i szczegółowości przekazywanych informacji. Mikroprzedsiębiorstwa i małe przedsiębiorstwa powinny mieć możliwość wyboru, czy skorzystają z dostępnego im uproszczonego formularza, czy też przedstawią obowiązkowe elementy związane z dokumentacją techniczną w formie rozszerzonej.

([30]) 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).

(94) Aby promować i chronić innowacje, należy w szczególny sposób uwzględnić interesy producentów, którzy są mikroprzedsiębiorstwami lub małymi lub średnimi przedsiębiorstwami, w szczególności mikroprzedsiębiorstwami i małymi przedsiębiorstwami, w tym przedsiębiorstwami typu start-up. W tym celu państwa członkowskie mogą opracowywać inicjatywy skierowane do producentów, którzy są mikroprzedsiębiorstwami lub małymi przedsiębiorstwami, dotyczące między innymi szkoleń, podnoszenia świadomości, komunikacji informacyjnej, testowania i działań stron trzecich w zakresie oceny zgodności, a także tworzenia piaskownic. Tłumaczenia związane z dokumentacją obowiązkową, taką jak dokumentacja techniczna oraz informacje i instrukcje dla użytkownika wymagane na podstawie niniejszego rozporządzenia, a także z komunikacją z organami, mogą stanowić znaczne koszty dla producentów, w szczególności tych mniejszych. Dlatego państwa członkowskie powinny mieć możliwość zdecydowania, aby jednym z języków wskazanych i akceptowanych przez nie do celów dokumentacji sporządzanej przez odpowiednich producentów oraz komunikacji z producentami był język powszechnie rozumiany przez możliwie największą liczbę użytkowników.

(95) Aby ułatwić stosowanie niniejszego rozporządzenia, państwa członkowskie powinny dążyć do zadbania, aby przed datą rozpoczęcia stosowania niniejszego rozporządzenia istniała wystarczająca liczba jednostek notyfikowanych do przeprowadzania ocen zgodności przez stronę trzecią. Komisja powinna wspierać w tym państwa członkowskie i inne odnośne strony, aby uniknąć zatorów i przeszkód, które utrudniają producentom wejście na rynek. Ukierunkowane szkolenia organizowane przez państwa członkowskie, w tym w stosownych przypadkach przy wsparciu Komisji, mogą zwiększyć dostępność wykwalifikowanego personelu, w tym potrzebnego do wspierania działalności jednostek notyfikowanych na podstawie niniejszego rozporządzenia. Ponadto biorąc pod uwagę koszty, jakie może pociągać za sobą ocena zgodności przeprowadzana przez stronę trzecią, należy rozważyć dofinansowanie na poziomie unijnym i krajowym, które zmniejszy koszty ponoszone przez mikroprzedsiębiorstwa i małe przedsiębiorstwa.

(96) W trosce o proporcjonalność, jednostki oceniające zgodność powinny przy ustalaniu opłat za procedury oceny zgodności uwzględniać szczególne interesy i potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, w tym przedsiębiorstw typu start-up. Jednostki oceniające zgodność powinny zwłaszcza stosować odpowiednią procedurę sprawdzającą i testy przewidziane w niniejszym rozporządzeniu wyłącznie w stosownych przypadkach i zgodnie z podejściem opartym na analizie ryzyka.

(97) Celem tzw. piaskownic regulacyjnych powinno być wspieranie innowacji i konkurencyjności przedsiębiorstw dzięki stworzeniu kontrolowanych warunków do testowania różnych rozwiązań przed wprowadzeniem do obrotu produktów z elementami cyfrowymi. Piaskownice regulacyjne powinny służyć zwiększaniu pewności prawa z punktu widzenia wszystkich podmiotów objętych zakresem stosowania niniejszego rozporządzenia oraz ułatwiać i przyspieszać dostęp do unijnego rynku produktom z elementami cyfrowymi, zwłaszcza jeżeli oferują je mikroprzedsiębiorstwa i małe przedsiębiorstwa, w tym przedsiębiorstwa typu start-up.

(98) 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.

(99) 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.

(100) Jednostki oceniające zgodność, które akredytowano i notyfikowano na podstawie prawa Unii ustanawiającego wymogi podobne do wymogów zawartych w niniejszym rozporządzeniu, takie jak jednostka oceniająca zgodność notyfikowana w ramach europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego na podstawie rozporządzenia (UE) 2019/881 lub notyfikowana na podstawie rozporządzenia delegowanego (UE) 2022/30, powinny być ponownie oceniane i notyfikowane na podstawie niniejszego rozporządzenia. Właściwe organy mogą jednak zidentyfikować synergie w odniesieniu do pokrywających się wymogów, aby zapobiec niepotrzebnemu obciążeniu finansowemu i administracyjnemu oraz zadbać o sprawny i terminowy proces notyfikacji.

(101) 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.

(102) 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.

(103) Organ notyfikujący powinien wysłać notyfikację jednostki oceniającej zgodność Komisji i pozostałym państwom członkowskim za pomocą systemu informacyjnego NANDO („New Approach Notified and Designated Organisations"). System informacyjny NANDO jest elektronicznym narzędziem do notyfikacji, opracowanym i zarządzanym przez Komisję, w którym można znaleźć wykaz wszystkich jednostek notyfikowanych.

(104) 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.

(105) 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.

(106) Nadzór rynku jest instrumentem istotnym dla zapewnienia właściwego i jednolitego stosowania prawa Unii. Dlatego właściwe jest stworzenie ram prawnych, w których można odpowiednio sprawować nadzór nad rynkiem. Do produktów z elementami cyfrowymi objętymi zakresem niniejszego rozporządzenia stosuje się przepisy dotyczące nadzoru rynku unijnego oraz kontroli produktów wprowadzanych na rynek Unii przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/1020.

(107) Zgodnie z rozporządzeniem (UE) 2019/1020 nadzór rynku na terytorium danego państwa członkowskiego sprawuje wyznaczony przez nie organ nadzoru rynku. Niniejsze rozporządzenie nie powinno uniemożliwiać państwom członkowskim wyboru organów właściwych do wykonywania zadań w zakresie nadzoru rynku. Każde państwo członkowskie powinno wyznaczyć na swoim terytorium co najmniej jeden organ nadzoru rynku. Państwa członkowskie powinny móc wyznaczyć do pełnienia funkcji organu nadzoru rynku dowolny istniejący lub nowy organ, w tym właściwe organy wyznaczone lub utworzone zgodnie z art. 8 dyrektywy (UE) 2022/2555, wyznaczone krajowe organy ds. certyfikacji cyberbezpieczeństwa wyznaczone zgodnie z art. 58 rozporządzenia (UE) 2019/881 lub organy nadzoru rynku wyznaczone do celów dyrektywy 2014/53/UE. 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 rynku 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.

(108) Na podstawie art. 30 ust. 2 rozporządzenia (UE) 2019/1020 należy ustanowić specjalną grupę ADCO zajmującą się cyberodpornością produktów z elementami cyfrowymi 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 wspierać współpracę między organami nadzoru rynku i zachęcać do takiej współpracy za pośrednictwem Unijnej Sieci ds. Zgodności Produktów ustanowionej zgodnie z 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 tego rozporządzenia, oraz – fakultatywnie – eksperta krajowego, przewodniczących grup ADCO oraz przedstawicieli Komisji. Komisja powinna uczestniczyć w posiedzeniach Unijnej Sieci ds. Zgodności Produktów, jej podgrup i odpowiedniej grupy ADCO. Powinna także wspierać grupę ADCO za pośrednictwem sekretariatu wykonawczego zapewniającego wsparcie techniczne i logistyczne. Grupa ADCO może również zaprosić niezależnych ekspertów do udziału w pracach i kontaktować się z innymi grupami ADCO, takimi jak grupa ustanowiona na mocy dyrektywy 2014/53/UE.

(109) Organy nadzoru rynku, za pośrednictwem grupy ADCO ustanowionej na mocy niniejszego rozporządzenia, powinny ściśle ze sobą współpracować i mieć możliwość przygotowania wytycznych, które ułatwią nadzór rynku na poziomie krajowym, np. dzięki opracowaniu najlepszych praktyk i wskaźników do skutecznego kontrolowania zgodności produktów z elementami cyfrowymi z niniejszym rozporządzeniem.

(110) W celu zapewnienia terminowych, proporcjonalnych i skutecznych środków dotyczących produktów z elementami cyfrowymi stwarzającymi istotne ryzyko w cyberprzestrzeni należy wprowadzić 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.

(111) 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 art. 3 ust. 1 dyrektywy (UE) 2022/2555, 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 lub odzyskania produktu lub wycofania go, w zależności od ryzyka. Gdy tylko organ nadzoru rynku ograniczy swobodny przepływ lub zakaże swobodnego przepływu produktu z elementami cyfrowymi, 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 stwarzających ryzyko produktów z elementami cyfrowymi, 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 powinna również rozważyć przyjęcie wniosków dotyczących zmiany właściwych przepisów Unii.

(112) 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, dla wypełnienia obowiązków wynikających z prawa Unii lub prawa krajowego mających na celu ochronę praw podstawowych, albo dla dostępności, autentyczności, integralności lub poufności usług oferowanych przy użyciu elektronicznego systemu informacyjnego przez podmioty kluczowe, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555, Komisja powinna móc zwrócić się do ENISA o przeprowadzenie oceny. Na podstawie tej oceny Komisja powinna móc przyjąć, w drodze aktów wykonawczych, środki naprawcze lub ograniczające na poziomie Unii, w tym nakaz wycofania z obrotu lub odzyskania przedmiotowych produktów z elementami cyfrowymi w rozsądnym terminie, stosownym do charakteru ryzyka. Komisja powinna móc 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 rynku nie wprowadziły żadnych skutecznych środków w celu zaradzenia sytuacji. Takimi wyjątkowymi okolicznościami mogą być sytuacje nadzwyczajne, w których przykładowo niezgodny produkt z elementami cyfrowymi jest szeroko udostępniany przez producenta w kilku państwach członkowskich i wykorzystywany także w kluczowych sektorach przez podmioty objęte zakresem dyrektywy (UE) 2022/2555, 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 powinna móc interweniować wyłącznie na czas trwania wyjątkowych okoliczności oraz jeśli niezgodność z niniejszym rozporządzeniem lub istotne ryzyko stwarzane przez produkt się utrzymują.

(113) Jeżeli 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.

(114) 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 z elementami cyfrowymi są często uznawane za stwarzające ryzyko w cyberprzestrzeni. Ponadto przy określaniu kategorii produktów podlegających akcjom kontrolnym organy nadzoru rynku powinny wziąć również pod uwagę okoliczności związane z pozatechnicznymi czynnikami ryzyka. Dlatego organy nadzoru rynku powinny móc uwzględnić wyniki skoordynowanego na poziomie Unii szacowania ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzonego zgodnie z art. 22 dyrektywy (UE) 2022/2555, w tym okoliczności związane z pozatechnicznymi czynnikami ryzyka. ENISA powinna składać wnioski dotyczące kategorii produktów z elementami cyfrowymi, w odniesieniu do których organy nadzoru rynku mogą organizować akcje kontrolne, między innymi na podstawie otrzymywanych zgłoszeń podatności oraz incydentów.

(115) Zważywszy na jej wiedzę specjalistyczną i mandat, ENISA powinna mieć możliwość wspierania procesu wdrażania niniejszego rozporządzenia. W szczególności ENISA 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 akcje kontrolne. W wyjątkowych okolicznościach ENISA powinna mieć, na wniosek Komisji, 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.

(116) Na mocy niniejszego rozporządzenia powierza się ENISA pewne zadania, które wymagają odpowiednich zasobów zarówno pod względem wiedzy fachowej, jak i zasobów kadrowych, aby umożliwić ENISA ich skuteczne wykonywanie. Przygotowując projekt budżetu ogólnego Unii, Komisja zaproponuje niezbędne zasoby budżetowe na potrzeby planu zatrudnienia ENISA, zgodnie z procedurą określoną w art. 29 rozporządzenia (UE) 2019/881. W trakcie tych przygotowań Komisja rozważy ogólne zasoby ENISA, aby umożliwić jej wykonywanie zadań, w tym zadań powierzonych jej na mocy niniejszego rozporządzenia.

(117) Aby w razie potrzeby zapewnić możliwość dostosowania ram regulacyjnych, należy przekazać Komisji uprawnienia do przyjmowania na podstawie art. 290 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) aktów w celu aktualizacji zawartego w załączniku do niniejszego rozporządzenia wykazu ważnych produktów z elementami cyfrowymi. 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, wraz ze wskazaniem, czy konieczne jest ograniczenie lub wyłączenie z zakresu niniejszego rozporządzenia, jak również – w stosownych przypadkach – zakresu tego ograniczenia. Należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z tym artykułem w odniesieniu do potencjalnego zobowiązania do certyfikacji w europejskim programie certyfikacji cyberbezpieczeństwa produktów krytycznych z elementami cyfrowymi określonych w załączniku do niniejszego rozporządzenia, a także do aktualizacji wykazu produktów krytycznych z elementami cyfrowymi w oparciu o kryteria krytyczności wskazane w niniejszym rozporządzeniu i do określenia europejskich programów certyfikacji cyberbezpieczeństwa przyjętych na podstawie rozporządzenia (UE) 2019/881, które mogą być stosowane do wykazania zgodności z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku do niniejszego rozporządzenia lub z ich częściami. Należy również przekazać Komisji uprawnienia do przyjmowania aktów w celu określenia minimalnego okresu wsparcia dla określonych kategorii produktów, jeżeli dane z nadzoru rynku wskazują, że te okresy są nieodpowiednie, a także w celu określenia warunków opóźnienia rozpowszechniania powiadomień o aktywnie wykorzystywanych podatnościach ze względu na ryzyko w cyberprzestrzeni. Ponadto należy przekazać Komisji uprawnienia do przyjmowania aktów w celu ustanowienia dobrowolnych programów poświadczania bezpieczeństwa na potrzeby oceny zgodności produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie z wszystkimi lub niektórymi zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa lub innymi obowiązkami określonymi w niniejszym rozporządzeniu, a także w celu 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 ([31]). 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. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w niniejszym rozporządzeniu, powinno się powierzyć Komisji na okres pięciu lat od dnia 10 grudnia 2024 r. Komisja powinna sporządzić sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem pięcioletniego okresu. Przekazanie uprawnień powinno zostać automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.

(118) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze w zakresie: określania opisu technicznego kategorii ważnych produktów z elementami cyfrowymi wymienionych w załączniku do niniejszego rozporządzenia, określania formatu i elementów zestawienia podstawowych materiałów do produkcji oprogramowania, dokładniejszego określenia formatu zgłoszeń aktywnie wykorzystywanych podatności oraz poważnych incydentów – i procedury ich składania – mających wpływ na bezpieczeństwo produktów z elementami cyfrowymi przekazywanych przez producentów, ustanowienia wspólnych specyfikacji obejmujących wymogi techniczne, które zapewnią środki umożliwiające spełnienie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku do niniejszego rozporządzenia, określania specyfikacji technicznych dotyczących etykiet, piktogramów lub wszelkich innych znaków związanych z bezpieczeństwem produktów z elementami cyfrowymi, ich okresu wsparcia oraz mechanizmów służących promowaniu ich wykorzystania i zwiększania świadomości społecznej na temat bezpieczeństwa produktów z elementami cyfrowymi, określania uproszczonego formularza na potrzeby mikroprzedsiębiorstw i małych przedsiębiorstw oraz podejmowania decyzji o zastosowaniu środków naprawczych lub ograniczających na poziomie

([31]) Dz.U. L 123 z 12.5.2016, s. 1.

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 ([32]).

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

(120) 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 czy producent jest mikroprzedsiębiorstwem lub małym lub średnim przedsiębiorstwem, w tym przedsiębiorstwem typu start-up, i czy wobec tego samego podmiotu gospodarczego za podobne naruszenia te same lub 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. Biorąc pod uwagę, że do mikroprzedsiębiorstw lub małych przedsiębiorstw nie mają zastosowania administracyjne kary pieniężne za niedotrzymanie 24-godzinnego terminu wczesnego ostrzegania o aktywnie wykorzystywanych podatnościach lub poważnych incydentach mających wpływ na bezpieczeństwo produktu z elementami cyfrowymi, a do opiekunów otwartego oprogramowania nie mają zastosowania takie kary za naruszenia niniejszego rozporządzenia, oraz z zastrzeżeniem zasady, że kary powinny być skuteczne, proporcjonalne i odstraszające, państwa członkowskie nie powinny nakładać na te podmioty innych rodzajów kar o charakterze pieniężnym.

(121) Jeżeli administracyjne kary pieniężne są nakładane na osobę niebędącą 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.

(122) Państwa członkowskie powinny zbadać, biorąc pod uwagę uwarunkowania krajowe, możliwość wykorzystania dochodów z kar przewidzianych w niniejszym rozporządzeniu lub ich odpowiedników finansowych do wspierania polityki cyberbezpieczeństwa i zwiększenia jego poziomu w Unii, między innymi poprzez zwiększenie liczby wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa, wzmocnienie potencjału mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, a także zwiększenie świadomości społecznej na temat cyberzagrożeń.

(123) W stosunkach z państwami trzecimi Unia 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 obowiązują umowy o wzajemnym uznawaniu z kilkoma krajami trzecimi. 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 partnerskimi krajami trzecimi, gdyż w perspektywie długoterminowej przyczyni się ona do wzmocnienia ram cyberbezpieczeństwa zarówno w Unii, jak i poza nią.

([32]) 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(124) Konsumenci powinni być uprawnieni, w odniesieniu do obowiązków nałożonych na podmioty gospodarcze zgodnie z niniejszym rozporządzeniem, do egzekwowania swoich praw w drodze powództw przedstawicielskich zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2020/1828 ([33]). W tym celu niniejsze rozporządzenie powinno stanowić, że dyrektywa (UE) 2020/1828 ma zastosowanie do powództw przedstawicielskich dotyczących naruszeń niniejszego rozporządzenia, które szkodzą lub mogą szkodzić zbiorowym interesom konsumentów. Należy w związku z tym wprowadzić odpowiednie zmiany w załączniku I do tej dyrektywy. Do państw członkowskich należy dopilnowanie, aby zmiany te zostały uwzględnione w środkach transpozycji przyjętych zgodnie z tą dyrektywą, chociaż przyjęcie krajowych środków transpozycji nie jest warunkiem stosowania dyrektywy do tych powództw przedstawicielskich. Stosowanie tej dyrektywy do powództw przedstawicielskich wytaczanych w związku z naruszeniami przepisów niniejszego rozporządzenia przez podmioty gospodarcze, szkodzącymi lub mogącymi szkodzić zbiorowym interesom konsumentów, powinno się rozpocząć dnia 11 grudnia 2027 r.

(125) Komisja powinna okresowo dokonywać oceny i przeglądu niniejszego rozporządzenia, w drodze konsultacji z odpowiednimi zainteresowanymi stronami, w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się warunków społecznych, politycznych, technologicznych lub rynkowych. Niniejsze rozporządzenie ułatwi podmiotom objętym zakresem rozporządzenia (UE) 2022/2554 i dyrektywy (UE) 2022/2555, które wykorzystują produkty z elementami cyfrowymi, wypełnianie obowiązków w zakresie bezpieczeństwa łańcucha dostaw. W ramach okresowego przeglądu Komisja powinna ocenić łączne skutki unijnych przepisów o cyberbezpieczeństwie.

(126) Podmiotom gospodarczym należy zapewnić wystarczająco dużo czasu na dostosowanie się do wymogów określonych w niniejszym rozporządzeniu. Niniejsze rozporządzenie powinno mieć zastosowanie od dnia 11 grudnia 2027 r., z wyjątkiem obowiązków w zakresie zgłaszania aktywnie wykorzystywanych podatności oraz poważnych incydentów mających wpływ na bezpieczeństwo produktów z elementami cyfrowymi, które powinny mieć zastosowanie od dnia 11 września 2026 r., oraz przepisów w sprawie notyfikacji jednostek oceniających zgodność, które powinny mieć zastosowanie od dnia 11 czerwca 2026 r.

(127) Ważne jest, aby zapewnić mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom, w tym przedsiębiorstwom typu start-up, wsparcie we wdrażaniu niniejszego rozporządzenia oraz zminimalizować ryzyko wynikające dla jego wdrażania z braku wiedzy fachowej na rynku, a także aby ułatwić producentom wypełnianie obowiązków określonych w niniejszym rozporządzeniu. Program „Cyfrowa Europa" i inne odpowiednie programy unijne oferują wsparcie finansowe i techniczne, które umożliwia tym przedsiębiorstwom przyczynianie się do wzrostu gospodarki Unii i do podniesienia wspólnego poziomu cyberbezpieczeństwa w Unii. Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa i krajowe ośrodki koordynacji, a także europejskie centra innowacji cyfrowych ustanowione przez Komisję i państwa członkowskie na poziomie unijnym lub krajowym mogłyby również wspierać przedsiębiorstwa i organizacje sektora publicznego oraz pomóc we wdrażaniu niniejszego rozporządzenia. W ramach swoich misji i obszarów kompetencji mogłyby one oferować wsparcie techniczne i naukowe mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom, np. w dziedzinie testów i ocen zgodności przeprowadzanych przez strony trzecie. Mogłyby również pomagać w stosowaniu narzędzi ułatwiających wdrażanie niniejszego rozporządzenia.

(128) Ponadto państwa członkowskie powinny rozważyć dodatkowe działania na rzecz przygotowania wytycznych i wsparcia mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, na przykład tworząc dla nich piaskownice regulacyjne i specjalne kanały komunikacji. Aby podnieść poziom cyberbezpieczeństwa w Unii, państwa członkowskie mogą również rozważyć zaoferowanie wsparcia na rzecz rozwoju zdolności i umiejętności związanych z cyberbezpieczeństwem produktów z elementami cyfrowymi, poprawę cyberodporności podmiotów gospodarczych, w szczególności mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, oraz zwiększanie świadomości społecznej na temat cyberbezpieczeństwa produktów z elementami cyfrowymi.

(129) 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.

(130) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 Parlamentu Europejskiego i Rady ([34]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który w dniu 9 listopada 2022 r. ([35]) wydał opinię,

([33]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2020/1828 z dnia 25 listopada 2020 r. w sprawie powództw przedstawicielskich wytaczanych w celu ochrony zbiorowych interesów konsumentów i uchylająca dyrektywę 2009/22/WE (Dz.U. L 409 z 4.12.2020, s. 1).

([34]) 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).

([35]) Dz.U. C 452 z 29.11.2022, s. 23.

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu ustanawia się:

a) przepisy dotyczące udostępniania na rynku produktów z elementami cyfrowymi w celu zapewnienia cyberbezpieczeństwa takich produktów;

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

c) zasadnicze wymagania w zakresie cyberbezpieczeństwa dotyczące wprowadzanych przez producentów procedur postępowania w przypadku wykrycia podatności w celu zapewnienia cyberbezpieczeństwa produktów z elementami cyfrowymi przez okres oczekiwanego użytkowania produktu oraz obowiązki podmiotów gospodarczych w odniesieniu do tych procedur;

d) przepisy dotyczące nadzoru rynku, w tym monitorowania, i egzekwowania wymienionych w niniejszym artykule przepisów i wymagań.

Artykuł 2

Zakres

1. Niniejsze rozporządzenie stosuje się do udostępnianych na rynku 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 prawne Unii:

a) rozporządzenie (UE) 2017/745;

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. Niniejszego rozporządzenia nie stosuje się do urządzeń objętych zakresem dyrektywy Parlamentu Europejskiego i Rady 2014/90/UE ([36]).

5. Stosowanie niniejszego rozporządzenia do produktów z elementami cyfrowymi objętych innymi przepisami unijnymi ustanawiającymi wymogi odnoszące się do wszystkich lub niektórych rodzajów ryzyka objętych zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa 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 lub wyższy poziom ochrony niż przewidziany w niniejszym rozporządzeniu.

Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 61 w celu uzupełnienia niniejszego rozporządzenia przez określenie, czy takie ograniczenie lub wyłączenie jest niezbędne, określenie odnośnych produktów i przepisów, jak również – w stosownych przypadkach – zakresu ograniczenia.

([36]) Dyrektywa Parlamentu Europejskiego i Rady 2014/90/UE z dnia 23 lipca 2014 r. w sprawie wyposażenia morskiego i uchylająca dyrektywę Rady 96/98/WE (Dz.U. L 257 z 28.8.2014, s. 146).

6. Niniejsze rozporządzenie nie stosuje się do części zamiennych, które są udostępniane na rynku w celu wymiany identycznych komponentów produktów z elementami cyfrowymi i które są wytwarzane zgodnie z tymi samymi specyfikacjami co komponenty, które mają wymienić.

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

8. Obowiązki ustanowione w niniejszym rozporządzeniu nie wiążą się z dostarczaniem informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności państw członkowskich.

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 są oddzielnie wprowadzane 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) „cyberbezpieczeństwo" oznacza cyberbezpieczeństwo zdefiniowane w art. 2 pkt 1 rozporządzenia (UE) 2019/881;

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

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

6) „komponent" oznacza oprogramowanie lub sprzęt przeznaczone do zintegrowania z elektronicznym systemem informacyjnym;

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

8) „połączenie logiczne" oznacza wirtualną reprezentację połączenia danych zrealizowanego za pośrednictwem interfejsu oprogramowania;

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

10) „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;

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

12) „podmiot gospodarczy" oznacza producenta, upoważnionego przedstawiciela, importera, dystrybutora lub każdą inną osobę fizyczną lub prawną podlegającą obowiązkom związanym z wytwarzaniem produktów z elementami cyfrowymi lub udostępnianiem produktów z elementami cyfrowymi na rynku zgodnie z niniejszym rozporządzeniem;

13) „producent" oznacza 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 handlową lub znakiem towarowym, za opłatą, na zasadzie monetyzacji lub bezpłatnie;

14) „opiekun oprogramowania otwartego" oznacza osobę prawną inną niż producent, której celem jest systematyczne i stałe wsparcie na rzecz opracowywania konkretnych produktów z elementami cyfrowymi, kwalifikujących się jako wolne i otwarte oprogramowanie oraz przeznaczonych do celów komercyjnych, oraz która zapewnia prawidłowe funkcjonowanie tych produktów;

15) „upoważniony przedstawiciel" oznacza osobę fizyczną lub prawną, która ma miejsce zamieszkania lub siedzibę w Unii i otrzymała pisemne pełnomocnictwo producenta do wykonywania w jego imieniu określonych zadań;

16) „importer” oznacza 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;

17) „dystrybutor” oznacza 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;

18) „konsument” oznacza osobę fizyczną działającą w celach niezwiązanych z jej działalnością handlową, gospodarczą, rzemieślniczą lub zawodową;

19) „mikroprzedsiębiorstwa”, „małe przedsiębiorstwa” oraz „średnie przedsiębiorstwa” oznaczają, odpowiednio, mikroprzedsiębiorstwa, małe przedsiębiorstwa i średnie przedsiębiorstwa zgodnie z definicją zawartą w załączniku do zalecenia 2003/361/WE;

20) „okres wsparcia” oznacza okres, w którym producent jest zobowiązany zapewniać, aby na podatności w zabezpieczeniach produktu z elementami cyfrowymi reagowano skutecznie i zgodnie z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część II;

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

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

23) „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;

24) „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 najpewniej wynika z dającego się racjonalnie przewidzieć zachowania człowieka, operacji technicznych lub interakcji;

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

26) „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;

27) „ocena zgodności” oznacza proces weryfikacji, czy spełniono zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I;

28) „jednostka oceniająca zgodność” oznacza jednostkę oceniającą zgodność w rozumieniu art. 2 pkt 13 rozporządzenia (WE) nr 765/2008;

29) „jednostka notyfikowana” oznacza jednostkę oceniającą zgodność wyznaczoną zgodnie z art. 43 i innym stosownym unijnym prawodawstwem harmonizacyjnym;

30) „istotna modyfikacja” oznacza zmianę w produkcie z elementami cyfrowymi po jego wprowadzeniu do obrotu, która wpływa na zgodność produktu z elementami cyfrowymi z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część I lub która powoduje zmianę przeznaczenia, w odniesieniu do którego oceniono produkt z elementami cyfrowymi;

31) „oznakowanie zgodności CE” oznacza oznakowanie, za pomocą którego producent wskazuje, że produkt z elementami cyfrowymi i procedury wprowadzone przez producenta spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I i innym mającym zastosowanie unijnym prawodawstwie harmonizacyjnym przewidującym umieszczanie takiego oznakowania;

32) „unijne prawodawstwo harmonizacyjne” oznacza przepisy Unii wymienione w załączniku I do rozporządzenia (UE) 2019/1020 oraz wszelkie inne przepisy Unii harmonizujące warunki wprowadzania do obrotu produktów, do których to rozporządzenie ma zastosowanie;

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

34) „norma międzynarodowa” oznacza normę międzynarodową zgodnie z definicją w art. 2 pkt 1 lit. a) rozporządzenia (UE) nr 1025/2012;

35) „norma europejska” oznacza normę europejską zgodnie z definicją w art. 2 pkt 1 lit. b) rozporządzenia (UE) nr 1025/2012;

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

37) „ryzyko w cyberprzestrzeni” oznacza potencjalną stratę lub potencjalne zakłócenie spowodowane incydentem i ma być wyrażone jako wypadkowa skali takiej straty lub zakłócenia oraz prawdopodobieństwa wystąpienia takiego incydentu;

38) „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;

39) „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;

40) „podatność” oznacza słabość, wrażliwość lub wadę produktu z elementami cyfrowymi, które można wykorzystać podczas cyberzagrożenia;

41) „nadająca się do wykorzystania podatność” oznacza podatność, która może zostać skutecznie wykorzystana przez atakującego w praktycznych warunkach eksploatacji;

42) „aktywnie wykorzystywana podatność” oznacza podatność, w przypadku której istnieją wiarygodne dowody, że podmiot działający w złych zamiarach wykorzystał ją w systemie bez zgody właściciela systemu;

43) „incydent” oznacza incydent zgodnie z definicją w art. 6 pkt 6 dyrektywy (UE) 2022/2555;

44) „incydent wywierający wpływ na bezpieczeństwo produktu z elementami cyfrowymi” oznacza incydent, który negatywnie wpływa lub może mieć negatywny wpływ na zdolność produktu z elementami cyfrowymi do ochrony dostępności, autentyczności, integralności lub poufności danych lub funkcji;

45) „potencjalne zdarzenie dla cyberbezpieczeństwa” oznacza potencjalne zdarzenie dla cyberbezpieczeństwa zgodnie z definicją w art. 6 pkt 5 dyrektywy (UE) 2022/2555;

46) „cyberzagrożenie” oznacza cyberzagrożenie zgodnie z definicją w art. 2 pkt 8 rozporządzenia (UE) 2019/881;

47) „dane osobowe” oznaczają dane osobowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

48) „wolne i otwarte oprogramowanie” oznacza oprogramowanie, którego kod źródłowy jest powszechnie dostępny, oferowane bezpłatnie i na otwartej licencji, która zapewnia wszystkim prawo do wolnego dostępu do niego, używania go, modyfikowania i redystrybucji;

49) „odzyskanie produktu” oznacza odzyskanie produktu zgodnie z definicją w art. 3 pkt 22 rozporządzenia (UE) 2019/1020;

50) „wycofanie z obrotu” oznacza wycofanie z obrotu zgodnie z definicją w art. 3 pkt 23 rozporządzenia (UE) 2019/1020;

51) „CSIRT wyznaczony jako koordynator” oznacza CSIRT wyznaczony na koordynatora zgodnie z art. 12 ust. 1 dyrektywy (UE) 2022/2555.

Artykuł 4

Swobodny przepływ

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

2. Podczas targów, wystaw, pokazów lub podobnych imprez państwa członkowskie nie uniemożliwiają prezentowania ani używania produktu z elementami cyfrowymi, który nie jest zgodny z niniejszym rozporządzeniem, w tym jego prototypów, pod warunkiem że dany produkt ma widoczne oznaczenie, które wskazuje, że nie jest on zgodny z niniejszym rozporządzeniem i nie będzie udostępniany na rynku, zanim nie będzie z nim zgodny.

3. Państwa członkowskie nie uniemożliwiają udostępniania na rynku nieukończonego oprogramowania, które nie jest zgodne z niniejszym rozporządzeniem, pod warunkiem że oprogramowanie to jest udostępniane jedynie na ograniczony okres wymagany do celów testowania wraz z widocznym oznaczeniem wyraźnie wskazującym, że nie jest ono zgodne z niniejszym rozporządzeniem i nie jest dostępne na rynku do celów innych niż testowanie.

4. Ust. 3 nie stosuje się do elementów bezpieczeństwa, o których mowa w unijnym prawodawstwie harmonizacyjnym innym niż niniejsze rozporządzenie.

Artykuł 5

Zamawianie lub stosowanie produktów z elementami cyfrowymi

1. Niniejsze rozporządzenie nie uniemożliwia państwom członkowskim objęcia produktów z elementami cyfrowymi dodatkowymi wymaganiami w zakresie cyberbezpieczeństwa przy zamawianiu lub stosowaniu tych produktów do konkretnych celów, w tym gdy produkty te są zamawiane lub stosowane do celów bezpieczeństwa narodowego lub obronności, pod warunkiem że takie wymagania są zgodne z obowiązkami państw członkowskich określonymi w prawie Unii oraz że są niezbędne i proporcjonalne do osiągnięcia tych celów.

2. Bez uszczerbku dla dyrektyw 2014/24/UE i 2014/25/UE, jeżeli zamawia się produkty z elementami cyfrowymi objęte zakresem niniejszego rozporządzenia, państwa członkowskie zapewniają, aby w procedurze udzielania zamówień przestrzegano zgodności z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I do niniejszego rozporządzenia, w tym zdolności producentów do skutecznego reagowania na podatności.

Artykuł 6

Wymagania dotyczące produktów z elementami cyfrowymi

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

a) spełniają one zasadnicze wymagania w zakresie cyberbezpieczeństwa przewidziane w załączniku I część 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 – zainstalowano stosowne aktualizacje zabezpieczeń; oraz

b) procedury wprowadzone przez producenta są zgodne z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część II.

Artykuł 7

Ważne produkty z elementami cyfrowymi

1. Produkty z elementami cyfrowymi, które posiadają podstawową funkcjonalność kategorii produktów określonej w załączniku III, uznaje się za ważne produkty z elementami cyfrowymi i podlegają one procedurom oceny zgodności, o których mowa w art. 32 ust. 2 i 3. Włączenie produktu z elementami cyfrowymi, który posiada podstawową funkcjonalność kategorii produktów określonej w załączniku III, samo w sobie nie powoduje, że produkt, z którym jest on zintegrowany, podlega procedurom oceny zgodności, o których mowa w art. 32 ust. 2 i 3.

2. Kategorie produktów z elementami cyfrowymi, o których mowa w ust. 1 niniejszego artykułu, podzielone na klasy I i II określone w załączniku III spełniają co najmniej jedno z następujących kryteriów:

a) produkt z elementami cyfrowymi pełni przede wszystkim funkcje kluczowe dla cyberbezpieczeństwa innych produktów, sieci lub usług, takie jak zabezpieczanie uwierzytelniania i dostępu, zapobieganie włamaniom i ich wykrywanie, ochrona punktów końcowych lub ochrona sieci;

b) produkt z elementami cyfrowymi pełni funkcję, taką jak funkcja systemu centralnego, w tym zarządzanie siecią, kontrola konfiguracji, wirtualizacja lub przetwarzanie danych osobowych, która wiąże się ze znacznym ryzykiem wystąpienia niekorzystnych skutków pod względem intensywności i zdolności do zakłócenia, kontrolowania lub spowodowania szkód w dużej liczbie innych produktów lub może zaszkodzić zdrowiu, bezpieczeństwu lub ochronie użytkowników poprzez bezpośrednią manipulację.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 61 w celu zmiany załącznika III przez uwzględnienie w wykazie nowej kategorii w każdej klasie kategorii produktów z elementami cyfrowymi i określenie ich definicji, przeniesienie kategorii produktów z jednej klasy do drugiej lub usunięcie z tego wykazu istniejącej kategorii. Przy ocenianiu potrzeby zmiany wykazu zawartego w załączniku III Komisja bierze pod uwagę funkcjonalności związane z cyberbezpieczeństwem lub funkcję oraz poziom ryzyka w cyberprzestrzeni, który stwarzają produkty z elementami cyfrowymi, jak określono w kryteriach, o których mowa w ust. 2 niniejszego artykułu.

Akty delegowane, o których mowa w akapicie pierwszym niniejszego ustępu, przewidują w stosownych przypadkach minimalny okres przejściowy wynoszący 12 miesięcy, w szczególności gdy do klasy I lub II dodaje się nową kategorię ważnych produktów z elementami cyfrowymi lub przenosi z klasy I do II, jak określono w załączniku III, przed rozpoczęciem stosowania odpowiednich procedur oceny zgodności, o których mowa w art. 32 ust. 2 i 3, chyba że szczególnie pilna potrzeba uzasadnia skrócenie okresu przejściowego.

4. Do dnia 11 grudnia 2025 r. Komisja przyjmuje akt wykonawczy zawierający techniczny opis kategorii produktów z elementami cyfrowymi w klasach I i II określonych w załączniku III oraz opis techniczny kategorii produktów z elementami cyfrowymi określonych w załączniku IV. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

Artykuł 8

Produkty krytyczne z elementami cyfrowymi

1. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 61 w celu uzupełnienia niniejszego rozporządzenia i określenia, które produkty z elementami cyfrowymi posiadające podstawową funkcjonalność kategorii produktu określonej w załączniku IV do niniejszego rozporządzenia mają być zobowiązane do uzyskania europejskiego certyfikatu cyberbezpieczeństwa co najmniej na „istotnym" poziomie uzasadnienia zaufania w ramach europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego na podstawie rozporządzenia (UE) 2019/881 w celu wykazania zgodności z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I do niniejszego rozporządzenia lub jego częściach, pod warunkiem że europejski program certyfikacji cyberbezpieczeństwa obejmujący te kategorie produktów z elementami cyfrowymi został przyjęty na podstawie rozporządzenia (UE) 2019/881 i jest on dostępny producentom. W aktach delegowanych określa się wymagany poziom zaufania, który jest proporcjonalny do poziomu ryzyka w cyberprzestrzeni związanego z produktami z elementami cyfrowymi i uwzględnia ich przeznaczenie, w tym krytyczną zależność od nich podmiotów kluczowych, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555.

Przed przyjęciem aktów delegowanych Komisja ocenia potencjalny wpływ planowanych środków na rynek i przeprowadza konsultacje z odpowiednimi interesariuszami, w tym z Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa, ustanowionej na mocy rozporządzenia (UE) 2019/881. W ocenie uwzględnia się gotowość i zdolność państw członkowskich do wdrożenia odpowiedniego europejskiego programu certyfikacji cyberbezpieczeństwa. Jeżeli nie przyjęto aktów delegowanych, o których mowa w akapicie pierwszym niniejszego ustępu, produkty z elementami cyfrowymi, które posiadają podstawową funkcjonalność kategorii produktu określonej w załączniku IV, podlegają procedurom oceny zgodności, o których mowa w art. 32 ust. 3.

Akty delegowane, o których mowa w akapicie pierwszym, przewidują co najmniej sześciomiesięczny okres przejściowy, chyba że szczególnie pilna potrzeba uzasadnia jego skrócenie.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 61 oraz do wprowadzania zmian w załączniku IV przez dodanie lub usunięcie kategorii produktów krytycznych z elementami cyfrowymi. Określając takie kategorie produktów krytycznych z elementami cyfrowymi i wymagany poziom zaufania, zgodnie z ust. 1 niniejszego artykułu, Komisja bierze pod uwagę kryteria, o których mowa w art. 7 ust. 2, oraz zapewnia, aby kategorie produktów z elementami cyfrowymi spełniały co najmniej jedno z następujących kryteriów:

a) krytyczną zależność podmiotów kluczowych, o których mowa w art. 3 dyrektywy (UE) 2022/2555 od kategorii produktów z elementami cyfrowymi;

b) incydenty i wykorzystane podatności dotyczące kategorii produktów z elementami cyfrowymi, które mogą prowadzić do poważnych zakłóceń w krytycznych łańcuchach dostaw na całym rynku wewnętrznym.

Przed przyjęciem aktów delegowanych Komisja przeprowadza ocenę, o której mowa w ust. 1.

Akty delegowane, o których mowa w akapicie pierwszym, przewidują co najmniej sześciomiesięczny okres przejściowy, chyba że szczególnie pilna potrzeba uzasadnia jego skrócenie.

Artykuł 9

Konsultacje z interesariuszami

1. Przygotowując środki do wdrożenia niniejszego rozporządzenia, Komisja konsultuje się z odpowiednimi interesariuszami, takimi jak właściwe organy państw członkowskich, przedsiębiorstwa sektora prywatnego, w tym mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, środowiska opracowujące otwarte oprogramowanie, organizacje konsumenckie, środowiska akademickie oraz odpowiednie agencje i organy Unii, a także grupy eksperckie ustanowione na poziomie unijnym, oraz bierze pod uwagę ich opinie. W stosownych przypadkach Komisja konsultuje się z interesariuszami i zasięga ich opinii w ustrukturyzowany sposób, w przypadku gdy:

a) przygotowuje wytyczne, o których mowa w art. 26;

b) przygotowuje opisy techniczne kategorii produktów określonych w załączniku III zgodnie z art. 7 ust. 4, ocenia konieczność ewentualnych aktualizacji wykazu kategorii produktów zgodnie z art. 7 ust. 3 i art. 8 ust. 2 lub ocenia potencjalny wpływ na rynek, o którym mowa w art. 8 ust. 1, bez uszczerbku dla art. 61;

c) przygotowuje się do oceny i przeglądu niniejszego rozporządzenia.

2. Co najmniej raz w roku Komisja organizuje regularne konsultacje i sesje informacyjne, aby poznać opinie interesariuszy, o których mowa w ust. 1, na temat wdrażania niniejszego rozporządzenia.

Artykuł 10

Doskonalenie umiejętności w cyberodpornym środowisku cyfrowym

Do celów niniejszego rozporządzenia oraz aby odpowiedzieć na potrzeby specjalistów we wspomaganiu wdrażania niniejszego rozporządzenia, państwa członkowskie, w stosownych przypadkach przy wsparciu Komisji, Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa i ENISA, przy pełnym poszanowaniu odpowiedzialności państw członkowskich w dziedzinie edukacji, propagują środki i strategie mające na celu:

a) rozwijanie umiejętności w zakresie cyberbezpieczeństwa oraz tworzenie narzędzi organizacyjnych i technologicznych w celu zapewnienia wystarczającej dostępności wykwalifikowanych specjalistów do wspierania działań organów nadzoru rynku i jednostek oceniających zgodność;

b) zacieśnienie współpracy między sektorem prywatnym, podmiotami gospodarczymi – w tym poprzez przekwalifikowanie lub podniesienie kwalifikacji pracowników producentów – konsumentami, dostawcami usług szkoleniowych oraz administracjami publicznymi, zwiększając tym samym możliwości dostępu młodych ludzi do miejsc pracy w sektorze cyberbezpieczeństwa.

Artykuł 11

Ogólne bezpieczeństwo produktów

Na zasadzie odstępstwa od art. 2 ust. 1 akapit trzeci lit. b) rozporządzenia (UE) 2023/988 rozdział III sekcja 1, rozdziały V i VII oraz rozdziały IX–XI tego rozporządzenia stosuje się do produktów z elementami cyfrowymi w odniesieniu do aspektów i zagrożeń lub kategorii zagrożeń nieobjętych niniejszym rozporządzeniem, jeżeli produkty te nie podlegają szczegółowym wymaganiom bezpieczeństwa określonym w innym „unijnym prawodawstwie harmonizacyjnym" zdefiniowanym w art. 3 pkt 27 rozporządzenia (UE) 2023/988.

Artykuł 12

Systemy sztucznej inteligencji wysokiego ryzyka

1. Bez uszczerbku dla wymagań dotyczących dokładności i solidności określonych w art. 15 rozporządzenia (UE) 2024/1689 produkty z elementami cyfrowymi, które wchodzą w zakres niniejszego rozporządzenia i są sklasyfikowane jako systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. 6 tego rozporządzenia, uznaje się za spełniające wymagania w zakresie cyberbezpieczeństwa określone w art. 15 tego rozporządzenia, jeżeli:

a) produkty te spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I część I;

b) procedury wprowadzone przez producenta są zgodne z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część II; oraz

c) osiągnięcie poziomu ochrony cyberbezpieczeństwa wymaganego na mocy art. 15 rozporządzenia (UE) 2024/1689 [zostało wykazane w deklaracji zgodności UE wydanej na mocy niniejszego rozporządzenia.

2. W przypadku produktów z elementami cyfrowymi i wymaganiami w zakresie cyberbezpieczeństwa, o których mowa w ust. 1 niniejszego artykułu, stosuje się odpowiednią procedurę oceny zgodności przewidzianą w art. 43 rozporządzenia (UE) 2024/1689. Do celów tej oceny jednostki notyfikowane, które są właściwe do kontroli zgodności systemów sztucznej inteligencji wysokiego ryzyka zgodnie z rozporządzeniem (UE) 2024/1689, są również właściwe do kontroli zgodności systemów sztucznej inteligencji wysokiego ryzyka objętych zakresem niniejszego rozporządzenia z wymaganiami określonymi w załączniku I do niniejszego rozporządzenia, pod warunkiem że zgodność tych jednostek notyfikowanych z wymaganiami określonymi w art. 39 niniejszego rozporządzenia oceniono w kontekście procedury notyfikacyjnej zgodnie z rozporządzeniem (UE) 2024/1689.

3. Na zasadzie odstępstwa od ust. 2 niniejszego artykułu ważne produkty z elementami cyfrowymi wymienione w załączniku III do niniejszego rozporządzenia, które podlegają procedurom oceny zgodności, o których mowa w art. 32 ust. 2 lit. a) i b) oraz art. 32 ust. 3 niniejszego rozporządzenia, oraz produkty krytyczne z elementami cyfrowymi wymienione w załączniku IV do niniejszego rozporządzenia, które muszą uzyskać europejski certyfikat cyberbezpieczeństwa zgodnie z art. 8 ust. 1 niniejszego rozporządzenia lub które w przypadku jego braku podlegają procedurom oceny zgodności, o których mowa w art. 32 ust. 3 niniejszego rozporządzenia, i które są również sklasyfikowane jako systemy sztucznej inteligencji wysokiego ryzyka na mocy art. 6 rozporządzenia (UE) 2024/1689 i do których stosuje się procedurę oceny zgodności opierającą się na kontroli wewnętrznej, o której mowa w załączniku VI do rozporządzenia (UE) 2024/1689, podlegają procedurom oceny zgodności ustanowionym w niniejszym rozporządzeniu w zakresie, w jakim dotyczy to zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w niniejszym rozporządzeniu.

4. Producenci produktów z elementami cyfrowymi, o których mowa w ust. 1 niniejszego artykułu, mogą uczestniczyć w piaskownicach regulacyjnych w zakresie sztucznej inteligencji, o których mowa w art. 57 rozporządzenia (UE) 2024/1689.

ROZDZIAŁ II

OBOWIĄZKI PODMIOTÓW GOSPODARCZYCH I PRZEPISY DOTYCZĄCE WOLNEGO I OTWARTEGO OPROGRAMOWANIA

Artykuł 13

Obowiązki producentów

1. Wprowadzając produkt z elementami cyfrowymi do obrotu, producenci zapewniają, aby został on zaprojektowany, opracowany i wyprodukowany zgodnie z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część I.

2. W celu zapewnienia zgodności z 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 ich skutków, w tym w odniesieniu do zdrowia i bezpieczeństwa użytkowników.

3. Ocena ryzyka w cyberprzestrzeni jest odpowiednio dokumentowana i aktualizowana w okresie wsparcia, który zostanie określony zgodnie z ust. 8 niniejszego artykułu. Ta ocena ryzyka w cyberprzestrzeni obejmuje co najmniej analizę ryzyka w cyberprzestrzeni w oparciu o przeznaczenie i racjonalnie przewidywalne wykorzystanie, a także warunki użytkowania produktu z elementami cyfrowymi, takie jak środowisko operacyjne lub aktywa, które mają być chronione, z uwzględnieniem oczekiwanego czasu użytkowania produktu. W ocenie ryzyka w cyberprzestrzeni wskazuje się, czy i w jaki sposób wymogi bezpieczeństwa określone w załączniku I część I pkt 2 stosują się do danego produktu z elementami cyfrowymi oraz w jaki sposób wymagania te są wdrażane zgodnie z oceną ryzyka w cyberprzestrzeni. Wskazuje się w niej również to, w jaki sposób producent ma stosować załącznik I część I pkt 1, oraz wymagania dotyczące postępowania w przypadku wykrycia podatności określone w załączniku I część II.

4. Wprowadzając produkt z elementami cyfrowymi do obrotu, producent włącza ocenę ryzyka w cyberprzestrzeni, o której mowa w ust. 3 niniejszego artykułu, do dokumentacji technicznej wymaganej na mocy art. 31 i załącznika VII. W przypadku produktów z elementami cyfrowymi, o których mowa w art. 12, podlegających również innym aktom prawnym Unii, ocena ryzyka w cyberprzestrzeni może być częścią oceny ryzyka wymaganej na podstawie tych odpowiednich aktów prawnych Unii. Jeżeli niektóre zasadnicze wymagania w zakresie cyberbezpieczeństwa nie mają zastosowania do produktu z elementami cyfrowymi, producent zamieszcza w tej dokumentacji technicznej wyraźne uzasadnienie.

5. W celu wypełnienia obowiązku określonego w ust. 1 producenci dokładają należytej staranności przy integrowaniu z produktami z elementami cyfrowymi komponentów pochodzących od stron trzecich, aby komponenty takie nie naruszały cyberbezpieczeństwa produktu z elementami cyfrowymi, w tym w przypadku zintegrowania komponentów wolnego i otwartego oprogramowania, które nie zostały udostępnione na rynku w ramach działalności komercyjnej.

6. Producenci, po zidentyfikowaniu podatności w komponencie, w tym w komponencie otwartego oprogramowania, który jest zintegrowany z produktem z elementami cyfrowymi, zgłaszają podatność osobie lub podmiotowi produkującemu lub utrzymującemu komponent oraz usuwają i naprawiają podatność zgodnie z wymogami dotyczącymi postępowania w przypadku wykrycia podatności określonymi w załączniku I część II. W przypadku gdy producenci opracowali modyfikację oprogramowania lub sprzętu komputerowego w celu wyeliminowania podatności w komponencie, udostępniają oni odpowiedni kod lub dokumentację osobie lub podmiotowi produkującemu lub utrzymującemu komponent, w stosownych przypadkach w formacie nadającym się do odczytu maszynowego.

7. Producenci systematycznie dokumentują, w sposób proporcjonalny do charakteru i ryzyka w cyberprzestrzeni, istotne aspekty cyberbezpieczeństwa dotyczące produktu z elementami cyfrowymi, w tym podatności, o których się dowiedzieli, oraz wszelkie istotne informacje przekazane przez strony trzecie, a także, w stosownych przypadkach, aktualizują ocenę ryzyka w cyberprzestrzeni produktów.

8. Przy wprowadzaniu produktu z elementami cyfrowymi do obrotu oraz przez okres wsparcia, producenci zapewniają skuteczne i zgodne z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część II postępowanie w przypadku wykrycia podatności tego produktu lub jego komponentów.

Producenci określają okres wsparcia w taki sposób, aby odzwierciedlał on długość okresu, w którym produkt ma być użytkowany, biorąc pod uwagę w szczególności uzasadnione oczekiwania użytkowników, charakter produktu, w tym jego przeznaczenie, a także odpowiednie prawo Unii określające cykl życia produktów z elementami cyfrowymi. Przy określaniu okresu wsparcia producenci mogą również uwzględnić okresy wsparcia produktów z elementami cyfrowymi oferujących podobną funkcjonalność i wprowadzanych do obrotu przez innych producentów, dostępność środowiska operacyjnego, okresy wsparcia zintegrowanych komponentów, które zapewniają podstawowe funkcje i są pozyskiwane od stron trzecich, a także odpowiednie wytyczne przedstawione przez specjalną grupę współpracy administracyjnej (grupę ADCO) ustanowioną na mocy art. 52 ust. 15 i Komisję. Kwestie, które należy uwzględnić w celu określenia długości okresu wsparcia, rozpatruje się w sposób zapewniający proporcjonalność.

Bez uszczerbku dla akapitu drugiego okres wsparcia wynosi co najmniej pięć lat. Jeżeli oczekuje się, że produkt z elementami cyfrowymi będzie użytkowany krócej niż pięć lat, okres wsparcia odpowiada przewidywanemu czasowi użytkowania.

Uwzględniając zalecenia grupy ADCO, o których mowa w art. 52 ust. 16, Komisja może przyjmować akty delegowane zgodnie z art. 61 w celu uzupełnienia niniejszego rozporządzenia poprzez wyznaczenie minimalnego okresu wsparcia dla określonych kategorii produktów, w przypadku gdy dane z nadzoru rynku sugerują nieodpowiednie okresy wsparcia.

Producenci przedstawiają informacje, które uwzględniono przy określaniu okresu wsparcia produktu z elementami cyfrowymi, w dokumentacji technicznej określonej w załączniku VII.

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

9. Producenci zapewniają, by każda aktualizacja zabezpieczeń, o której mowa w załączniku I część II pkt 8 i która została udostępniona użytkownikom w okresie wsparcia, była nadal dostępna po jej wydaniu przez okres co najmniej 10 lat lub przez pozostałą część okresu wsparcia, w zależności od tego, który z tych okresów jest dłuższy.

10. W przypadku gdy producent wprowadził do obrotu kolejne istotnie zmodyfikowane wersje oprogramowania, może zapewnić zgodność z zasadniczym wymaganiem w zakresie cyberbezpieczeństwa określonym w załączniku I część II pkt 2 wyłącznie w odniesieniu do wersji ostatnio wprowadzonej przez siebie do obrotu, pod warunkiem że użytkownicy wersji uprzednio wprowadzonych do obrotu mają bezpłatny dostęp do wersji ostatnio wprowadzonej do obrotu i nie ponoszą dodatkowych kosztów związanych z dostosowaniem sprzętu i oprogramowania, dzięki którym korzystają z pierwotnej wersji tego produktu.

11. Producenci mogą prowadzić publiczne archiwa oprogramowania usprawniające dostęp użytkowników do wersji historycznych. W takich przypadkach użytkownicy są wyraźnie i w łatwo dostępny sposób informowani o ryzyku związanym ze stosowaniem niewspieranego oprogramowania.

12. Przed wprowadzeniem produktu z elementami cyfrowymi do obrotu producenci sporządzają dokumentację techniczną, o której mowa w art. 31.

Producenci przeprowadzają wybrane procedury oceny zgodności, o których mowa w art. 32, lub zlecają ich przeprowadzenie.

W przypadku wykazania zgodności produktu z elementami cyfrowymi z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część I oraz zgodności procedur wprowadzonych przez producenta z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część II w wyniku przeprowadzenia takiej procedury oceny zgodności producenci sporządzają deklarację zgodności UE zgodnie z art. 28 i umieszczają oznakowanie zgodności CE zgodnie z art. 30.

13. Producenci przechowują dokumentację techniczną i deklarację zgodności UE do dyspozycji organów nadzoru rynku przez okres co najmniej 10 lat po wprowadzeniu produktu z elementami cyfrowymi do obrotu lub przez okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy.

14. Producenci zapewniają wprowadzenie procedur mających na celu utrzymanie zgodności z niniejszym rozporządzeniem produktów z elementami cyfrowymi, które są częścią serii produkcyjnej. Producenci odpowiednio uwzględniają 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. 27, w odniesieniu do których deklaruje się zgodność produktu z elementami cyfrowymi lub przez stosowanie których weryfikuje się jego zgodność.

15. Producenci zapewniają, by ich produkty z elementami cyfrowymi były opatrzone numerem typu, partii lub numerem seryjnym bądź innym elementem umożliwiającym ich identyfikację, a w przypadku gdy nie jest to możliwe, by informacje te były umieszczone na ich opakowaniu lub w dokumencie dołączonym do produktu z elementami cyfrowymi.

16. Na produkcie z elementami cyfrowymi, na jego opakowaniu lub w dokumencie dołączonym do produktu z elementami cyfrowymi producenci podają nazwę, zarejestrowaną nazwę handlową lub zarejestrowany znak towarowy producenta oraz adres pocztowy, adres e-mail lub inne cyfrowe dane kontaktowe, a także, w stosownych przypadkach, stronę internetową, dzięki którym można skontaktować się z producentem. Informacje te należy również zawrzeć w informacjach i instrukcjach dla użytkowników określonych w załączniku II. Dane kontaktowe podaje się w języku łatwo zrozumiałym dla użytkowników i organów nadzoru rynku.

17. Do celów niniejszego rozporządzenia producenci wyznaczają pojedynczy punkt kontaktowy, aby umożliwić użytkownikom bezpośrednią i szybką komunikację z nimi, w tym w celu ułatwienia zgłaszania podatności produktu z elementami cyfrowymi.

Producenci zapewniają, aby pojedynczy punkt kontaktowy był łatwo rozpoznawalny dla użytkowników. Umieszczają oni również pojedynczy punkt kontaktowy w informacjach i instrukcjach dla użytkowników określonych w załączniku II.

Pojedynczy punkt kontaktowy umożliwia użytkownikom wybór preferowanych środków komunikacji i nie ogranicza tych środków do narzędzi zautomatyzowanych.

18. Producenci zapewniają, aby do produktów z elementami cyfrowymi dołączano informacje i instrukcje dla użytkowników określone w załączniku II, w postaci elektronicznej lub papierowej. Takie informacje i instrukcje podaje się w języku łatwo zrozumiałym dla użytkowników i organów nadzoru rynku. Muszą być one jasne, zrozumiałe, przystępne i czytelne. Umożliwiają one bezpieczną instalację, obsługę i bezpieczne użytkowanie produktów z elementami cyfrowymi. Producenci przechowują informacje i instrukcje dla użytkowników określone w załączniku II do dyspozycji użytkowników i organów nadzoru rynku przez okres co najmniej 10 lat po wprowadzeniu produktu z elementami cyfrowymi do obrotu lub przez okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy. W przypadku gdy takie informacje i instrukcje są udostępniane online, producenci zapewniają, by były one dostępne, przyjazne dla użytkownika i udostępniane w internecie przez okres co najmniej 10 lat od wprowadzenia produktu z elementami cyfrowymi do obrotu lub przez okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy.

19. Producenci zapewniają, by w momencie zakupu data zakończenia okresu wsparcia, o którym mowa w ust. 8, obejmująca co najmniej miesiąc i rok, była jasno i zrozumiale określona w łatwo dostępny sposób oraz, w stosownych przypadkach, na produkcie z elementami cyfrowymi, na jego opakowaniu lub za pomocą środków cyfrowych.

Jeżeli jest to technicznie wykonalne ze względu na charakter produktu z elementami cyfrowymi, producenci wyświetlają użytkownikom powiadomienie informujące ich, że zakończył się okres wsparcia ich produktu z elementami cyfrowymi.

20. Producenci dołączają do produktu z elementami cyfrowymi albo deklarację zgodności UE, albo uproszczoną deklarację zgodności UE. Jeżeli dostarcza się uproszczoną deklarację zgodności UE, musi ona zawierać dokładny adres strony internetowej, na której jest dostępna pełna deklaracja zgodności UE.

21. Od chwili wprowadzenia do obrotu i przez okres wsparcia producenci, którzy wiedzą lub mają powody, by sądzić, że produkt z elementami cyfrowymi lub procedury wprowadzone przez producenta nie są zgodne z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I, niezwłocznie wprowadzają środki naprawcze niezbędne do zapewnienia zgodności tego produktu z elementami cyfrowymi lub procedur producenta lub do wycofania produktu z obrotu lub odzyskania go, w stosownych przypadkach.

22. Na uzasadniony wniosek organu nadzoru rynku producenci przekazują temu organowi, w łatwo zrozumiałym dla tego organu 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 wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I. Na żądanie tego organu producenci 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.

23. Producent, który zaprzestaje działalności i w rezultacie nie jest w stanie zapewnić zgodności z niniejszym rozporządzeniem, informuje o nieuchronnym zaprzestaniu działalności przed zaprzestaniem tej działalności odpowiednie organy nadzoru rynku, a także, za pomocą wszelkich dostępnych środków i w możliwie jak najszerszym zakresie, użytkowników odpowiednich produktów z elementami cyfrowymi wprowadzonych do obrotu.

24. Komisja może – w drodze aktów wykonawczych uwzględniających europejskie lub międzynarodowe normy i najlepsze praktyki – określić format i elementy zestawienia podstawowych materiałów do produkcji oprogramowania, o którym mowa w załączniku I część II pkt 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

25. Aby ocenić zależność państw członkowskich i całej Unii od komponentów oprogramowania, a w szczególności od komponentów kwalifikujących się jako wolne i otwarte oprogramowanie, grupa ADCO może podjąć decyzję o przeprowadzeniu ogólnounijnej oceny zależności w odniesieniu do określonych kategorii produktów z elementami cyfrowymi. W tym celu organy nadzoru rynku mogą zwrócić się do producentów takich kategorii produktów z elementami cyfrowymi o udostępnienie odpowiednich zestawień podstawowych materiałów do produkcji oprogramowania, o których mowa w załączniku I część II pkt 1. Na podstawie takich informacji organy nadzoru rynku mogą przekazywać grupie ADCO zanonimizowane i zagregowane informacje na temat zależności od oprogramowania. Grupa ADCO przedkłada Grupie Współpracy, ustanowionej na mocy art. 14 dyrektywy (UE) 2022/2555, sprawozdanie z wyników tej oceny zależności.

Artykuł 14

Obowiązki producentów w zakresie zgłaszania

1. Producent jednocześnie zgłasza jakiekolwiek aktywnie wykorzystywane podatności zawarte w produkcie z elementami cyfrowymi, o których się dowiedział, CSIRT-owi wyznaczonemu na koordynatora zgodnie z ust. 7 niniejszego artykułu oraz ENISA. Producent zgłasza aktywnie wykorzystywaną podatność za pośrednictwem pojedynczej platformy sprawozdawczej ustanowionej na podstawie art. 16.

2. Do celów zgłoszenia, o którym mowa w ust. 1, producent przedkłada:

a) wczesne ostrzeżenie o aktywnie wykorzystywanej podatności, bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od momentu, w którym producent się o niej dowiedział, ze wskazaniem, w stosownych przypadkach, państw członkowskich, o których producent wie, że na ich terytorium został udostępniony jego produkt z elementami cyfrowymi;

b) o ile odpowiednie informacje nie zostały już przekazane, zgłoszenie podatności, bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od momentu, w którym producent dowiedział się o aktywnie wykorzystywanej podatności, z podaniem ogólnych informacji dostępnych na temat danego produktu z elementami cyfrowymi, ogólnego charakteru wykorzystania i danej podatności, a także wszelkich podjętych środków naprawczych lub łagodzących, a także środków naprawczych lub łagodzących, które mogą podjąć użytkownicy, a także ze wskazaniem, w stosownych przypadkach, w jakim stopniu producent uznaje zgłoszone informacje za szczególnie chronione;

c) o ile odpowiednie informacje nie zostały już przekazane, sprawozdanie końcowe, nie później niż 14 dni po udostępnieniu środka naprawczego lub łagodzącego, zawierające co najmniej następujące informacje:

   (i) opis podatności, w tym jej dotkliwości i skutków;

   (ii) jeżeli są dostępne, informacje dotyczące każdego podmiotu działającego w złym zamiarze, który wykorzystał lub wykorzystuje podatność;

   (iii) szczegółowe informacje dotyczące aktualizacji zabezpieczeń lub innych środków naprawczych, które zostały udostępnione w celu eliminacji podatności.

3. Producent jednocześnie zgłasza każdy poważny incydent mający wpływ na bezpieczeństwo produktu z elementami cyfrowymi, o którym się dowie, CSIRT-owi wyznaczonemu na koordynatora zgodnie z ust. 7 niniejszego artykułu oraz ENISA. Producent zgłasza taki incydent za pośrednictwem pojedynczej platformy sprawozdawczej ustanowionej na podstawie art. 16.

4. Do celów zgłoszenia, o którym mowa w ust. 3, producent przedkłada:

a) wczesne ostrzeżenie o poważnym incydencie mającym wpływ na bezpieczeństwo produktu z elementami cyfrowymi, bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od momentu, w którym producent się o nim dowiedział, obejmujące co najmniej informacje, czy istnieją podejrzenia, że poważny incydent został spowodowany działaniem bezprawnym lub działaniem dokonanym w złym zamiarze, ze wskazaniem również, w stosownych przypadkach, państw członkowskich, o których producent wie, że na ich terytorium udostępniono jego produkt z elementami cyfrowymi;

b) o ile odpowiednie informacje nie zostały już przekazane, zgłoszenie incydentu, bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od momentu, w którym producent dowiedział się o incydencie, w którym to zgłoszeniu podaje się ogólne informacje, jeżeli są dostępne, na temat rodzaju incydentu, a także wszelkie podjęte środki naprawcze lub łagodzące, a także środki naprawcze lub łagodzące, które mogą podjąć użytkownicy, a także wskazuje, w stosownych przypadkach, w jakim stopniu producent uznaje zgłoszone informacje za szczególnie chronione;

c) o ile odpowiednie informacje nie zostały już przekazane, sprawozdanie końcowe – w terminie jednego miesiąca od zgłoszenia incydentu zgodnie z lit. b), zawierające co najmniej następujące elementy:

(i) szczegółowy opis incydentu, w tym jego dotkliwości i skutków;

(ii) rodzaj zagrożenia lub pierwotną przyczynę, która prawdopodobnie była źródłem incydentu;

(iii) zastosowane i bieżące środki ograniczające ryzyko.

5. Do celów ust. 3 incydent mający wpływ na bezpieczeństwo produktu z elementami cyfrowymi uznaje się za poważny, jeżeli:

a) negatywnie wpływa on lub może mieć negatywny wpływ na zdolność produktu z elementami cyfrowymi do ochrony dostępności, autentyczności, integralności lub poufności wrażliwych lub ważnych danych lub funkcji; lub

b) prowadził on lub może prowadzić do wprowadzenia lub uruchomienia kodu złośliwego w produkcie z elementami cyfrowymi lub w sieci i systemach informatycznych użytkownika produktu z elementami cyfrowymi.

6. W razie potrzeby CSIRT wyznaczony na koordynatora, który jako pierwszy otrzymał zgłoszenie, może zwrócić się do producentów o przedstawienie sprawozdania okresowego na temat odpowiednich aktualizacji statusu aktywnie wykorzystywanej podatności lub poważnego incydentu mających wpływ na bezpieczeństwo produktu z elementami cyfrowymi.

7. Zgłoszenia, o których mowa w ust. 1 i 3 niniejszego artykułu, przekazuje się za pośrednictwem pojedynczej platformy sprawozdawczej, o której mowa w art. 16, z wykorzystaniem jednego z punktów zgłoszeń elektronicznych, o których mowa w art. 16 ust. 1. Zgłoszenie składa się z wykorzystaniem punktu zgłoszeń elektronicznych CSIRT wyznaczonego na koordynatora tego państwa członkowskiego, w którym producenci mają główną siedzibę w Unii, i jest ono jednocześnie dostępne dla ENISA.

Do celów niniejszego rozporządzenia uznaje się, że producent ma główną siedzibę w Unii w tym państwie członkowskim, w którym głównie podejmowane są decyzje związane z cyberbezpieczeństwem jego produktów z elementami cyfrowymi. Jeżeli nie można ustalić takiego państwa członkowskiego, uznaje się, że główna siedziba znajduje się w państwie członkowskim, w którym dany producent ma siedzibę o największej liczbie pracowników w Unii.

W przypadku gdy producent nie ma głównej siedziby w Unii, dokonuje on zgłoszeń, o których mowa w ust. 1 i 3, z wykorzystaniem punktu zgłoszeń elektronicznych CSIRT wyznaczonego na koordynatora w państwie członkowskim określonym zgodnie z następującą kolejnością i na podstawie informacji dostępnych producentowi:

a) państwo członkowskie, w którym ma siedzibę upoważniony przedstawiciel działający w imieniu producenta w odniesieniu do największej liczby produktów z elementami cyfrowymi tego producenta;

b) państwo członkowskie, w którym ma siedzibę importer wprowadzający do obrotu największą liczbę produktów z elementami cyfrowymi tego producenta;

c) państwo członkowskie, w którym ma siedzibę dystrybutor udostępniający na rynku największą liczbę produktów z elementami cyfrowymi tego producenta;

d) państwo członkowskie, w którym znajduje się największa liczba użytkowników produktów z elementami cyfrowymi tego producenta.

W odniesieniu do akapitu trzeciego lit. d) producent może przekazywać zgłoszenia dotyczące wszelkich późniejszych aktywnie wykorzystywanych podatności lub poważnego incydentu mających wpływ na bezpieczeństwo produktu z elementami cyfrowymi temu samemu CSIRT-owi wyznaczonemu na koordynatora, któremu uprzednio przekazał zgłoszenie.

8. Po otrzymaniu informacji o wystąpieniu aktywnie wykorzystywanej podatności lub poważnego incydentu mającego wpływ na bezpieczeństwo produktu z elementami cyfrowymi producent informuje użytkowników produktu z elementami cyfrowymi, na których incydent ma wpływ, oraz, w stosownych przypadkach, wszystkich użytkowników o tej podatności lub tym incydencie oraz, w razie potrzeby, o środkach łagodzących oraz wszelkich środkach naprawczych, które użytkownicy mogą wdrożyć w celu złagodzenia skutków tej podatności lub incydentu, w stosownych przypadkach w ustrukturyzowanym i łatwo przetwarzalnym automatycznie formacie nadającym się do odczytu maszynowego. Jeżeli producent nie poinformuje użytkowników produktu z elementami cyfrowymi w odpowiednim czasie, CSIRT-y wyznaczone na koordynatorów, do których dotarło zgłoszenie, mogą przekazać takie informacje użytkownikom, jeżeli zostanie to uznane za proporcjonalne i konieczne do zapobieżenia skutkom tej podatności lub incydentu lub łagodzenia ich skutków.

9. Do dnia 11 grudnia 2025 r. Komisja przyjmuje akty delegowane zgodnie z art. 61 niniejszego rozporządzenia w celu uzupełnienia niniejszego rozporządzenia poprzez określenie warunków zastosowania względów cyberbezpieczeństwa w odniesieniu do opóźniania rozpowszechniania zgłoszeń, o których mowa w art. 16 ust. 2 niniejszego rozporządzenia. Przy przygotowywaniu projektu tych aktów delegowanych Komisja współpracuje z siecią CSIRT, ustanowioną na podstawie art. 15 dyrektywy (UE) 2022/2555, oraz z ENISA.

10. Komisja może, w drodze aktów wykonawczych, doprecyzować format i procedurę składania zgłoszeń, o których mowa w niniejszym artykule oraz w art. 15 i 16. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2. Komisja współpracuje z siecią CSIRT oraz z ENISA przy przygotowywaniu tych projektów aktów wykonawczych.

Artykuł 15

Dobrowolne zgłaszanie

1. Producenci oraz inne osoby fizyczne lub prawne mogą dobrowolnie zgłaszać CSIRT-owi wyznaczonemu na koordynatora lub ENISA wszelkie podatności zawarte w produkcie z elementami cyfrowymi, a także cyberzagrożenia, które mogłyby mieć wpływ na profil ryzyka produktu z elementami cyfrowymi.

2. Producenci oraz inne osoby fizyczne lub prawne mogą dobrowolnie zgłaszać CSIRT-owi wyznaczonemu na koordynatora lub ENISA każdy incydent mający wpływ na bezpieczeństwo produktu z elementami cyfrowymi, a także potencjalne zdarzenia dla cyberbezpieczeństwa, które mogły doprowadzić do takiego incydentu.

3. CSIRT wyznaczony na koordynatora lub ENISA rozpatrują zgłoszenia, o których mowa w ust. 1 i 2 niniejszego artykułu, zgodnie z procedurą określoną w art. 16.

CSIRT wyznaczony na koordynatora może rozpatrywać zgłoszenia obowiązkowe priorytetowo w stosunku do zgłoszeń dobrowolnych.

4. W przypadku gdy osoba fizyczna lub prawna inna niż producent zgłasza aktywnie wykorzystywaną podatność lub poważny incydent mający wpływ na bezpieczeństwo produktu z elementami cyfrowymi zgodnie z ust. 1 lub 2, CSIRT wyznaczony na koordynatora bez zbędnej zwłoki informuje o tym producenta.

5. CSIRT-y wyznaczone na koordynatorów oraz ENISA zapewniają poufność i odpowiednią ochronę informacji przekazanych przez osobę fizyczną lub prawną dokonującą zgłoszenia. Bez uszczerbku dla zapobiegania przestępstwom, prowadzenia postępowań w ich sprawie, ich wykrywania i ścigania dobrowolne zgłaszanie nie może powodować nałożenia na osobę fizyczną lub prawną dokonującą zgłoszenia żadnych dodatkowych obowiązków, którym by nie podlegała, gdyby nie przekazała zgłoszenia.

Artykuł 16

Ustanowienie pojedynczej platformy sprawozdawczej

1. Do celów zgłoszeń, o których mowa w art. 14 ust. 1 i 3 oraz art. 15 ust. 1 i 2, oraz w celu uproszczenia obowiązków sprawozdawczych producentów ENISA ustanawia pojedynczą platformę sprawozdawczą. ENISA zarządza bieżącą działalnością tej pojedynczej platformy sprawozdawczej i utrzymuje ją. Architektura pojedynczej platformy sprawozdawczej umożliwia państwom członkowskim i ENISA wprowadzenie własnych punktów zgłoszeń elektronicznych.

2. Po otrzymaniu zgłoszenia CSIRT wyznaczony na koordynatora, który jako pierwszy otrzymał zgłoszenie, niezwłocznie przekazuje je za pośrednictwem pojedynczej platformy sprawozdawczej do CSIRT-ów wyznaczonych na koordynatorów na terytorium, na którym producent wskazał, że produkt z elementami cyfrowymi został udostępniony.

W wyjątkowych okolicznościach, w szczególności na wniosek producenta i w świetle poziomu wrażliwości zgłoszonych informacji wskazanego przez producenta zgodnie z art. 14 ust. 2 lit. a) niniejszego rozporządzenia, rozpowszechnienie zgłoszenia może zostać opóźnione z uzasadnionych przyczyn związanych z cyberbezpieczeństwem o absolutnie niezbędny okres, w tym w przypadku gdy podatność podlega skoordynowanej procedurze ujawniania, o której mowa w art. 12 ust. 1 dyrektywy (UE) 2022/2555. W przypadku gdy CSIRT podejmie decyzję o nieujawnianiu zgłoszenia, niezwłocznie informuje ENISA o tej decyzji i przedstawia zarówno uzasadnienie nieujawnienia zgłoszenia, jak i wskazanie, kiedy rozpowszechni zgłoszenie zgodnie z procedurą rozpowszechniania określoną w niniejszym ustępie. ENISA może poprzeć stanowisko CSIRT-u dotyczące zastosowania względów cyberbezpieczeństwa w odniesieniu do opóźnienia rozpowszechnienia zgłoszenia.

W szczególnie wyjątkowych okolicznościach, jeżeli producent wskazuje w zgłoszeniu, o którym mowa w art. 14 ust. 2 lit. b):

a) że zgłoszona podatność została aktywnie wykorzystana przez podmiot działający w złym zamiarze i, zgodnie z dostępnymi informacjami, nie została wykorzystana w żadnym innym państwie członkowskim niż to, którego CSIRT wyznaczono na koordynatora i któremu producent zgłosił podatność;

b) że jakiekolwiek natychmiastowe dalsze rozpowszechnienie zgłoszonej podatności prawdopodobnie doprowadziłoby do dostarczenia informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami tego państwa członkowskiego; lub

c) że dalsze rozpowszechnianie zgłoszenia podatności stwarza bezpośrednie wysokie ryzyko w cyberprzestrzeni;

jedynie informacje o tym, że producent dokonał zgłoszenia, ogólne informacje na temat produktu, informacje o ogólnym charakterze wykorzystania oraz informacje o tym, że powołano się na względy bezpieczeństwa, są jednocześnie udostępniane ENISA, aż do momentu rozpowszechnienia pełnego zgłoszenia wśród zainteresowanych CSIRT-ów i ENISA. Jeżeli na podstawie tych informacji ENISA uzna, że istnieje ryzyko systemowe mające wpływ na bezpieczeństwo na rynku wewnętrznym, zaleca CSIRT-owi, który otrzymał zgłoszenie, aby przekazał pełne zgłoszenie pozostałym CSIRT-om wyznaczonym na koordynatorów oraz samej ENISA.

3. Po otrzymaniu zgłoszenia o aktywnie wykorzystywanej podatności w produkcie z elementami cyfrowymi lub o poważnym incydencie mającym wpływ na bezpieczeństwo produktu z elementami cyfrowymi CSIRT-y wyznaczone na koordynatorów przekazują organom nadzoru rynku swoich państw członkowskich zgłoszone informacje niezbędne organom nadzoru rynku do wypełniania ich obowiązków wynikających z niniejszego rozporządzenia.

4. ENISA przyjmuje odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa pojedynczej platformy sprawozdawczej oraz informacji przekazywanych lub rozpowszechnianych za pośrednictwem pojedynczej platformy sprawozdawczej. ENISA bez zbędnej zwłoki powiadamia sieć CSIRT oraz Komisję o każdym incydencie bezpieczeństwa mającym wpływ na pojedynczą platformę sprawozdawczą.

5. ENISA, we współpracy z siecią CSIRT, zapewnia i wdraża specyfikacje dotyczące środków technicznych, operacyjnych i organizacyjnych dotyczących ustanowienia, utrzymania i bezpiecznego funkcjonowania pojedynczej platformy sprawozdawczej, o której mowa w ust. 1, w tym co najmniej ustalenia dotyczące bezpieczeństwa związane z ustanowieniem, funkcjonowaniem i utrzymaniem pojedynczej platformy sprawozdawczej, a także punktów zgłoszeń elektronicznych ustanowionych przez CSIRT-y wyznaczone na koordynatorów na poziomie krajowym i ENISA na poziomie Unii, w tym aspektów proceduralnych mających zapewnić, że w przypadku gdy dla zgłoszonej podatności nie ma dostępnych środków naprawczych lub łagodzących, informacje o tej podatności będą udostępniane zgodnie ze ścisłymi protokołami bezpieczeństwa i na zasadzie ograniczonego dostępu.

6. W przypadku gdy CSIRT wyznaczony na koordynatora został powiadomiony o aktywnie wykorzystywanej podatności w ramach procedury skoordynowanego ujawniania podatności, o której mowa w art. 12 ust. 1 dyrektywy (UE) 2022/2555, CSIRT wyznaczony na koordynatora, który jako pierwszy otrzymał zgłoszenie, może opóźnić rozpowszechnienie stosownego zgłoszenia za pośrednictwem pojedynczej platformy sprawozdawczej z uzasadnionych względów cyberbezpieczeństwa o okres nie dłuższy niż jest to absolutnie niezbędne i do czasu wyrażenia zgody na ujawnienie przez strony zaangażowane w skoordynowane ujawnienie podatności. Wymóg ten nie uniemożliwia producentom dobrowolnego zgłaszania takiej podatności zgodnie z procedurą określoną w niniejszym artykule.

Artykuł 17

Inne przepisy dotyczące sprawozdawczości

1. ENISA może przekazać europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) ustanowionej na mocy art. 16 dyrektywy (UE) 2022/2555 informacje zgłoszone zgodnie z art. 14 ust. 1 i 3 oraz art. 15 ust. 1 i 2 niniejszego rozporządzenia, jeżeli takie informacje są istotne z perspektywy skoordynowanego zarządzania cyberincydentami i cyberkryzysami na dużą skalę na szczeblu operacyjnym. Do celów określenia takiej istotności ENISA może uwzględnić analizy techniczne przeprowadzone przez sieć CSIRT, jeżeli są one dostępne.

2. W przypadku gdy świadomość społeczna jest niezbędna, aby zapobiec poważnemu incydentowi mającemu wpływ na bezpieczeństwo produktu z elementami cyfrowymi lub złagodzić jego skutki, lub aby poradzić sobie z trwającym incydentem, lub w przypadku gdy ujawnienie incydentu leży w interesie publicznym, CSIRT wyznaczony na koordynatora odpowiedniego państwa członkowskiego może, po konsultacji z zainteresowanym producentem i, w stosownych przypadkach, we współpracy z ENISA, poinformować opinię publiczną o incydencie lub zażądać tego od producenta.

3. ENISA, na podstawie zgłoszeń otrzymywanych zgodnie z art. 14 ust. 1 i 3 oraz art. 15 ust. 1 i 2 niniejszego rozporządzenia, przygotowuje co 24 miesiące sprawozdanie techniczne na temat pojawiających się tendencji w zakresie ryzyka w cyberprzestrzeni dotyczącego produktów z elementami cyfrowymi oraz przedkłada je Grupie Współpracy ustanowionej na podstawie art. 14 dyrektywy (UE) 2022/2555. Pierwsze takie sprawozdanie przedkłada się w terminie 24 miesięcy od dnia rozpoczęcia stosowania obowiązków określonych w art. 14 ust. 1 i 3. W sprawozdaniu o stanie cyberbezpieczeństwa w Unii sporządzanym na podstawie art. 18 dyrektywy (UE) 2022/2555 ENISA uwzględnia odpowiednie informacje ze swoich sprawozdań technicznych.

4. Samo zgłoszenie zgodnie z art. 14 ust. 1 i 3 lub art. 15 ust. 1 i 2 nie powoduje zwiększenia odpowiedzialności osoby fizycznej lub prawnej dokonującej zgłoszenia.

5. Po udostępnieniu aktualizacji zabezpieczeń lub innej formy środka naprawczego lub łagodzącego ENISA, w porozumieniu z producentem danego produktu z elementami cyfrowymi, dodaje publicznie znaną podatność, zgłoszoną zgodnie z art. 14 ust. 1 lub art. 15 ust. 1 niniejszego rozporządzenia, do europejskiej bazy danych dotyczących podatności ustanowionej zgodnie z art. 12 ust. 2 dyrektywy (UE) 2022/2555.

6. CSIRT-y wyznaczone na koordynatorów zapewniają producentom, a w szczególności producentom, którzy kwalifikują się jako mikroprzedsiębiorstwa lub małe lub średnie przedsiębiorstwa, wsparcie działu pomocy technicznej w odniesieniu do obowiązków sprawozdawczych zgodnie z art. 14.

Artykuł 18

Upoważnieni przedstawiciele

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

2. Obowiązki określone w art. 13 ust. 1–11, art. 13 ust. 12 akapit pierwszy oraz art. 13 ust. 14 nie wchodzą w zakres pełnomocnictwa upoważnionego przedstawiciela.

3. Upoważniony przedstawiciel wykonuje zadania określone w pełnomocnictwie otrzymanym od producenta. Upoważniony przedstawiciel na żądanie organów nadzoru rynku przedstawia im kopię swojego pełnomocnictwa. Pełnomocnictwo umożliwia upoważnionemu przedstawicielowi wykonywanie co najmniej następujących obowiązków:

a) przechowywanie deklaracji zgodności UE, o której mowa w art. 28, oraz dokumentacji technicznej, o której mowa w art. 31, do dyspozycji organów nadzoru rynku przez okres co najmniej 10 lat po wprowadzeniu produktu z elementami cyfrowymi do obrotu lub przez okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy;

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 19

Obowiązki importerów

1. Importerzy wprowadzają do obrotu wyłącznie produkty z elementami cyfrowymi, które spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I część I i w przypadku których procedury wprowadzone przez producenta są zgodne z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część II.

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

a) producent przeprowadził odpowiednie procedury oceny zgodności, o których mowa w art. 32;

b) producent sporządził dokumentację techniczną;

c) produkt z elementami cyfrowymi nosił oznakowanie CE, o którym mowa w art. 30, oraz by towarzyszyła mu deklaracja zgodności UE, o której mowa w art. 13 ust. 20, oraz informacje i instrukcje dla użytkownika określone w załączniku II, w języku łatwo zrozumiałym dla użytkowników i organów nadzoru rynku;

d) producent spełnił wymogi określone w art. 13 ust. 15, 16 i 19.

Do celów niniejszego ustępu importerzy muszą być w stanie przedstawić niezbędne dokumenty potwierdzające spełnienie wymogów określonych w niniejszym artykule.

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 niniejszym rozporządzeniem, nie wprowadza produktu do obrotu, dopóki nie zostanie zapewniona zgodność tego produktu lub tych procedur wprowadzonych przez producenta z niniejszym rozporządzeniem. Ponadto, jeżeli produkt z elementami cyfrowymi stwarza znaczne ryzyko w cyberprzestrzeni, importer informuje o tym producenta oraz organy nadzoru rynku.

W przypadku gdy importer ma powody sądzić, że produkt z elementami cyfrowymi może stwarzać istotne ryzyko w cyberprzestrzeni w kontekście pozatechnicznych czynników ryzyka, importer informuje o tym organy nadzoru rynku. Po otrzymaniu takich informacji organy nadzoru rynku postępują zgodnie z procedurami, o których mowa w art. 54 ust. 2.

4. Importerzy umieszczają na produkcie z elementami cyfrowymi lub 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, adres e-mail lub inną cyfrową formę kontaktu, a także, w stosownych przypadkach, stronę internetową, za pośrednictwem których można się z nimi skontaktować. Dane kontaktowe podaje się w języku łatwo zrozumiałym dla użytkowników i organów nadzoru rynku.

5. Importerzy, którzy wiedzą lub mają powody sądzić, że wprowadzony przez nich na rynek produkt z elementami cyfrowymi nie jest zgodny z niniejszym rozporządzeniem, niezwłocznie wprowadzają środki naprawcze niezbędne do zapewnienia zgodności produktu z elementami cyfrowymi z niniejszym rozporządzeniem lub do wycofania produktu z obrotu, lub odzyskania go, w stosownych przypadkach.

Po uzyskaniu informacji o 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.

6. Importerzy przechowują kopię deklaracji zgodności UE do dyspozycji organów nadzoru rynku przez co najmniej 10 lat po wprowadzeniu produktu z elementami cyfrowymi do obrotu lub przez okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy, i na wniosek tych organów udostępniają im dokumentację techniczną.

7. 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 wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część I, a także zgodności procedur wprowadzonych przez producenta z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część II, 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.

8. 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 20

Obowiązki dystrybutorów

1. Udostępniając produkt z elementami cyfrowymi na rynku, dystrybutorzy działają z należytą starannością w odniesieniu do wymogów określonych w niniejszym rozporządzeniu.

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 w art. 13 ust. 15, 16, 18, 19 i 20 oraz art. 19 ust. 4 i dostarczyli dystrybutorowi wszystkie niezbędne dokumenty.

3. W przypadku gdy na podstawie posiadanych informacji dystrybutor uznaje lub ma powody sądzić, że produkt z elementami cyfrowymi lub procedury wprowadzone przez producenta nie są zgodne z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa 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 z niniejszym rozporządzeniem. Ponadto, jeżeli produkt z elementami cyfrowymi stwarza istotne ryzyko w cyberprzestrzeni, dystrybutor bez zbędnej zwłoki informuje o tym producenta oraz organy nadzoru rynku.

4. Dystrybutorzy, którzy na podstawie posiadanych informacji wiedzą lub mają powody sądzić, że udostępniony przez nich na rynku produkt z elementami cyfrowymi lub procedury wprowadzone przez producenta nie są zgodne z niniejszym rozporządzeniem, 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 uzyskaniu informacji o 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 niniejszym rozporządzeniem 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 na podstawie posiadanych informacji dowiaduje się, że producent tego produktu zaprzestał działalności i w związku z tym nie jest w stanie wypełnić obowiązków określonych w niniejszym rozporządzeniu, dystrybutor bez zbędnej zwłoki 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 21

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 art. 13 i 14, 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 22

Inne przypadki, w których mają zastosowanie obowiązki producentów

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

2. Osoba, o której mowa w ust. 1 niniejszego artykułu, podlega obowiązkom określonym w art. 13 i 14 w odniesieniu do części produktu z elementami cyfrowymi poddanej istotnej modyfikacji lub – jeżeli taka istotna modyfikacja ma wpływ na cyberbezpieczeństwo produktu z elementami cyfrowymi jako całości – w odniesieniu do całego produktu.

Artykuł 23

Identyfikacja podmiotów gospodarczych

1. Na wniosek organów nadzoru rynku 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) o ile są dostępne – 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 10 lat od dostarczenia im produktu z elementami cyfrowymi oraz przez 10 lat od dostarczenia przez nie produktu z elementami cyfrowymi.

Artykuł 24

Obowiązki opiekunów otwartego oprogramowania

1. Opiekunowie otwartego oprogramowania wprowadzają i dokumentują w weryfikowalny sposób politykę cyberbezpieczeństwa w celu wspierania rozwoju bezpiecznego produktu z elementami cyfrowymi, a także skutecznego radzenia sobie z podatnościami przez twórców tego produktu. Polityka ta wspiera również dobrowolne zgłaszanie podatności zgodnie z art. 15 przez twórców tego produktu i uwzględnia szczególny charakter opiekuna otwartego oprogramowania oraz ustalenia prawne i organizacyjne, którym on podlega. Polityka ta obejmuje w szczególności aspekty związane z dokumentowaniem, rozwiązywaniem i eliminowaniem podatności oraz promowaniem udostępniania informacji dotyczących wykrytych podatności w ramach społeczności zajmujących się otwartym oprogramowaniem.

2. Opiekunowie otwartego oprogramowania współpracują z organami nadzoru rynku, na ich wniosek, w celu ograniczenia ryzyka w cyberprzestrzeni stwarzanego przez produkt z elementami cyfrowymi kwalifikujący się jako wolne i otwarte oprogramowanie.

Na uzasadniony wniosek organu nadzoru rynku opiekunowie otwartego oprogramowania dostarczają temu organowi, w języku łatwo zrozumiałym dla tego organu, dokumentację, o której mowa w ust. 1, w formie papierowej lub elektronicznej.

3. Obowiązki określone w art. 14 ust. 1 stosuje się do opiekunów otwartego oprogramowania w zakresie, w jakim są oni zaangażowani w rozwój produktów z elementami cyfrowymi. Obowiązki określone w art. 14 ust. 3 i 8 stosuje się do opiekunów otwartego oprogramowania w zakresie, w jakim poważne incydenty mające wpływ na bezpieczeństwo produktów z elementami cyfrowymi dotyczą sieci i systemów informatycznych dostarczonych przez opiekunów otwartego oprogramowania w celu rozwoju takich produktów.

Artykuł 25

Poświadczanie bezpieczeństwa wolnego i otwartego oprogramowania

W celu ułatwienia wypełniania obowiązku należytej staranności określonego w art. 13 ust. 5, w szczególności w odniesieniu do producentów, którzy włączają do swoich produktów z elementami cyfrowymi komponenty wolnego i otwartego oprogramowania, Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 61 w celu uzupełnienia niniejszego rozporządzenia poprzez ustanowienie dobrowolnych programów poświadczania bezpieczeństwa umożliwiających twórcom lub użytkownikom produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie, a także innym stronom trzecim ocenę zgodności takich produktów ze wszystkimi lub niektórymi zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa lub innymi obowiązkami określonymi w niniejszym rozporządzeniu.

Artykuł 26

Wytyczne

1. Aby ułatwić wdrożenie i zapewnić jego spójność, Komisja publikuje wytyczne, aby pomóc podmiotom gospodarczym w stosowaniu niniejszego rozporządzenia, ze szczególnym naciskiem na ułatwienie zachowania zgodności mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom.

2. W przypadku gdy Komisja zamierza przedstawić wytyczne, o których mowa w ust. 1, zajmuje się ona co najmniej następującymi aspektami:

a) zakres niniejszego rozporządzenia, ze szczególnym uwzględnieniem rozwiązań w zakresie zdalnego przetwarzania danych oraz wolnego i otwartego oprogramowania;

b) stosowanie okresów wsparcia w odniesieniu do poszczególnych kategorii produktów z elementami cyfrowymi;

c) wytyczne skierowane do producentów podlegających niniejszemu rozporządzeniu, którzy podlegają również unijnemu prawodawstwu harmonizacyjnemu innemu niż niniejsze rozporządzenie lub innym powiązanym aktom prawnym Unii;

d) pojęcie istotnej modyfikacji.

Komisja prowadzi również łatwo dostępny wykaz aktów delegowanych i wykonawczych przyjętych na podstawie niniejszego rozporządzenia.

3. Przy sporządzaniu wytycznych zgodnie z niniejszym artykułem Komisja konsultuje się z odpowiednimi zainteresowanymi stronami.

ROZDZIAŁ III

ZGODNOŚĆ PRODUKTU Z ELEMENTAMI CYFROWYMI

Artykuł 27

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*, domniemywa się, że spełniają one zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I objęte tymi normami lub ich częściami.

Komisja, zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012, zwraca się do jednej lub kilku europejskich organizacji normalizacyjnych z wnioskiem o przygotowanie norm zharmonizowanych dotyczących zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I do niniejszego rozporządzenia. Sporządzając wnioski o normalizację na potrzeby niniejszego rozporządzenia, Komisja stara się uwzględnić istniejące europejskie i międzynarodowe normy w dziedzinie cyberbezpieczeństwa, które są już dostępne lub w trakcie opracowywania, aby uprościć opracowanie norm zharmonizowanych zgodnie z rozporządzeniem (UE) nr 1025/2012.

2. Komisja może przyjmować akty wykonawcze ustanawiające wspólne specyfikacje obejmujące wymogi techniczne, które zapewniają środki umożliwiające spełnienie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I w odniesieniu do produktów z elementami cyfrowymi objętych zakresem stosowania niniejszego rozporządzenia.

Te akty wykonawcze przyjmuje się wyłącznie wtedy, jeżeli spełnione są następujące warunki:

a) zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012 Komisja zwróciła się do co najmniej jednej europejskiej organizacji normalizacyjnej z wnioskiem o przygotowanie zharmonizowanej normy dotyczącej zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I oraz:

   (i) wniosek ten nie został zaakceptowany;

   (ii) normy zharmonizowane stanowiące odpowiedź na ten wniosek nie zostały dostarczone w terminie określonym zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012; lub

   (iii) normy zharmonizowane nie są zgodne z wnioskiem; oraz

b) w *Dzienniku Urzędowym Unii Europejskiej* nie opublikowano żadnego odniesienia do zharmonizowanych norm obejmujących odnośne zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I do niniejszego rozporządzenia zgodnie z rozporządzeniem (UE) nr 1025/2012 i nie przewiduje się opublikowania takiego odniesienia w rozsądnym terminie.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

3. Przed przygotowaniem projektu aktu wykonawczego określonego w ust. 2 niniejszego artykułu Komisja informuje komitet, o którym mowa w art. 22 rozporządzenia (UE) nr 1025/2012, że uznaje warunki określone w ust. 2 niniejszego artykułu za spełnione.

4. Przygotowując projekt aktu wykonawczego, o którym mowa w ust. 2, Komisja uwzględnia opinie odpowiednich organów i należycie konsultuje się ze wszystkimi odpowiednimi zainteresowanymi stronami.

5. Produkty z elementami cyfrowymi i procedury wprowadzone przez producenta, zgodne ze wspólnymi specyfikacjami ustanowionymi aktami wykonawczymi, o których mowa w ust. 2 niniejszego artykułu, lub ich częściami, uznaje się za spełniające zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I objęte tymi wspólnymi specyfikacjami lub ich częściami.

6. W przypadku gdy norma zharmonizowana zostaje przyjęta przez europejską organizację normalizacyjną i zaproponowana Komisji w celu opublikowania odniesienia do niej w *Dzienniku Urzędowym Unii Europejskiej*, Komisja ocenia normę zharmonizowaną zgodnie z rozporządzeniem (UE) nr 1025/2012. W przypadku opublikowania odniesienia do normy zharmonizowanej w *Dzienniku Urzędowym Unii Europejskiej* Komisja uchyla akty wykonawcze, o których mowa w ust. 2 niniejszego artykułu, lub ich części, które obejmują zasadnicze wymagania w zakresie cyberbezpieczeństwa takie same jak objęte tą normą zharmonizowaną.

7. Jeżeli państwo członkowskie uzna, że wspólna specyfikacja nie spełnia całkowicie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I, informuje o tym Komisję, przedstawiając szczegółowe wyjaśnienie. Komisja ocenia to szczegółowe wyjaśnienie i w stosownych przypadkach może zmienić akt wykonawczy ustanawiający daną wspólną specyfikację.

8. Domniemywa 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, są zgodne z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I w zakresie, w jakim unijna deklaracja zgodności lub europejski certyfikat cyberbezpieczeństwa, lub ich części, obejmują te wymogi.

9. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 61 niniejszego rozporządzenia w celu uzupełnienia niniejszego rozporządzenia poprzez określenie europejskich programów certyfikacji cyberbezpieczeństwa przyjętych na podstawie rozporządzenia (UE) 2019/881, które mogą być stosowane do wykazania zgodności produktów z elementami cyfrowymi z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa lub ich częściami określonymi w załączniku I do niniejszego rozporządzenia. Ponadto wydanie europejskiego certyfikatu cyberbezpieczeństwa wydanego w ramach takich programów, przynajmniej na „istotnym" poziomie uzasadnienia zaufania, zwalnia producenta z obowiązku przeprowadzenia oceny zgodności przez stronę trzecią w odniesieniu do odpowiednich wymogów, jak określono w art. 32 ust. 2 lit. a) i b) oraz art. 32 ust. 3 lit. a) i b) niniejszego rozporządzenia.

Artykuł 28

Deklaracja zgodności UE

1. Deklarację zgodności UE sporządzają producenci zgodnie z art. 13 ust. 12 i potwierdza się w niej, że wykazano spełnienie mających zastosowanie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I.

2. Deklarację zgodności UE sporządza się według wzoru określonego w załączniku V i zawiera ona elementy wyszczególnione w odpowiednich procedurach oceny zgodności określonych w załączniku VIII. Taka deklaracja jest w stosownych przypadkach aktualizowana. Deklarację udostępnia się w językach wymaganych przez państwo członkowskie, w którym produkt z elementami cyfrowymi jest wprowadzany do obrotu lub udostępniany na rynku.

Uproszczona deklaracja zgodności UE, o której mowa w art. 13 ust. 20, zawiera wzór określony w załączniku VI. Deklarację udostępnia się w językach wymaganych przez państwo członkowskie, w którym produkt z elementami cyfrowymi jest wprowadzany do obrotu lub udostępniany na rynku.

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

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

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 61 w celu uzupełnienia niniejszego rozporządzenia przez dodanie elementów do minimalnego zakresu treści deklaracji zgodności UE określonego w załączniku V, aby uwzględnić rozwój technologiczny.

Artykuł 29

Ogólne zasady dotyczące oznakowania CE

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

Artykuł 30

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. 28, 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. 28, albo na stronie internetowej poświęconej oprogramowaniu. W drugim z tych przypadków odpowiednia sekcja strony internetowej jest łatwo i bezpośrednio dostępna dla konsumentów.

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 w cyberprzestrzeni 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. 32.

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 unijnemu prawodawstwu harmonizacyjnemu innemu niż niniejsze rozporządzenie, w którym również przewiduje się umieszczenie oznakowania CE, oznakowanie to wskazuje, że produkt spełnia również wymogi określone w takim innym unijnym prawie harmonizacyjnym.

6. Komisja może – w drodze aktów wykonawczych – ustanowić specyfikacje techniczne etykiet, piktogramów lub wszelkich innych oznakowań związanych z bezpieczeństwem produktów z elementami cyfrowymi, okresy wsparcia oraz mechanizmy zachęcające do ich stosowania oraz zwiększające świadomość społeczną na temat bezpieczeństwa produktów z elementami cyfrowymi. Przygotowując projekty aktów wykonawczych, Komisja konsultuje się z odpowiednimi zainteresowanymi stronami oraz z grupą ADCO, jeżeli już ją ustanowiono zgodnie z art. 52 ust. 15. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

Artykuł 31

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 wymagania w zakresie cyberbezpieczeństwa określone w załączniku I. Zawiera ona co najmniej elementy określone w załączniku VII.

2. Dokumentację techniczną sporządza się przed wprowadzeniem do obrotu produktu z elementami cyfrowymi i – w razie potrzeby – jest ona stale aktualizowana, przynajmniej podczas okresu wsparcia.

3. W przypadku produktów z elementami cyfrowymi, o których mowa w art. 12, które podlegają również innym aktom prawnym Unii przewidującym dokumentację techniczną, sporządza się jedną dokumentację techniczną zawierającą informacje, o których mowa w załączniku VII, oraz informacje wymagane w tych aktach prawnych 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. 61 w celu uzupełnienia niniejszego rozporządzenia poprzez dodanie elementów, które należy włączyć do dokumentacji technicznej określonej w załączniku VII, aby uwzględnić rozwój technologiczny, jak również o zmiany napotkane w procesie wdrażania niniejszego rozporządzenia. W tym celu Komisja dąży do zapewnienia współmierności obciążeń administracyjnych nakładanych na mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa.

Artykuł 32

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 wymagania w zakresie cyberbezpieczeństwa określone w załączniku I. Producent wykazuje zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa, stosując dowolną z następujących procedur:

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

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

c) ocenę zgodności opartą na pełnym zapewnieniu jakości (zgodnie z modułem H) określoną w załączniku VIII; lub

d) o ile jest dostępny i ma zastosowanie – europejski program certyfikacji cyberbezpieczeństwa zgodnie z art. 27 ust. 9.

2. Jeżeli przy ocenie zgodności ważnego produktu z elementami cyfrowymi należącego do klasy I, jak określono w załączniku III, oraz procedur wprowadzonych przez jego producenta z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I producent nie zastosował norm zharmonizowanych, wspólnych specyfikacji lub europejskich programów certyfikacji cyberbezpieczeństwa przynajmniej na „istotnym" poziomie uzasadnienia zaufania, o których mowa w art. 27, 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 wymagań w zakresie cyberbezpieczeństwa jednej z następujących procedur:

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

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

3. Jeżeli produkt jest ważnym produktem z elementami cyfrowymi należącym do klasy II, jak określono w załączniku III, producent wykazuje zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I, stosując dowolną z następujących procedur:

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

b) ocenę zgodności opartą na pełnym zapewnieniu jakości (zgodnie z modułem H) określoną w załączniku VIII; lub

c) jeżeli jest dostępny i ma zastosowanie – europejski program certyfikacji cyberbezpieczeństwa zgodnie z art. 27 ust. 9 niniejszego rozporządzenia przynajmniej na „istotnym" poziomie uzasadnienia zaufania zgodnie z rozporządzeniem (UE) 2019/881.

4. Produkty krytyczne z elementami cyfrowymi wymienione w załączniku IV wykazują zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I za pomocą jednej z następujących procedur:

a) europejski program certyfikacji cyberbezpieczeństwa zgodnie z art. 8 ust. 1; lub

b) w przypadku gdy warunki określone w art. 8 ust. 1 nie są spełnione, którejkolwiek z procedur, o których mowa w ust. 3 niniejszego artykułu.

5. Producenci produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie, które należą do kategorii określonych w załączniku III, są zdolni do wykazania zgodności z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I za pomocą jednej z procedur, o których mowa w ust. 1 niniejszego artykułu, pod warunkiem że dokumentacja techniczna, o której mowa w art. 31, jest publicznie dostępna w momencie wprowadzania tych produktów do obrotu.

6. Przy ustalaniu opłat za procedury oceny zgodności uwzględnia się szczególne interesy i potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, w tym przedsiębiorstw typu start-up, i obniża się te opłaty proporcjonalnie do ich szczególnych interesów i potrzeb.

Artykuł 33

Środki wsparcia dla mikroprzedsiębiorstw małych i średnich przedsiębiorstw, w tym przedsiębiorstw typu start-up

1. W stosownych przypadkach państwa członkowskie podejmują następujące działania dostosowane do potrzeb mikroprzedsiębiorstw i małych przedsiębiorstw:

a) organizują specjalne działania uświadamiające i szkoleniowe dotyczące stosowania niniejszego rozporządzenia;

b) ustanawiają specjalny kanał komunikacji z mikroprzedsiębiorstwami i małymi przedsiębiorstwami oraz, w stosownych przypadkach, z lokalnymi organami publicznymi w celu udzielania porad i odpowiedzi na pytania dotyczące wdrażania niniejszego rozporządzenia;

c) wspierają działania w zakresie testowania i oceny zgodności, w tym w stosownych przypadkach przy wsparciu Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa.

2. Państwa członkowskie mogą, w stosownych przypadkach, ustanowić piaskownice regulacyjne w zakresie cyberodporności. Takie piaskownice regulacyjne zapewniają kontrolowane środowiska testowe dla innowacyjnych produktów z elementami cyfrowymi, aby ułatwić ich opracowywanie, projektowanie, walidację i testowanie w celu zapewnienia zgodności z niniejszym rozporządzeniem przez ograniczony czas przed wprowadzeniem do obrotu. Komisja oraz, w stosownych przypadkach, ENISA mogą zapewnić wsparcie techniczne, doradztwo i narzędzia na potrzeby ustanowienia i funkcjonowania piaskownic regulacyjnych. Piaskownice regulacyjne są tworzone pod bezpośrednim nadzorem organów nadzoru rynku, zgodnie z ich wytycznymi i przy ich wsparciu. Państwa członkowskie informują Komisję i inne organy nadzoru rynku o utworzeniu piaskownicy regulacyjnej za pośrednictwem grupy ADCO. Piaskownice regulacyjne pozostają bez wpływu na uprawnienia właściwych organów w zakresie nadzoru i stosowania środków naprawczych. Państwa członkowskie zapewniają otwarty, sprawiedliwy i przejrzysty dostęp do piaskownic regulacyjnych, a w szczególności ułatwiają dostęp mikroprzedsiębiorstwom i małym przedsiębiorstwom, w tym przedsiębiorstwom typu start-up.

3. Zgodnie z art. 26 Komisja zapewnia mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom wytyczne dotyczące wykonania niniejszego rozporządzenia.

4. Komisja ogłasza dostępne wsparcie finansowe w ramach regulacyjnych istniejących programów Unii, w szczególności w celu zmniejszenia obciążeń finansowych dla mikroprzedsiębiorstw oraz małych przedsiębiorstw.

5. Mikroprzedsiębiorstwa i małe przedsiębiorstwa mogą dostarczać wszystkie elementy dokumentacji technicznej określonej w załączniku VII przy użyciu uproszczonego formatu. W tym celu Komisja – w drodze aktów wykonawczych – określa uproszczony formularz dokumentacji technicznej ukierunkowany na potrzeby mikroprzedsiębiorstw i małych przedsiębiorstw, w tym sposób dostarczania elementów określonych w załączniku VII. W przypadku gdy mikroprzedsiębiorstwo lub małe przedsiębiorstwo postanowi przekazywać informacje określone w załączniku VII w sposób uproszczony, stosuje formularz, o którym mowa w niniejszym ustępie. Jednostki notyfikowane akceptują ten formularz do celów oceny zgodności.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

Artykuł 34

Umowy o wzajemnym uznawaniu

Uwzględniając poziom rozwoju technicznego i podejście do oceny zgodności państwa trzeciego, Unia może zawierać umowy o wzajemnym uznawaniu z państwami trzecimi, zgodnie z art. 218 TFUE, w celu wspierania i ułatwiania handlu międzynarodowego.

ROZDZIAŁ IV

NOTYFIKACJA JEDNOSTEK OCENIAJĄCYCH ZGODNOŚĆ

Artykuł 35

Notyfikacja

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

2. Państwa członkowskie dążą do zapewnienia, aby do dnia 11 grudnia 2026 r. wyznaczono w Unii wystarczającą liczbę jednostek notyfikowanych do przeprowadzania ocen zgodności, co pozwoli uniknąć wąskich gardeł oraz barier utrudniających wejście na rynek.

Artykuł 36

Organy notyfikujące

1. Każde państwo członkowskie wyznacza organ notyfikujący, który odpowiada za opracowanie i przeprowadzanie procedur koniecznych do oceny, wyznaczania i notyfikowania jednostek oceniających zgodność oraz do ich monitorowania, w tym na potrzeby zapewnienia zgodności z art. 41.

2. Państwa członkowskie mogą zdecydować, że ocena oraz monitorowanie, o których mowa w ust. 1, są prowadzone przez krajową jednostkę akredytującą w rozumieniu rozporządzenia (WE) nr 765/2008 oraz zgodnie z tym rozporządzeniem.

3. W przypadku gdy organ notyfikujący przekazuje lub w inny sposób powierza ocenę, notyfikację lub monitorowanie, o których mowa w ust. 1 niniejszego artykułu, podmiotowi, który nie jest instytucją rządową, taki podmiot musi posiadać osobowość prawną oraz stosować się odpowiednio do art. 37. Podmiot taki musi ponadto posiadać mechanizmy zapewniające pokrycie zobowiązań wynikających z jego działalności.

4. Organ notyfikujący ponosi pełną odpowiedzialność za zadania wykonywane przez podmiot, o którym mowa w ust. 3.

Artykuł 37

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 38

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 informacje, o których mowa w ust. 1, do wiadomości publicznej.

Artykuł 39

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 jest osobą trzecią, funkcjonującą niezależnie od organizacji lub produktu z elementami cyfrowymi, który ocenia.

Za taką osobę trzecią można uznać 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, 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, importerami, dystrybutorami, 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 takich produktów do celów prywatnych.

Jednostka oceniająca zgodność, jej kierownictwo najwyższego szczebla oraz pracownicy odpowiedzialni za realizację zadań związanych z oceną zgodności nie angażują się bezpośrednio w projektowanie, opracowywanie, przywóz, dystrybucję, produkcję, wprowadzanie do obrotu, instalację, użytkowanie lub konserwację produktów z elementami cyfrowymi, które oceniają, 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 VIII 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:

a) niezbędnym personelem posiadającym wiedzę techniczną oraz wystarczające doświadczenie, odpowiednie do realizacji zadań związanych z oceną zgodności;

b) niezbędnymi opisami procedur, zgodnie z którymi należy przeprowadzać ocenę zgodności, zapewniającymi przejrzystość i powtarzalność tych procedur; jednostka musi posiadać odpowiednią politykę i stosowne procedury, dzięki którym możliwe jest odróżnienie zadań, jakie wykonuje jako jednostka notyfikowana, od pozostałych działań;

c) niezbędnymi 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 oceniająca zgodność 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. Personel odpowiedzialny za realizację działań związanych z oceną zgodności musi 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 wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I, obowiązujących norm zharmonizowanych i wspólnych specyfikacji oraz stosownych przepisów unijnego prawodawstwa harmonizacyjnego i aktów wykonawczych;

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

8. Zapewnia 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 przejęta jest przez ich państwo członkowskie lub państwo członkowskie bezpośrednio odpowiada za ocenę zgodności.

10. Personel jednostki oceniającej zgodność jest zobowiązany dochować tajemnicy zawodowej w odniesieniu do wszystkich informacji, które uzyskuje w trakcie wykonywania swoich zadań zgodnie z załącznikiem VIII 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. 51, lub zapewniają informowanie o takiej działalności swojego personelu przeprowadzającego 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, proporcjonalnych i rozsądnych warunkach, unikając przy tym zbędnych obciążeń dla podmiotów gospodarczych, w szczególności biorąc pod uwagę interesy mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw w odniesieniu do opłat.

Artykuł 40

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*, domniemuje się, że jednostka ta spełnia wymogi określone w art. 39, jeżeli mające zastosowanie normy zharmonizowane obejmują te wymogi.

Artykuł 41

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. 39, 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 42

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 z elementami cyfrowymi wchodzących w zakres kompetencji danej jednostki, jak również, w stosownych przypadkach, certyfikat akredytacji wydany przez krajową jednostkę akredytującą, potwierdzający, że jednostka oceniająca zgodność spełnia wymogi określone w art. 39.

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. 39.

Artykuł 43

Procedura notyfikacji

1. Organy notyfikujące notyfikują wyłącznie te jednostki oceniające zgodność, które spełniają wymogi określone w art. 39.

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 z elementami cyfrowymi, których to dotyczy, oraz stosowne poświadczenie kompetencji.

4. W przypadku gdy podstawy notyfikacji nie stanowi certyfikat akredytacji, o którym mowa w art. 42 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. 39.

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 44

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 prawnych 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 45

Zmiany w notyfikacji

1. W przypadku gdy organ notyfikujący stwierdza lub otrzymuje informację, że jednostka notyfikowana przestała spełniać wymogi określone w art. 39 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 46

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 swojej 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 47

Obowiązki operacyjne jednostek notyfikowanych

1. Jednostki notyfikowane przeprowadzają oceny zgodności zgodnie z procedurami oceny zgodności określonymi w art. 32 i załączniku VIII.

2. Oceny zgodności przeprowadza się w sposób proporcjonalny, unikając przy tym zbędnych obciążeń dla podmiotów gospodarczych. Jednostki oceniające zgodność wykonują swoje działania, uwzględniając wielkość przedsiębiorstw, w szczególności mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, sektor, w którym działają, ich strukturę, stopień złożoności i poziom ryzyka w cyberprzestrzeni związanego z danymi produktami zawierającymi elementy cyfrowe oraz technologię i masowy lub seryjny charakter procesu produkcji.

3. Jednostki notyfikowane zachowują jednak odpowiednią rygorystyczność i odpowiedni poziom ochrony wymagane dla zagwarantowania zgodności produktów z elementami cyfrowymi z niniejszym rozporządzeniem.

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. 27, 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 z elementami cyfrowymi 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 48

Środek zaskarżenia od decyzji jednostek notyfikowanych

Państwa członkowskie zapewniają możliwość wniesienia środka zaskarżenia od decyzji jednostek notyfikowanych.

Artykuł 49

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 z elementami cyfrowymi odpowiednie informacje o kwestiach, w których wyniki oceny zgodności były negatywne, a na wniosek również tych, w których były one pozytywne.

Artykuł 50

Wymiana doświadczeń

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

Artykuł 51

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 52

Nadzór rynku i kontrola produktów z elementami cyfrowymi na rynku Unii

1. Do produktów z elementami cyfrowymi, które są objęte zakresem niniejszego rozporządzenia, stosuje się 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. Organy nadzoru rynku wyznaczone na podstawie ust. 2 niniejszego artykułu są również odpowiedzialne za prowadzenie działań w zakresie nadzoru rynku w odniesieniu do obowiązków opiekunów otwartego oprogramowania określonych w art. 24. W przypadku gdy organ nadzoru rynku stwierdzi, że opiekun otwartego oprogramowania nie spełnia obowiązków określonych w tym artykule, wymaga ona, aby opiekun otwartego oprogramowania zapewnił, że zostaną podjęte wszelkie odpowiednie działania naprawcze. Opiekunowie otwartego oprogramowania zapewniają, aby zostały podjęte wszelkie odpowiednie działania naprawcze w odniesieniu do ich obowiązków wynikających z niniejszego rozporządzenia.

4. W stosownych przypadkach organy nadzoru rynku współpracują z krajowymi organami ds. certyfikacji cyberbezpieczeństwa wyznaczonymi na mocy art. 58 rozporządzenia (UE) 2019/881 i regularnie wymieniają się informacjami. Wyznaczone organy nadzoru rynku regularnie współpracują i wymieniają się informacjami z CSIRT-ami wyznaczonymi na koordynatorów oraz z ENISA w odniesieniu do nadzoru nad realizacją obowiązków w zakresie zgłaszania, o których mowa w art. 14 niniejszego rozporządzenia.

5. Organy nadzoru rynku mogą zwrócić się do CSIRT-u wyznaczonego na koordynatora lub do ENISA o udzielenie im porad technicznych w kwestiach związanych z wdrażaniem i egzekwowaniem niniejszego rozporządzenia. Przeprowadzając postępowanie wyjaśniające zgodnie z art. 54, organy nadzoru rynku mogą zwrócić się do CSIRT-u wyznaczonego na koordynatora lub do ENISA o dostarczenie analizy na poparcie oceny zgodności produktów z elementami cyfrowymi.

6. W stosownych przypadkach organy nadzoru rynku współpracują z innymi organami nadzoru rynku wyznaczonymi na podstawie unijnego prawodawstwa harmonizacyjnego innego niż niniejsze rozporządzenie oraz regularnie wymieniają się informacjami.

7. W stosownych przypadkach organy nadzoru rynku współpracują z organami nadzorującymi egzekwowanie unijnego prawa ochrony 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. 10, jeżeli takie wskazówki i porady dotyczą przetwarzania danych osobowych.

Organy nadzorujące egzekwowanie unijnego prawa ochrony 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.

8. Państwa członkowskie zapewniają, aby wyznaczone organy nadzoru rynku dysponowały odpowiednimi zasobami finansowymi i technicznymi, w tym w stosownych przypadkach narzędziami automatyzacji przetwarzania, a także zasobami ludzkimi mającymi umiejętności w zakresie cyberbezpieczeństwa niezbędne do wykonywania zadań powierzonych im zgodnie z niniejszym rozporządzeniem.

9. Komisja zachęca do wymiany doświadczeń między wyznaczonymi organami nadzoru rynku i sprzyja jej.

10. Organy nadzoru rynku mogą udzielać podmiotom gospodarczym wskazówek i porad dotyczących wdrażania niniejszego rozporządzenia, przy wsparciu Komisji oraz, w stosownych przypadkach, CSIRT-ów i ENISA.

11. Organy nadzoru rynku informują konsumentów o tym, gdzie można składać skargi mogące wskazywać na niezgodność z niniejszym rozporządzeniem, zgodnie z art. 11 rozporządzenia (UE) 2019/1020, oraz o tym, gdzie i jak można uzyskać dostęp do mechanizmów ułatwiających zgłaszanie podatności, incydentów i cyberzagrożeń, które mogą mieć wpływ na produkty z elementami cyfrowymi.

12. Organy nadzoru rynku ułatwiają w stosownych przypadkach współpracę z odpowiednimi zainteresowanymi stronami, w tym organizacjami naukowymi, badawczymi i konsumenckimi.

13. 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.

14. W przypadku produktów z elementami cyfrowymi, które są objęte zakresem niniejszego rozporządzenia, zaklasyfikowanych jako systemy sztucznej inteligencji wysokiego ryzyka na mocy art. 6 rozporządzenia (UE) 2024/1689, organy nadzoru rynku wyznaczone do celów tego rozporządzenia są organami odpowiedzialnymi za działania w zakresie nadzoru rynku wymagane na podstawie niniejszego rozporządzenia. W stosownych przypadkach organy nadzoru rynku wyznaczone na podstawie rozporządzenia (UE) 2024/1689 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. 14 niniejszego rozporządzenia, z CSIRT-ami wyznaczonymi na koordynatorów oraz z ENISA. Organy nadzoru rynku wyznaczone na podstawie rozporządzenia (UE) 2024/1689 informują w szczególności organy nadzoru rynku wyznaczone na podstawie niniejszego rozporządzenia o wszelkich ustaleniach istotnych dla realizacji ich zadań związanych z wdrożeniem niniejszego rozporządzenia.

15. Do celów jednolitego stosowania niniejszego rozporządzenia ustanawia się 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. Grupa ADCO zajmuje się również szczegółowymi kwestiami związanymi z działaniami w zakresie nadzoru rynku w odniesieniu do obowiązków nałożonych na opiekunów otwartego oprogramowania.

16. Organy nadzoru rynku monitorują, jak producenci stosują kryteria, o których mowa w art. 13 ust. 8, przy określaniu okresu wsparcia dla ich produktów z elementami cyfrowymi.

Grupa ADCO podaje do wiadomości publicznej, w przyjaznej dla użytkownika formie, odpowiednie statystyki dotyczące kategorii produktów z elementami cyfrowymi, w tym średnich okresów wsparcia, określonych przez producenta zgodnie z art. 13 ust. 8, a także zapewnia wytyczne zawierające orientacyjne okresy wsparcia dla kategorii produktów z elementami cyfrowymi.

Jeżeli dane wskazują, że okresy wsparcia dla określonych kategorii produktów z elementami cyfrowymi są niedostateczne, grupa ADCO może wydać zalecenia dla organów nadzoru rynku, aby skoncentrowały swoje działania na takich kategoriach produktów z elementami cyfrowymi.

Artykuł 53

Dostęp do danych i dokumentacji

Jeżeli jest to konieczne do oceny zgodności produktów z elementami cyfrowymi i procedur wprowadzonych przez ich producentów z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I, organom nadzoru rynku na uzasadniony wniosek przyznaje się dostęp, w języku łatwo zrozumiałym dla tych organów, do danych niezbędnych do oceny projektu, procesu opracowania, produkcji i postępowania w przypadku wykrycia podatności, w tym dostęp do powiązanej dokumentacji wewnętrznej dotyczącej odnośnego podmiotu gospodarczego.

Artykuł 54

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

1. Jeżeli organ nadzoru rynku państwa członkowskiego ma wystarczający powód sądzić, że produkt z elementami cyfrowymi, w tym dotyczące go postępowanie w przypadku wykrycia podatności, stwarza istotne ryzyko w cyberprzestrzeni, organ przeprowadza, bez zbędnej zwłoki i w stosownych przypadkach we współpracy z odpowiednim CSIRT-em, 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 w cyberprzestrzeni, zgodnie z zaleceniami organu nadzoru rynku.

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

2. Określając znaczenie ryzyka w cyberprzestrzeni, o którym mowa w ust. 1 niniejszego artykułu, organy nadzoru rynku uwzględniają również pozatechniczne czynniki ryzyka, w szczególności te ustalone w wyniku skoordynowanych na poziomie Unii ocen ryzyka w zakresie bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzonych zgodnie z art. 22 dyrektywy (UE) 2022/2555. W przypadku gdy organ nadzoru rynku ma wystarczający powód sądzić, że produkt z elementami cyfrowymi stwarza istotne ryzyko w cyberprzestrzeni w świetle pozatechnicznych czynników ryzyka, informuje o tym właściwe organy wyznaczone lub ustanowione na podstawie art. 8 dyrektywy (UE) 2022/2555 i w razie potrzeby współpracuje z tymi organami.

3. 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.

4. Podmiot gospodarczy zapewnia podjęcie wszelkich odpowiednich działań naprawczych w odniesieniu do wszystkich określonych produktów z elementami cyfrowymi, które udostępnił na rynku w całej Unii.

5. W przypadku niepodjęcia przez podmiot gospodarczy 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 z elementami cyfrowymi na rynku krajowym, wycofania produktu z obrotu lub odzyskania go.

Organ ten niezwłocznie notyfikuje te środki Komisji i pozostałym państwom członkowskim.

6. Informacje, o których mowa w ust. 5, obejmują wszelkie dostępne informacje szczegółowe, w szczególności dane niezbędne do identyfikacji niezgodnego z przepisami produktu z elementami cyfrowymi, pochodzenie tego 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 z elementami cyfrowymi lub procedury wprowadzone przez producenta zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I;

b) niedociągnięć w normach zharmonizowanych, europejskich programach certyfikacji cyberbezpieczeństwa lub wspólnych specyfikacjach, o których mowa w art. 27.

7. 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 elementami cyfrowymi z przepisami lub przedstawiają swoje zastrzeżenia, jeżeli nie zgadzają się ze zgłoszonym środkiem krajowym.

8. W przypadku gdy w terminie trzech miesięcy od dnia otrzymania notyfikacji, o której mowa w ust. 5 niniejszego artykułu, ani państwo członkowskie, ani Komisja nie zgłoszą sprzeciwu wobec środka tymczasowego przyjętego 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.

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

Artykuł 55

Unijna procedura ochronna

1. Jeżeli w terminie trzech miesięcy od dnia otrzymania informacji, o której mowa w art. 54 ust. 5, państwo członkowskie zgłosi zastrzeżenia dotyczące środka wprowadzonego przez inne państwo członkowskie lub jeżeli Komisja uzna taki środek za sprzeczny z prawem 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. 54 ust. 5, 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 produktu z elementami cyfrowymi ze swoich rynków oraz informują o tym Komisję. W przypadku gdy środek krajowy nie zostaje uznany za uzasadniony, państwo członkowskie, którego to dotyczy, cofa go.

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. 11 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. 27, Komisja rozważa, czy zmienić lub uchylić którykolwiek akt delegowany przyjęty na podstawie art. 27 ust. 9, 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. 27, Komisja rozważa, czy zmienić lub uchylić akt wykonawczy przyjęty na podstawie art. 27 ust. 2, określający te wspólne specyfikacje.

Artykuł 56

Procedura na poziomie Unii dotycząca produktów z elementami cyfrowymi stwarzających istotne ryzyko w cyberprzestrzeni

1. W przypadku gdy Komisja ma wystarczający powód sądzić, w tym na podstawie informacji przekazanych przez ENISA, że produkt z elementami cyfrowymi, który stwarza istotne ryzyko w cyberprzestrzeni, nie spełnia wymogów określonych w niniejszym rozporządzeniu, informuje o tym odpowiednie organy nadzoru rynku. W przypadku gdy organy nadzoru rynku przeprowadzają ocenę tego produktu z elementami cyfrowymi, który może stwarzać znaczące ryzyko w cyberprzestrzeni w związku z jego zgodnością z wymogami określonymi w niniejszym rozporządzeniu, stosuje się procedury, o których mowa w art. 54 i 55.

2. W przypadku gdy Komisja ma wystarczający powód sądzić, że produkt z elementami cyfrowymi stwarza istotne ryzyko w cyberprzestrzeni w świetle pozatechnicznych czynników ryzyka, informuje o tym właściwe organy nadzoru rynku oraz, w stosownych przypadkach, właściwe organy wyznaczone lub ustanowione na podstawie art. 8 dyrektywy (UE) 2022/2555 i w razie potrzeby współpracuje z tymi organami. Komisja rozpatruje również znaczenie zidentyfikowanego ryzyka dla tego produktu z elementami cyfrowymi w świetle swoich zadań dotyczących skoordynowanych na poziomie Unii szacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw, o których mowa w art. 22 dyrektywy (UE) 2022/2555, i w razie potrzeby konsultuje się z Grupą Współpracy ustanowioną na podstawie art. 14 dyrektywy (UE) 2022/2555 i z ENISA.

3. W okolicznościach, które uzasadniają niezwłoczną interwencję w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego, i jeżeli Komisja ma wystarczający powód sądzić, że produkt z elementami cyfrowymi, 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 przeprowadza ocenę zgodności i może zwrócić się do ENISA o dostarczenie analizy na jej poparcie. Komisja informuje o tym odpowiednie organy nadzoru rynku. W razie potrzeby odpowiednie podmioty gospodarcze współpracują z ENISA.

4. Na podstawie oceny, o której mowa w ust. 3, Komisja może zdecydować, że konieczne jest wprowadzenie środka naprawczego lub ograniczającego na poziomie Unii. W tym celu Komisja niezwłocznie przeprowadza konsultacje z zainteresowanymi państwami członkowskimi i odpowiednim podmiotem gospodarczym lub podmiotami gospodarczymi.

5. Na podstawie konsultacji, o których mowa w ust. 4 niniejszego artykułu, Komisja może przyjąć akty wykonawcze w celu określenia środków naprawczych lub ograniczających na poziomie Unii, w tym wymagające wycofania z obrotu lub odzyskania określonych produktów z elementami cyfrowymi w rozsądnym terminie, stosownym do charakteru ryzyka. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

6. Komisja niezwłocznie informuje odpowiedni podmiot gospodarczy lub odpowiednie podmioty gospodarcze o aktach wykonawczych, o których mowa w ust. 5. Państwa członkowskie niezwłocznie wprowadzają w życie te akty wykonawcze i informują o tym Komisję.

7. Przepisy ust. 3–6 mają zastosowanie przez okres trwania wyjątkowej sytuacji, która uzasadniała interwencję Komisji, pod warunkiem że nie zapewniono zgodności danego produktu z elementami cyfrowymi z niniejszym rozporządzeniem.

Artykuł 57

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

1. Organ nadzoru rynku państwa członkowskiego zobowiązuje podmiot gospodarczy do podjęcia wszelkich odpowiednich środków, jeżeli po przeprowadzeniu oceny na podstawie art. 54 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:

a) zdrowia lub bezpieczeństwa osób;

b) wypełnienia obowiązków wynikających z prawa Unii lub prawa krajowego mających na celu ochronę praw podstawowych;

c) dostępności, autentyczności, integralności lub poufności usług oferowanych przy użyciu elektronicznego systemu informacyjnego przez podmioty niezbędne, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555; lub

d) innych aspektów ochrony interesu publicznego.

Środki, o których mowa w akapicie pierwszym, mogą obejmować środki mające na celu zapewnienie, aby dany produkt z elementami cyfrowymi i procedury wprowadzone przez producenta nie stwarzały już określonego ryzyka w momencie udostępnienia na rynku, wycofania z obrotu danego produktu z elementami cyfrowymi lub jego odzyskania, i są stosowne do charakteru tego ryzyka.

2. Producent lub inne właściwe podmioty gospodarcze zapewniają podjęcie działań naprawczych w odniesieniu do określonych 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 decyzję, o której mowa w ust. 4, do państw członkowskich.

6. W przypadku gdy Komisja ma wystarczający powód sądzić, 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 niniejszego artykułu, informuje ona odpowiedni organ lub odpowiednie organy nadzoru rynku i może zwrócić się do nich o przeprowadzenie oceny i zastosowanie procedur, o których mowa w art. 54 oraz w ust. 1, 2 i 3 niniejszego artykułu.

7. W okolicznościach, które uzasadniają niezwłoczną interwencję w celu utrzymania prawidłowego funkcjonowania rynku wewnętrznego, i jeżeli Komisja ma wystarczający powód sądzić, że produkt z elementami cyfrowymi, 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 przeprowadza ocenę ryzyka stwarzanego przez ten produkt z elementami cyfrowymi i może zwrócić się do ENISA o dostarczenie analizy na poparcie tej oceny oraz informuje o tym odpowiednie organy nadzoru rynku. W razie potrzeby odpowiednie podmioty gospodarcze współpracują z ENISA.

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

9. Na podstawie konsultacji, o których mowa w ust. 8 niniejszego artykułu, Komisja może przyjąć akty wykonawcze w celu podjęcia decyzji o wprowadzeniu środków naprawczych lub ograniczających na poziomie Unii, w tym wymagających wycofania określonych produktów z elementami cyfrowymi z obrotu lub odzyskania ich w rozsądnym terminie, stosownym do charakteru ryzyka. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

10. Komisja niezwłocznie informuje odpowiedni podmiot gospodarczy lub odpowiednie podmioty gospodarcze o aktach wykonawczych, o których mowa w ust. 9. Państwa członkowskie niezwłocznie wprowadzają w życie te akty wykonawcze i informują o tym Komisję.

11. Przepisy ust. 6–10 stosuje się przez okres trwania wyjątkowej sytuacji, która uzasadniała interwencję Komisji, oraz tak długo, jak dany produkt z elementami cyfrowymi stwarza ryzyko, o którym mowa w ust. 1.

Artykuł 58

Formalna niezgodność z przepisami

1. Jeżeli organ nadzoru rynku państwa członkowskiego stwierdzi jedno z poniższych, wymaga od właściwego producenta usunięcia danej niezgodności:

a) umieszczenie oznakowania CE z naruszeniem art. 29 i 30;

b) nieumieszczenie oznakowania CE;

c) niesporządzenie deklaracji zgodności UE;

d) nieprawidłowe sporządzenie deklaracji zgodności UE;

e) w stosownych przypadkach nieumieszczenie numeru identyfikacyjnego jednostki notyfikowanej uczestniczącej w procedurze oceny zgodności;

f) niedostępna albo niekompletna dokumentacja techniczna.

2. Jeżeli niezgodność, o której mowa w ust. 1, utrzymuje się, dane państwo członkowskie wprowadza wszelkie odpowiednie środki, by ograniczyć lub zakazać udostępniania danego produktu z elementami cyfrowymi na rynku bądź zapewnić jego odzyskanie lub wycofanie z obrotu.

Artykuł 59

Wspólne działania organów nadzoru rynku

1. Organy nadzoru rynku mogą zawierać z innymi odpowiednimi organami porozumienia o wspólnych działaniach mających zapewnić cyberbezpieczeństwo i ochronę konsumentów w odniesieniu do określonych produktów z elementami cyfrowymi wprowadzonych do obrotu lub udostępnionych na rynku, zwłaszcza produktów z elementami cyfrowymi często stwarzających ryzyko w cyberprzestrzeni.

2. Komisja lub ENISA proponują przeprowadzenie przez organy nadzoru rynku wspólnych działań z zakresu kontroli zgodności z niniejszym rozporządzeniem na podstawie wskazań lub informacji w szeregu państw członkowskich o potencjalnej niezgodności produktów z elementami cyfrowymi objętych zakresem stosowania niniejszego rozporządzenia z określonymi w nim wymogami.

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

4. Organ nadzoru rynku może wykorzystać wszelkie informacje uzyskane w wyniku wspólnych działań prowadzonych w ramach wszczętego przezeń postępowania przygotowawczego.

5. Dany organ nadzoru rynku oraz, w stosownych przypadkach, Komisja udostępniają publicznie porozumienie o wspólnych działaniach, w tym nazwy uczestniczących stron.

Artykuł 60

Akcje kontrolne

1. Organy nadzoru rynku prowadzą jednoczesne skoordynowane akcje kontrolne dotyczące określonych produktów z elementami cyfrowymi lub ich kategorii w celu sprawdzenia zgodności z niniejszym rozporządzeniem lub wykrycia jego naruszeń. Akcje kontrolne mogą obejmować kontrole produktów z elementami cyfrowymi nabytych pod ukrytą tożsamością.

2. Akcje kontrolne koordynuje Komisja, chyba że uczestniczące w nich organy nadzoru rynku uzgodnią inaczej. Koordynator akcji kontrolnej w stosownych przypadkach podaje zagregowane wyniki do publicznej wiadomości.

3. Jeżeli wykonując swoje zadania, w tym na podstawie zgłoszeń otrzymanych zgodnie z art. 14 ust. 1 i 3, ENISA wykryje kategorie produktów z elementami cyfrowymi, dla których można organizować akcje kontrolne, przedkłada propozycję akcji kontrolnej koordynatorowi, o którym mowa w ust. 2 niniejszego artykułu, do rozpatrzenia przez organy nadzoru rynku.

4. Prowadząc akcje kontrolne, uczestniczące w nich organy nadzoru rynku mogą korzystać z uprawnień w zakresie postępowania przygotowawczego określonych w art. 52–58 i wszelkich innych uprawnień nadanych im na mocy przepisów prawa krajowego.

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

ROZDZIAŁ VI

PRZEKAZANE UPRAWNIENIA I PROCEDURA KOMITETOWA

Artykuł 61

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. 5 akapit drugi, art. 7 ust. 3, art. 8 ust. 1 i 2, art. 13 ust. 8 akapit czwarty, art. 14 ust. 9, art. 25, art. 27 ust. 9, art. 28 ust. 5 i art. 31 ust. 5, powierza się Komisji na okres pięciu lat od dnia 10 grudnia 2024 r. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu pięciu lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.

3. Przekazanie uprawnień, o którym mowa w art. 2 ust. 5 akapit drugi, art. 7 ust. 3, art. 8 ust. 1 i 2, art. 13 ust. 8 akapit czwarty, art. 14 ust. 9, art. 25, art. 27 ust. 9, art. 28 ust. 5 i art. 31 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. 5 akapit drugi, art. 7 ust. 3, art. 8 ust. 1 lub 2, art. 13 ust. 8 akapit czwarty, art. 14 ust. 9, art. 25, art. 27 ust. 9, art. 28 ust. 5 lub art. 31 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 62

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 63

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 (UE) 2016/943 ([37]);

b) skuteczne wdrożenie niniejszego rozporządzenia, zwłaszcza do celów inspekcji, postępowań przygotowawczych 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 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 się informacjami szczególnie chronionymi z odpowiednimi organami państw trzecich, z którymi zawarły dwustronne lub wielostronne porozumienia o poufności gwarantujące odpowiedni stopień ochrony.

Artykuł 64

Kary

1. Państwa członkowskie ustanawiają przepisy dotyczące kar za naruszenie przepisów niniejszego rozporządzenia i stosują wszelkie środki niezbędne do zapewnienia ich wykonywania. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają niezwłocznie Komisję o tych przepisach i środkach oraz o wszelkich późniejszych zmianach w nich.

2. Niezgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I oraz z obowiązkami określonymi w art. 13 i 14 podlega administracyjnej karze pieniężnej w wysokości do 15 000 000 EUR lub, jeżeli za naruszenie odpowiada przedsiębiorstwo – w wysokości do 2,5 % jego łącznego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot jest wyższa.

3. Niezgodność z obowiązkami określonymi w art. 18–23, art. 28, art. 30 ust. 1–4, art. 31 ust. 1–4, art. 32 ust. 1, 2 i 3, art. 33 ust. 5, art. 39, 41, 47, 49 i 53 podlega administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR lub, jeżeli za naruszenie odpowiada przedsiębiorstwo – w wysokości do 2 % jego łącznego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot jest wyższa.

4. Przekazywanie jednostkom notyfikowanym i organom nadzoru rynku w odpowiedzi na ich wniosek informacji nieprawidłowych, niekompletnych lub wprowadzających w błąd podlega administracyjnej karze pieniężnej w wysokości do 5 000 000 EUR lub, jeżeli za naruszenie odpowiada przedsiębiorstwo – w wysokości do 1 % jego łącznego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot jest wyższa.

([37]) 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).

5. 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 te same lub inne organy nadzoru rynku nałożyły już na ten sam podmiot gospodarczy administracyjne kary pieniężne za podobne naruszenie;

c) wielkość podmiotu gospodarczego dopuszczającego się naruszenia, zwłaszcza w przypadku mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, w tym przedsiębiorstw typu start-up, a także jego udział w rynku.

6. Organy nadzoru rynku, które stosują administracyjne kary pieniężne, przekazują informacje o ich nałożeniu organom nadzoru rynku pozostałych państw członkowskich za pośrednictwem systemu informacyjnego i komunikacyjnego, o którym mowa w art. 34 rozporządzenia (UE) 2019/1020.

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

8. 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 poziomie krajowym w tych państwach członkowskich. Stosowanie takich przepisów w tych państwach członkowskich ma skutek równoważny.

9. 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.

10. Na zasadzie odstępstwa od ust. 3–9 administracyjne kary pieniężne, o których mowa w tych ustępach, nie mają zastosowania do:

a) producentów kwalifikujących się jako mikroprzedsiębiorstwa lub małe przedsiębiorstwa w przypadku niedotrzymania terminu, o którym mowa w art. 14 ust. 2 lit. a) lub art. 14 ust. 4 lit. a);

b) wszelkich naruszeń niniejszego rozporządzenia przez opiekunów oprogramowania otwartego.

Artykuł 65

Powództwa przedstawicielskie

Do powództw przedstawicielskich wytaczanych przeciwko podmiotom gospodarczym za naruszenia przepisów niniejszego rozporządzenia szkodzące lub mogące szkodzić zbiorowym interesom konsumentów zastosowanie ma dyrektywa (UE) 2020/1828.

ROZDZIAŁ VIII

PRZEPISY PRZEJŚCIOWE I KOŃCOWE

Artykuł 66

Zmiana w rozporządzeniu (UE) 2019/1020

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

„72. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 (*).

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz.U. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).”.

Artykuł 67

Zmiana dyrektywy (UE) 2020/1828

W załączniku I do dyrektywy (UE) 2020/1828 dodaje się punkt w brzmieniu:

„69) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2487 (*).

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2487 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz.U. L, 2024/2487, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).”.

Artykuł 68

Zmiana rozporządzenia (UE) nr 168/2013

W części C1 w tabeli w załączniku II do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 168/2013 ([38]) dodaje się pozycję w brzmieniu:

”

16	18	ochrona pojazdu przed cyberatakami		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

”

Artykuł 69

Przepisy przejściowe

1. Certyfikaty badania typu UE i decyzje o zatwierdzeniu wydane w odniesieniu do wymagań w zakresie cyberbezpieczeństwa dotyczących produktów z elementami cyfrowymi, które podlegają unijnemu prawodawstwu harmonizacyjnemu innemu niż niniejsze rozporządzenie, zachowują ważność do dnia 11 czerwca 2028 r., chyba że ich ważność wygasa przed tą datą lub że określono inaczej w tym innym prawodawstwie harmonizacyjnym Unii, kiedy to zachowują ważność zgodnie z tym prawodawstwem.

2. Produkty z elementami cyfrowymi, które wprowadzono do obrotu przed dniem 11 grudnia 2027 r., podlegają wymaganiom określonym w niniejszym rozporządzeniu tylko wtedy, gdy po tej dacie nastąpią istotne modyfikacje tych produktów.

3. Na zasadzie odstępstwa od ust. 2 niniejszego artykułu obowiązki określone w art. 14 stosuje się do wszystkich produktów z elementami cyfrowymi objętych zakresem stosowania niniejszego rozporządzenia, które wprowadzono do obrotu przed dniem 11 grudnia 2027 r.

Artykuł 70

Ocena i przegląd

1. Do dnia 11 grudnia 2030 r., a następie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdania z oceny i przeglądu niniejszego rozporządzenia. Sprawozdania te są podawane do wiadomości publicznej.

2. Do dnia 11 września 2028 r. Komisja, po konsultacji z ENISA i siecią CSIRT, przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie oceniające skuteczność jednolitej platformy sprawozdawczej, o której mowa w art. 16, a także wpływ stosowania przez wyznaczonych na koordynatorów CSIRT-y względów cyberbezpieczeństwa, o których mowa w art. 16 ust. 2, na skuteczność jednolitej platformy sprawozdawczej pod kątem terminowego rozpowszechniania otrzymanych zgłoszeń wśród innych odpowiednich CSIRT-ów.

Artykuł 71

Wejście w życie i rozpoczęcie stosowania

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

([38]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 168/2013 z dnia 15 stycznia 2013 r. w sprawie homologacji i nadzoru rynku pojazdów dwu- lub trzykołowych oraz czterokołowców (Dz.U. L 60 z 2.3.2013, s. 52).

2. Niniejsze rozporządzenie stosuje się od dnia 11 grudnia 2027 r.

Art. 14 stosuje się jednak od dnia 11 września 2026 r., a rozdział IV (art. 35–51) stosuje się od dnia 11 czerwca 2026 r.

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

Sporządzono w Strasburgu dnia 23 października 2024 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*
R. METSOLA	ZSIGMOND B. P.

ZAŁĄCZNIK I

ZASADNICZE WYMAGANIA W ZAKRESIE CYBERBEZPIECZEŃSTWA

Część I Wymagania w zakresie cyberbezpieczeństwa dotyczące cech produktów z elementami cyfrowymi

1) Produkty z elementami cyfrowymi należy projektować, opracowywać i produkować tak, by zapewniały odpowiedni poziom cyberbezpieczeństwa stosownie do ryzyka;

2) Na podstawie oceny ryzyka w cyberprzestrzeni, o której mowa w art. 13 ust. 2, i w stosownych przypadkach produkty z elementami cyfrowymi:

   a) są udostępniane bez żadnych znanych i możliwych do wykorzystania podatności;

   b) są udostępniane na rynku w bezpiecznej konfiguracji domyślnej, obejmującej możliwość zresetowania produktu do stanu pierwotnego, chyba że producent i użytkownik biznesowy uzgodnią inaczej w odniesieniu do produktu z elementami cyfrowymi dostosowanego do indywidualnych potrzeb;

   c) zapewniają możliwość eliminowania podatności przez aktualizacje zabezpieczeń, w tym w stosownych przypadkach automatyczne aktualizacje zabezpieczeń instalowane w odpowiednim czasie dzięki ustawieniom domyślnym, z jasnym i łatwym do zastosowania mechanizmem opt-out oraz z powiadamianiem użytkowników o dostępnych aktualizacjach oraz możliwości ich tymczasowego odroczenia;

   d) zapewniają ochronę przed nieuprawnionym dostępem dzięki odpowiednim mechanizmom kontroli, w tym między innymi systemom uwierzytelniania, identyfikacji lub zarządzania dostępem, a także raportowania o potencjalnym nieuprawnionym dostępie;

   e) zapewniają ochronę poufności przechowywanych, przekazywanych lub w inny sposób przetwarzanych danych, w tym danych osobowych lub innych, w tym przez szyfrowanie odpowiednich danych odłożonych lub danych przesyłanych z wykorzystaniem najnowocześniejszych mechanizmów oraz przez zastosowanie innych środków technicznych;

   f) zapewniają ochronę integralności przechowywanych, przekazywanych lub w inny sposób przetwarzanych danych, w tym danych osobowych lub innych, komend, programów i konfiguracji przed wszelką manipulacją lub modyfikacją nieautoryzowaną przez użytkownika, a także powiadamiają o uszkodzeniach danych;

   g) przetwarzają tylko te dane, w tym dane osobowe lub inne, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne w związku z przeznaczeniem produktu z elementami cyfrowymi (minimalizacja danych);

   h) zapewniają ochronę dostępności najważniejszych i podstawowych funkcji, również po incydencie, w tym dzięki odporności na ataki typu „odmowa usługi" i środkom łagodzącym ich skutki;

   i) minimalizują negatywny wpływ samych produktów lub urządzeń podłączonych do internetu na dostępność usług dostarczanych przez inne urządzenia lub sieci;

   j) są projektowane, opracowywane i produkowane tak, by ograniczyć powierzchnię ataku, w tym interfejsów zewnętrznych;

   k) są projektowane, opracowywane i produkowane tak, by zmniejszyć wpływ incydentu przy użyciu odpowiednich mechanizmów i technik łagodzenia skutków wykorzystania;

   l) dostarczają informacje związane z bezpieczeństwem dzięki rejestrowaniu i monitorowaniu odpowiedniej aktywności wewnętrznej, w tym dostępu do danych, usług lub funkcji lub ich modyfikacji, z mechanizmem opt-out dla użytkownika;

   m) dają użytkownikom możliwość bezpiecznego i łatwego usuwania na stałe wszystkich danych i ustawień, a jeżeli takie dane mogą być przekazywane do innych produktów lub systemów, zapewniają, że odbywa się to bezpiecznie.

Część II Wymagania dotyczące postępowania w przypadku wykrycia podatności

Producenci produktów z elementami cyfrowymi mają obowiązek:

1) identyfikowania i dokumentowania podatności i komponentów zawartych w produkcie z elementami cyfrowymi, w tym przez sporządzenie zestawienia podstawowych materiałów do produkcji oprogramowania w powszechnie używanym formacie nadającym się do odczytu maszynowego, obejmującego co najmniej zależności najwyższego poziomu produktów;

2) w odniesieniu do ryzyka, jakie stwarzają produkty z elementami cyfrowymi – bezzwłocznego reagowania na podatności i ich eliminowania, w tym przez udostępnianie aktualizacji zabezpieczeń; jeżeli jest to technicznie wykonalne, nowe aktualizacje zabezpieczeń dostarcza się oddzielnie od aktualizacji funkcji;

3) przeprowadzania skutecznych i regularnych testów i przeglądów bezpieczeństwa produktu z elementami cyfrowymi;

4) po udostępnieniu aktualizacji zabezpieczeń – udostępniania i publicznego ujawniania informacji o naprawionych podatnościach, w tym opisu podatności, informacji pozwalających użytkownikom zidentyfikować produkt z elementami cyfrowymi, którego te podatności dotyczą, skutków podatności i ich dotkliwości, a także jasnych i dostępnych informacji pomagających użytkownikom wyeliminować podatności; w należycie uzasadnionych przypadkach, jeżeli producenci uznają, że ryzyko dla bezpieczeństwa związane z publikacją przewyższa korzyści w zakresie bezpieczeństwa, mogą opóźnić podanie do wiadomości publicznej informacji o naprawionych podatnościach do czasu, gdy użytkownicy będą mogli wprowadzić odpowiednią poprawkę (patch);

5) wprowadzania i egzekwowania polityki skoordynowanego ujawniania podatności;

6) przyjmowania środków ułatwiających wymianę informacji o potencjalnych podatnościach w ich produkcie z elementami cyfrowymi, a także w komponentach strony trzeciej zawartych w tym produkcie, w tym przez udostępnienie adresu do kontaktu służącego do zgłaszania podatności wykrytych w produkcie z elementami cyfrowymi;

7) zapewniania mechanizmów bezpiecznej dystrybucji aktualizacji zabezpieczeń produktów z elementami cyfrowymi w celu zapewnienia naprawy lub ograniczenia podatności w odpowiednim czasie, a w przypadku aktualizacji zabezpieczeń – automatycznie;

8) zapewniania – gdy dostępne są aktualizacje zabezpieczeń służące rozwiązaniu zidentyfikowanych problemów bezpieczeństwa – ich rozpowszechniania bezzwłocznie i bezpłatnie, chyba że producent i użytkownik biznesowy uzgodnią inaczej w odniesieniu do produktu z elementami cyfrowymi dostosowanego do indywidualnych potrzeb, wraz z komunikatami doradczymi zawierającymi odpowiednie informacje dla użytkowników, w tym o potencjalnych działaniach, które należy podjąć.

ZAŁĄCZNIK II

INFORMACJE I INSTRUKCJE DLA UŻYTKOWNIKÓW

Produktowi z elementami cyfrowymi muszą towarzyszyć co najmniej następujące informacje:

1) imię i nazwisko lub nazwa, zarejestrowana nazwa handlowa lub zarejestrowany znak towarowy producenta oraz adres pocztowy, adres e-mail lub inna cyfrowa forma kontaktu, a jeżeli jest dostępna – również strona internetowa, za pomocą której można skontaktować się z producentem;

2) pojedynczy punkt kontaktowy, w którym można zgłosić i otrzymać informacje o podatnościach produktu z elementami cyfrowymi oraz o tym, gdzie można się zapoznać z polityką producenta w zakresie skoordynowanego ujawniania podatności;

3) nazwa i rodzaj oraz wszelkie dodatkowe informacje umożliwiające jednoznaczną identyfikację produktu z elementami cyfrowymi;

4) przeznaczenie produktu z elementami cyfrowymi, w tym środowisko bezpieczeństwa zapewnione przez producenta, a także zasadnicze funkcje produktu i informacje o zabezpieczeniach;

5) wszelkie znane lub dające się przewidzieć okoliczności wykorzystania produktu z elementami cyfrowymi zgodnie z przeznaczeniem lub w warunkach racjonalnie przewidywalnego niewłaściwego wykorzystania, które mogą powodować istotne ryzyko w cyberprzestrzeni;

6) w stosownych przypadkach adres strony internetowej, na której jest dostępna deklaracja zgodności UE;

7) rodzaj wsparcia technicznego w zakresie bezpieczeństwa oferowanego przez producenta oraz data zakończenia okresu wsparcia, przez który użytkownicy mogą spodziewać się, że podatności zostaną usunięte i otrzymywania aktualizacji zabezpieczeń;

8) szczegółowe instrukcje lub adres strony internetowej z takimi szczegółowymi instrukcjami oraz informacjami na temat:

   a) środków niezbędnych do zapewnienia bezpiecznego użytkowania produktu z elementami cyfrowymi przy pierwszym uruchomieniu oraz przez cały okres użytkowania;

   b) możliwego wpływu zmian w produkcie z elementami cyfrowymi na bezpieczeństwo danych;

   c) sposobu instalowania aktualizacji istotnych dla bezpieczeństwa;

   d) bezpiecznego wycofania produktu z elementami cyfrowymi z użytku, w tym informacji o tym, jak bezpiecznie usunąć dane użytkownika;

   e) wyłączenia ustawień domyślnych umożliwiających automatyczną instalację aktualizacji zabezpieczeń, zgodnie z wymaganiami załącznika I część I pkt 2 lit. c);

   f) jeżeli produkt z elementami cyfrowymi ma być integrowany z innymi produktami z elementami cyfrowymi – informacje niezbędne osobie integrującej do spełnienia zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I oraz wymagań dotyczących dokumentacji określonych w załączniku VII;

9) jeżeli producent zdecyduje, że udostępni użytkownikowi zestawienie podstawowych materiałów do produkcji oprogramowania, informacje o tym, gdzie można uzyskać dostęp do tego zestawienia.

ZAŁĄCZNIK III

WAŻNE PRODUKTY Z ELEMENTAMI CYFROWYMI

Klasa I

1. Oprogramowanie systemów zarządzania tożsamością i zarządzania uprzywilejowanym dostępem oraz odpowiedni sprzęt, w tym czytniki do uwierzytelniania i kontroli dostępu, także biometryczne
2. Samodzielne i wbudowane przeglądarki
3. Menedżery haseł
4. Oprogramowanie, które wyszukuje, usuwa lub poddaje kwarantannie złośliwe oprogramowanie
5. Produkty z elementami cyfrowymi z funkcją wirtualnej sieci prywatnej (VPN)
6. Systemy zarządzania siecią
7. Systemy zarządzania informacjami i zdarzeniami zabezpieczeń (SIEM)
8. Menedżery uruchamiania systemu
9. Infrastruktura klucza publicznego i oprogramowanie do wystawiania certyfikatów cyfrowych
10. Fizyczne i wirtualne interfejsy sieciowe
11. Systemy operacyjne
12. Routery, modemy przeznaczone do podłączenia do internetu oraz przełączniki
13. Mikroprocesory z funkcjami bezpieczeństwa
14. Mikrokontrolery z funkcjami bezpieczeństwa
15. Specjalizowane układy scalone (ASIC) i bezpośrednio programowalne macierze bramek (FPGA) z funkcjami bezpieczeństwa
16. Wirtualni asystenci inteligentnego domu ogólnego przeznaczenia
17. Produkty inteligentnego domu z funkcjami bezpieczeństwa, w tym inteligentne zamki do drzwi, kamery systemów bezpieczeństwa, nianie elektroniczne i systemy alarmowe
18. Zabawki podłączone do internetu objęte dyrektywą Parlamentu Europejskiego i Rady 2009/48/WE ([1]) z interaktywnymi funkcjami społecznymi (np. mówienie lub filmowanie) lub z funkcją śledzenia lokalizacji
19. Produkty do noszenia lub umieszczania na ciele ludzkim mające monitorować stan zdrowia (np. śledzące aktywność fizyczną), do których nie stosuje się rozporządzenia (UE) 2017/745 ani rozporządzenia (UE) 2017/746, lub przedmioty osobiste do noszenia na ciele, które mają być używane przez dzieci i dla dzieci

Klasa II

1. Hiperwizory i systemy środowiska uruchomieniowego, które wspomagają zwirtualizowane wykonanie systemów operacyjnych i podobnych środowisk
2. Zapory sieciowe, systemy wykrywania włamań lub zapobiegania włamaniom
3. Mikroprocesory odporne na manipulacje
4. Mikrokontrolery odporne na manipulacje

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2009/48/WE z dnia 18 czerwca 2009 r. w sprawie bezpieczeństwa zabawek (Dz. U. L 170 z 30.6.2009, s. 1).

ZAŁĄCZNIK IV

PRODUKTY KRYTYCZNE Z ELEMENTAMI CYFROWYMI

1. Urządzenia sprzętowe ze skrzynkami zabezpieczającymi
2. Bramy inteligentnych liczników w inteligentnych systemach pomiarowych zdefiniowanych w art. 2 pkt 23 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/944 ([1]) oraz inne urządzenia do zaawansowanych celów bezpieczeństwa, w tym do bezpiecznego kryptoprzetwarzania
3. Karty inteligentne lub podobne urządzenia, w tym elementy zabezpieczające

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/944 z dnia 5 czerwca 2019 r. w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej oraz zmieniająca dyrektywę 2012/27/UE (Dz.U. L 158 z 14.6.2019, s. 125).

ZAŁĄCZNIK V

DEKLARACJA ZGODNOŚCI UE

W deklaracji zgodności UE, o której mowa w art. 28, należy zamieścić wszystkie następujące informacje:

1) nazwę i rodzaj oraz wszelkie dodatkowe informacje umożliwiające jednoznaczną identyfikację produktu z elementami cyfrowymi

2) nazwę lub imię i nazwisko oraz adres producenta lub jego upoważnionego przedstawiciela

3) oświadczenie, że deklarację zgodności UE wydano na wyłączną odpowiedzialność dostawcy

4) przedmiot deklaracji (identyfikacja produktu z elementami cyfrowymi umożliwiająca identyfikowalność, w stosownych przypadkach wraz z fotografią)

5) oświadczenie, że opisany powyżej przedmiot deklaracji jest zgodny z odpowiednimi wymaganiami unijnego prawodawstwa harmonizacyjnego

6) odniesienia do wszelkich zastosowanych odpowiednich norm zharmonizowanych lub wszelkich innych wspólnych specyfikacji lub certyfikacji cyberbezpieczeństwa, z którymi deklaruje się zgodność

7) w stosownych przypadkach nazwę i numer jednostki notyfikowanej, opis przeprowadzonej procedury oceny zgodności oraz dane identyfikacyjne wydanego certyfikatu

8) informacje dodatkowe:

Podpisano w imieniu:

(miejsce i data wydania):

(imię i nazwisko, stanowisko) (podpis):

ZAŁĄCZNIK VI

UPROSZCZONA DEKLARACJA ZGODNOŚCI UE

Uproszczoną deklarację zgodności UE, o której mowa w art. 13 ust. 20, składa się w następującej formie:

… [nazwa producenta] niniejszym oświadcza, że produkt z elementami cyfrowymi typu … [nazwa typu produktu z elementem cyfrowym] jest zgodny z rozporządzeniem (UE) 2024/2847 ([1]).

Pełny tekst deklaracji zgodności UE jest dostępny pod następującym adresem internetowym: …

([1]) Dz.U. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

ZAŁĄCZNIK VII

ZAWARTOŚĆ DOKUMENTACJI TECHNICZNEJ

Dokumentacja techniczna, o której mowa w art. 31, musi zawierać co najmniej te spośród następujących informacji, które mają zastosowanie do danego produktu z elementami cyfrowymi:

1) ogólny opis produktu z elementami cyfrowymi, w tym:

   a) jego przeznaczenie;

   b) wersje oprogramowania mające wpływ na zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa;

   c) jeżeli produkt z elementami cyfrowymi jest sprzętem – zdjęcia lub ilustracje przedstawiające cechy zewnętrzne, oznakowanie i układ wewnętrzny;

   d) informacje i instrukcje dla użytkowników zgodnie z treścią załącznika II;

2) opis projektowania, opracowywania i produkcji produktu z elementami cyfrowymi oraz procedur postępowania w przypadku wykrycia podatności, w tym:

   a) niezbędne informacje o projektowaniu i opracowaniu produktu z elementami cyfrowymi, w tym w stosownych przypadkach rysunki i schematy lub opis architektury systemu wyjaśniający, jak elementy oprogramowania współgrają ze sobą lub wzajemnie się uzupełniają oraz włączają się w ogólne przetwarzanie;

   b) niezbędne informacje i specyfikacje wprowadzonych przez producenta procedur postępowania w przypadku wykrycia podatności, w tym zestawienie podstawowych materiałów do produkcji oprogramowania, politykę skoordynowanego ujawniania podatności, dowód, że podano adres do kontaktu do celów zgłaszania podatności, oraz opis rozwiązań technicznych wybranych na potrzeby bezpiecznej dystrybucji aktualizacji;

   c) niezbędne informacje i specyfikacje dotyczące procesów produkcji i monitorowania produktu z elementami cyfrowymi oraz walidacji tych procesów;

3) ocenę ryzyka w cyberprzestrzeni, na wypadek którego zaprojektowano, opracowano, wyprodukowano, dostarczono i utrzymywano produkt z elementami cyfrowymi, zgodnie z art. 13, w tym w jakim sposób mają zastosowanie zasadnicze wymagania w zakresie cyberbezpieczeństwa określone załączniku I część I;

4) istotne informacje uwzględnione przy określaniu dla produktu z elementami cyfrowymi okresu wsparcia, o którym mowa w art. 13 ust. 8;

5) wykaz norm zharmonizowanych stosowanych w całości lub w części, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, wspólne specyfikacje określone w art. 27 niniejszego rozporządzenia lub europejskie programy certyfikacji cyberbezpieczeństwa przyjęte zgodnie z rozporządzeniem (UE) 2019/881 według art. 27 ust. 8 niniejszego rozporządzenia oraz – jeżeli nie zastosowano takich norm zharmonizowanych, wspólnych specyfikacji lub europejskich systemów certyfikacji cyberbezpieczeństwa – opisy rozwiązań przyjętych w celu spełnienia zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I część I i II, w tym wykaz innych odpowiednich zastosowanych specyfikacji technicznych; w przypadku częściowego zastosowania norm zharmonizowanych, wspólnych specyfikacji lub europejskich programów certyfikacji cyberbezpieczeństwa w dokumentacji technicznej należy określić, które części zastosowano;

6) sprawozdania z prób przeprowadzonych w celu weryfikacji zgodności produktu z elementami cyfrowymi oraz procedur postępowania w przypadku wykrycia podatności z mającymi zastosowanie zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część I i II;

7) kopię deklaracji zgodności UE;

8) w stosownych przypadkach zestawienie podstawowych materiałów do produkcji oprogramowania, na uzasadniony wniosek organu nadzoru rynku, pod warunkiem że jest to niezbędne, aby organ ten mógł sprawdzić zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I.

ZAŁĄCZNIK VIII

PROCEDURY OCENY ZGODNOŚCI

Część I Procedura oceny zgodności opierająca się na kontroli wewnętrznej (zgodnie z modułem A)

1. Kontrola wewnętrzna jest procedurą oceny zgodności, w której producent wypełnia obowiązki określone w pkt 2, 3 i 4 niniejszej części oraz zapewnia i deklaruje na swoją wyłączną odpowiedzialność, że produkt z elementami cyfrowymi spełnia wszystkie zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I część I, a producent spełnia zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I część II.

2. Producent sporządza dokumentację techniczną określoną w załączniku VII.

3. Projektowanie, opracowywanie i produkcja produktów z elementami cyfrowymi oraz postępowanie w przypadku wykrycia podatności

   Producent stosuje wszelkie środki niezbędne, aby projektowanie, opracowywanie, produkcja i procedury postępowania w przypadku wykrycia podatności i ich monitoring zapewniały zgodność produkowanych lub opracowywanych produktów z elementami cyfrowymi i wprowadzonych przez producenta procedur z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część I i II.

4. Oznakowanie zgodności i deklaracja zgodności

   4.1. Producent umieszcza oznakowanie CE na każdym produkcie z elementami cyfrowymi spełniającym mające zastosowanie wymagania określone w niniejszym rozporządzeniu.

   4.2. Producent sporządza pisemną deklarację zgodności UE dla każdego produktu z elementami cyfrowymi zgodnie z art. 28 i przechowuje ją wraz z dokumentacją techniczną do dyspozycji organów krajowych przez okres 10 lat po wprowadzeniu do obrotu danego produktu z elementami cyfrowymi lub przez przewidywany okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy. W deklaracji zgodności UE należy wskazać produkt z elementami cyfrowymi, dla którego ją sporządzono. Kopię deklaracji zgodności UE udostępnia się na żądanie właściwym organom.

5. Upoważnieni przedstawiciele

   Obowiązki producenta określone w pkt 4 mogą być, w jego imieniu i na jego odpowiedzialność, wypełniane przez upoważnionego przedstawiciela, pod warunkiem że zostały dane obowiązki określone w pełnomocnictwie.

Część II Badanie typu UE (zgodnie z modułem B)

1. Badanie typu UE jest elementem procedury oceny zgodności, w której jednostka notyfikowana bada projektowanie i opracowywanie techniczne produktu z elementami cyfrowymi oraz wprowadzone przez producenta procedury postępowania w przypadku wykrycia podatności, a także poświadcza, że produkt z elementami cyfrowymi spełnia zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I część I, a producent spełnia zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I część II.

2. Badanie typu UE polega na ocenie adekwatności projektowania i opracowywania technicznego produktu z elementami cyfrowymi przez zbadanie dokumentacji technicznej i dowodów potwierdzających, o których mowa w pkt 3, oraz zbadanie próbek co najmniej jednej z istotnych części produktu (połączenie typu produkcji i typu projektu).

3. Producent składa wniosek o badanie typu UE w jednej wybranej przez siebie jednostce notyfikowanej.

   Wniosek taki zawiera:

   3.1. nazwę lub imię i nazwisko oraz adres producenta, a jeżeli wniosek składa upoważniony przedstawiciel – również nazwę lub imię i nazwisko oraz adres tego upoważnionego przedstawiciela;

   3.2. pisemną deklarację, że tego samego wniosku nie złożono w żadnej innej jednostce notyfikowanej;

   3.3. dokumentację techniczną, która musi umożliwiać przeprowadzenie oceny zgodności produktu z elementami cyfrowymi z mającymi zastosowanie zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część I oraz oceny wprowadzonych przez producenta procedur postępowania w przypadku wykrycia podatności określonych w załączniku I część II, a także zawiera odpowiednią analizę i ocenę ryzyka; w dokumentacji technicznej należy określić mające zastosowanie wymagania i ująć, w stopniu właściwym dla oceny, projektowanie, produkcję i działanie produktu z elementami cyfrowymi; w stosownych przypadkach dokumentacja techniczna musi zawierać co najmniej elementy określone w załączniku VII;

3.4. dowody potwierdzające adekwatność projektowania technicznego i rozwiązań dotyczących opracowywania oraz procedur postępowania w przypadku wykrycia podatności; w dowodach tych należy wymienić wszelkie wykorzystane dokumenty, zwłaszcza jeśli nie zastosowano w pełni odpowiednich norm zharmonizowanych lub specyfikacji technicznych; w razie potrzeby dowody potwierdzające muszą obejmować wyniki testów przeprowadzonych przez odpowiednie laboratorium producenta lub przez inne laboratorium badawcze w jego imieniu i na jego odpowiedzialność.

4. Jednostka notyfikowana:

4.1. bada dokumentację techniczną i dowody potwierdzające, aby ocenić adekwatność projektowania i opracowywania technicznego produktu z elementami cyfrowymi w odniesieniu do zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I część I oraz wprowadzonych przez producenta procedur postępowania w przypadku wykrycia podatności w odniesieniu do zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I część II;

4.2. sprawdza czy egzemplarze opracowano lub wyprodukowano zgodnie z dokumentacją techniczną, i wskazuje elementy, które zaprojektowano i opracowano zgodnie z mającymi zastosowanie przepisami odpowiednich norm zharmonizowanych lub specyfikacji technicznych, jak również tych elementów, które zaprojektowano i opracowano bez stosowania odpowiednich przepisów tych norm;

4.3. prowadzi odpowiednie badania i testy lub zleca ich przeprowadzenia, aby – w przypadku gdy producent zdecydował się na zastosowanie rozwiązań określonych w odpowiednich normach zharmonizowanych lub specyfikacjach technicznych odnoszących się do wymagań przewidzianych w załączniku I – sprawdzić, czy zastosowano je prawidłowo;

4.4. prowadzi odpowiednie badania i testy lub zleca ich przeprowadzenia, aby – w przypadku gdy nie zastosowano rozwiązań określonych w odpowiednich normach zharmonizowanych lub specyfikacjach technicznych odnoszących się do wymagań przedstawionych w załączniku I – sprawdzić, czy rozwiązania przyjęte przez producenta spełniają odpowiednie zasadnicze wymagania w zakresie cyberbezpieczeństwa;

4.5. uzgadnia z producentem miejsca, w którym zostaną przeprowadzone badania i testy.

5. Jednostka notyfikowana sporządza sprawozdanie z oceny, w którym odnotowuje działania podjęte zgodnie z pkt 4 i ich rezultaty. Bez uszczerbku dla swoich obowiązków wobec organów notyfikujących jednostka notyfikowana udostępnia treść takiego sprawozdania, w całości lub w części, wyłącznie za zgodą producenta.

6. Jeżeli typ oraz procedury postępowania w przypadku wykrycia podatności spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I, jednostka notyfikowana wydaje producentowi certyfikat badania typu UE. Certyfikat musi zawierać imię i nazwisko lub nazwę i adres producenta, wnioski z badań, (ewentualne) warunki jego ważności oraz dane niezbędne do identyfikacji zatwierdzonego typu i procedur postępowania w przypadku wykrycia podatności. Do certyfikatu można dołączyć załącznik lub załączniki.

Certyfikat i załączniki do niego zawierają wszystkie istotne informacje umożliwiające ocenę zgodności wyprodukowanych lub opracowanych produktów z elementami cyfrowymi w odniesieniu do badanego typu i procedur postępowania w przypadku wykrycia podatności oraz kontrolę w trakcie eksploatacji.

Jeżeli typ oraz procedury postępowania w przypadku wykrycia podatności nie spełniają mających zastosowanie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I, jednostka notyfikowana odmawia wydania certyfikatu badania typu UE oraz informuje o tym wnioskodawcę, przedstawiając szczegółowe uzasadnienie odmowy.

7. Jednostka notyfikowana śledzi wszelkie zmiany w powszechnie uznanym stanie wiedzy technicznej wskazujące, że zatwierdzony typ oraz zatwierdzone procedury postępowania w przypadku wykrycia podatności mogą nie spełniać już mających zastosowanie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I, oraz musi ustalić, czy zmiany takie wymagają dalszego badania. Jeżeli tak jest, jednostka notyfikowana musi poinformować o tym producenta.

Producent informuje jednostkę notyfikowaną, która przechowuje dokumentację techniczną dotyczącą certyfikatu badania typu UE, o wszystkich modyfikacjach zatwierdzonego typu i zatwierdzonych procedur postępowania w przypadku wykrycia podatności mogących wpływać na zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I lub warunkami ważności certyfikatu. Takie modyfikacje wymagają dodatkowego zatwierdzenia w formie dodatku do pierwotnego certyfikatu badania typu UE.

8. Jednostka notyfikowana prowadzi audyty okresowe, by zapewnić odpowiednie wdrażanie procesów postępowania w przypadku wykrycia podatności określonych w załączniku I część II.

9. Każda jednostka notyfikowana informuje właściwy organ notyfikujący o certyfikatach badania typu UE i wszelkich dodatkach do nich, które wydała lub cofnęła, oraz, okresowo lub na żądanie, udostępniać właściwemu organowi notyfikującemu wykaz tych certyfikatów i wszelkich dodatków do nich, których wydania odmówiła, które zawiesiła lub objęła innymi ograniczeniami.

   Każda jednostka notyfikowana informuje pozostałe jednostki notyfikowane o certyfikatach badania typu UE i wszelkich dodatkach do nich, których wydania odmówiła, które cofnęła, zawiesiła lub objęła innymi ograniczeniami oraz, na żądanie, o certyfikatach i wszelkich dodatkach do nich, które wydała.

   Komisja, państwa członkowskie i pozostałe jednostki notyfikowane mogą na żądanie otrzymać kopie certyfikatów badania typu UE lub dodatków do nich. Komisja i państwa członkowskie mogą otrzymać na żądanie kopię dokumentacji technicznej oraz wyniki badań przeprowadzonych przez jednostkę notyfikowaną. Jednostka notyfikowana przechowuje kopie certyfikatu badania typu UE, załączników i dodatków do niego, a także dokumentów technicznych, w tym dokumentacji przedłożonej przez producenta, do czasu wygaśnięcia ważności certyfikatu.

10. Producent przechowuje kopie certyfikatu badania typu UE, załączników i dodatków do niego wraz z dokumentacją techniczną do dyspozycji organów krajowych przez okres 10 lat po wprowadzeniu produktu z elementami cyfrowymi do obrotu lub przez okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy.

11. Upoważniony przedstawiciel producenta może złożyć wniosek, o którym mowa w pkt 3, oraz wypełniać obowiązki określone w pkt 7 i 10, pod warunkiem że dane obowiązki zostały określone w upoważnieniu.

Część III Zgodność z typem w oparciu o wewnętrzną kontrolę produkcji (zgodnie z modułem C)

1. Zgodność z typem w oparciu o wewnętrzną kontrolę produkcji to element procedury oceny zgodności, w której producent wypełnia obowiązki określone w pkt 2 i 3 niniejszej części oraz zapewnia i deklaruje, że dane produkty z elementami cyfrowymi są zgodne z typem opisanym w certyfikacie badania typu UE i spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa przewidziane w załączniku I część I, a producent spełnia zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I część II.

2. Produkcja

   Producent stosuje wszelkie niezbędne środki, aby proces produkcji i jego monitorowanie zapewniały zgodność wyprodukowanych produktów z elementami cyfrowymi z zatwierdzonym typem opisanym w certyfikacie badania typu UE i z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa przewidzianymi w załączniku I część I, oraz zapewnia spełnianie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I część II.

3. Oznakowanie zgodności i deklaracja zgodności

   3.1. Producent umieszcza oznakowania CE na każdym egzemplarzu produktu z elementami cyfrowymi zgodnym z typem opisanym w certyfikacie badania typu UE i spełniającym mające zastosowanie wymagania określone w niniejszym rozporządzeniu.

   3.2. Producent sporządza pisemną deklarację zgodności dla modelu produktu z elementami cyfrowymi i przechowuje ją do dyspozycji organów krajowych przez okres 10 lat po wprowadzeniu produktu do obrotu lub przez okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy. W deklaracji zgodności należy wskazać produkt, dla którego została ona sporządzona. Kopię deklaracji zgodności należy na żądanie udostępnić właściwym organom.

4. Upoważniony przedstawiciel

   Obowiązki producenta określone w pkt 3 mogą być, w jego imieniu i na jego odpowiedzialność, wypełniane przez upoważnionego przedstawiciela, pod warunkiem że dane obowiązki zostały określone w pełnomocnictwie.

Część IV Zgodność oparta na pełnym zapewnieniu jakości (zgodnie z modułem H)

1. Zgodność oparta na pełnym zapewnieniu jakości jest procedurą oceny zgodności, w której producent wypełnia obowiązki określone w pkt 2 i 5 niniejszej części oraz zapewnia i deklaruje na swoją wyłączną odpowiedzialność, że dane produkty lub kategorie produktów z elementami cyfrowymi spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w załączniku I część I, a wprowadzone przez producenta procedury postępowania w przypadku wykrycia podatności spełniają zasadnicze wymagania określone w załączniku I część II.

2. Projektowanie, opracowywanie, produkcja i postępowanie w przypadku wykrycia podatności w odniesieniu do produktów z elementami cyfrowymi

Producent ma zatwierdzony system jakości określony w pkt 3 w odniesieniu do projektowania i opracowywania danych produktów z elementami cyfrowymi, inspekcji i testowania produktów końcowych, postępowania w przypadku wykrycia podatności oraz utrzymania wydajności tych produktów przez cały okres wsparcia, a także podlega nadzorowi zgodnie z pkt 4.

3. System jakości

3.1. Producent składa w wybranej przez siebie jednostce notyfikowanej wniosek o ocenę jego systemu jakości dla danych produktów z elementami cyfrowymi.

Wniosek taki zawiera:

a) nazwę lub imię i nazwisko oraz adres producenta, a jeżeli wniosek składa upoważniony przedstawiciel – również nazwę lub imię i nazwisko oraz adres tego upoważnionego przedstawiciela;

b) dokumentację techniczną dla jednego modelu każdej kategorii produktów z elementami cyfrowymi, które mają być produkowane lub opracowywane; w stosownych przypadkach dokumentacja techniczna musi zawierać co najmniej elementy określone w załączniku VII;

c) dokumentację dotyczącą systemu jakości; oraz

d) pisemną deklarację, że tego samego wniosku nie złożono w żadnej innej jednostce notyfikowanej.

3.2. System jakości musi zapewniać zgodność produktów z elementami cyfrowymi z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w załączniku I część I oraz zgodność wprowadzonych przez producenta procedur postępowania w przypadku wykrycia podatności z wymaganiami określonymi w załączniku I część II.

Wszystkie elementy, wymagania i środki przyjęte przez producenta muszą być w systematyczny i uporządkowany sposób udokumentowane w formie pisemnych zaleceń, procedur i instrukcji. Dokumentacja systemu jakości musi umożliwiać spójną interpretację programów, planów, ksiąg i zapisów dotyczących jakości.

Dokumentacja ta zawiera w szczególności stosowny opis:

a) celów jakości i struktury organizacyjnej, obowiązków oraz uprawnień kierownictwa w odniesieniu do projektowania, opracowywania, jakości produktu i postępowania w przypadku wykrycia podatności;

b) specyfikacji technicznych projektowania i opracowywania, w tym norm, które będą stosowane, oraz – jeżeli dane normy zharmonizowane lub specyfikacje techniczne nie będą stosowane w pełni – środków, które zostaną wprowadzone, by zapewnić spełnienie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I część I mających zastosowanie do produktów z elementami cyfrowymi;

c) specyfikacji procedur, w tym norm, które będą stosowane, oraz – jeżeli dane normy zharmonizowane lub specyfikacje techniczne nie będą stosowane w pełni – środków, które zostaną wprowadzone, by zapewnić spełnienie zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w załączniku I część II mających zastosowanie do producenta;

d) kontroli projektowania i opracowywania oraz technik weryfikacji projektowania i opracowywania, procesów i systematycznych działań, które będą podejmowane podczas projektowania i opracowywania produktów z elementami cyfrowymi należących do danej kategorii produktów;

e) odpowiednich technik produkcji, kontroli jakości i zapewnienia jakości, procesów i systematycznych działań, które będą podejmowane;

f) badań i testów, które będą wykonywane przed rozpoczęciem, w trakcie i po zakończeniu produkcji oraz ich częstotliwości;

g) zapisów dotyczących jakości, takich jak sprawozdania z kontroli i dane z badań, dane dotyczące wzorcowania oraz sprawozdania dotyczące kwalifikacji odpowiedniego personelu;

h) środków monitorowania osiągania wymaganej jakości projektowania i produktu oraz skutecznego działania systemu jakości.

3.3. Jednostka notyfikowana ocenia systemu jakości w celu stwierdzenia, czy spełnia on wymagania, o których mowa w pkt 3.2.

Zakłada ona zgodność z tymi wymaganiami w odniesieniu do elementów systemu jakości zgodnych z odpowiednimi specyfikacjami normy krajowej wdrażającej odnośną normę zharmonizowaną lub specyfikację techniczną.

Oprócz doświadczenia w zakresie systemów zarządzania jakością co najmniej jeden członek zespołu audytowego musi mieć doświadczenie z zakresu oceny w dziedzinie danego produktu i danej technologii, a także znać mające zastosowanie wymagania określone w niniejszym rozporządzeniu. Audyt musi obejmować wizytę oceniającą w zakładzie producenta, jeżeli taki zakład istnieje. Zespół audytowy wykonuje przegląd dokumentacji technicznej, o której mowa w pkt 3.1 lit b), by zweryfikować zdolność producenta do identyfikowania mających zastosowanie wymagań określonych w niniejszym rozporządzeniu oraz do prowadzenia badań koniecznych do zapewnienia zgodności produktu z elementami cyfrowymi z tymi wymaganiami.

O decyzji powiadamia się producenta lub jego upoważnionego przedstawiciela.

Powiadomienie takie zawiera wnioski z audytu oraz uzasadnioną decyzję dotyczącą oceny.

3.4. Producent podejmuje się wypełnienia zobowiązań wynikających z zatwierdzonego systemu jakości oraz utrzymania go w taki sposób, aby pozostawał odpowiedni oraz wydajny.

3.5. Producent na bieżąco informuje jednostkę notyfikowaną, która zatwierdziła system jakości, o wszelkich zamierzonych modyfikacjach systemu jakości.

Jednostka notyfikowana ocenia proponowane zmiany oraz decyduje, czy zmodyfikowany system jakości nadal będzie spełniał wymagania, o których mowa w pkt 3.2, lub czy konieczna jest ponowna jego ocena.

Powiadamia ona producenta o swojej decyzji. Powiadomienie takie musi zawierać wnioski z badania oraz uzasadnioną decyzję dotyczącą oceny.

4. Nadzór, za który odpowiedzialna jest jednostka notyfikowana

4.1. Celem nadzoru jest sprawdzenie, czy producent należycie wypełnia obowiązki wynikające z zatwierdzonego systemu jakości.

4.2. Do celów oceny producent umożliwia jednostce notyfikowanej dostęp do miejsc projektowania, opracowywania, produkcji, kontroli, badań i magazynowania oraz przedstawia wszelkie niezbędne informacje, a w szczególności:

a) dokumentację systemu jakości;

b) zapisy dotyczące jakości przewidziane w projektowej części systemu jakości, takie jak wyniki analiz, obliczeń i badań;

c) zapisy dotyczące jakości przewidziane w produkcyjnej części systemu jakości, takie jak sprawozdania z inspekcji, dane uzyskane podczas badań, dane dotyczące wzorcowania i dane dotyczące kwalifikacji odpowiednich pracowników.

4.3. Jednostka notyfikowana ma przeprowadza okresowe audyty, by sprawdzić, czy producent utrzymuje i stosuje system jakości, oraz przekazuje producentowi sprawozdania z audytu.

5. Oznakowanie zgodności i deklaracja zgodności

5.1. Producent umieszcza oznakowania CE oraz, na odpowiedzialność jednostki notyfikowanej, o której mowa w pkt 3.1, jej numer identyfikacyjny na każdym egzemplarzu produktu z elementami cyfrowymi spełniającym wymagania określone w załączniku I część I.

5.2. Producent sporządza pisemną deklarację zgodności dla każdego modelu produktu i przechowuje ją do dyspozycji organów krajowych przez okres 10 lat po wprowadzeniu produktu z elementami cyfrowymi do obrotu lub przez okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy. W deklaracji zgodności należy wskazać produkt, dla którego została ona sporządzona.

Kopię deklaracji zgodności udostępnia się na żądanie właściwym organom.

6. Producent przechowuje do dyspozycji organów krajowych, przez co najmniej 10 lat od wprowadzenia do obrotu produktu z elementami cyfrowymi lub przez okres wsparcia, w zależności od tego, który z tych okresów jest dłuższy, następujące dokumenty:

a) dokumentację techniczną, o której mowa w pkt 3.1;

b) dokumentację dotyczącą systemu jakości, o której mowa w pkt 3.1;

c) zatwierdzoną zmianę, o której mowa w pkt 3.5;

d) decyzje i sprawozdania jednostki notyfikowanej, o których mowa w pkt 3.5 i 4.3.

7. Każda jednostka notyfikowana informuje odpowiednia organy notyfikujące o wydanych lub cofniętych zatwierdzeniach systemów jakości oraz, okresowo lub na żądanie, udostępnia odpowiednim organom notyfikującym wykaz zatwierdzeń systemów jakości, których wydania odmówiono, które zawieszono lub poddano innym ograniczeniom.

Każda jednostka notyfikowana informuje pozostałe jednostki notyfikowane o zatwierdzeniach systemów jakości, których wydania odmówiła, które cofnęła lub zawiesiła oraz, na żądanie, o zatwierdzeniach systemów jakości, które wydała.

8. Upoważniony przedstawiciel

Obowiązki producenta określone w pkt 3.1, 3.5, 5 i 6 może w jego imieniu i na jego odpowiedzialność wypełniać jego upoważniony przedstawiciel, o ile dane obowiązki zostały określone w pełnomocnictwie.

W odniesieniu do niniejszego aktu złożone zostało oświadczenie, które jest dostępne w Dz.U. C, 2024/6786, 20.11.2024, ELI: http://data.europa.eu/eli/C/2024/6786/oj.