Dziennik Urzędowy
Unii Europejskiej

PL
Seria C

C/2026/6013

17.11.2026

KOMUNIKAT KOMISJI

Wytyczne Komisji dotyczące stosowania rozporządzenia (UE) 2024/2847 (aktu o cyberodporności)

(C/2026/6013)

Spis treści

Strona

1. WPROWADZENIE 3
   - 1.1. Akt o cyberodporności 3
   - 1.2. Cel niniejszych wytycznych 3
2. ZAKRES STOSOWANIA 4
   - 2.1. Wprowadzenie do obrotu 4
   - 2.2. Oprogramowanie jako produkt z elementami cyfrowymi 5
   - 2.3. Kod komputerowy 6
   - 2.4. Połączenie sprzętu i oprogramowania tworzące produkt z elementami cyfrowymi 7
   - 2.5. Połączenie danych 8
   - 2.6. Systemy złożone 8
   - 2.7. Produkty z elementami cyfrowymi zaprojektowane przed rozpoczęciem stosowania aktu o cyberodporności 9
3. WOLNE I OTWARTE OPROGRAMOWANIE 11
   - 3.1. Ustalenie, czy dana osoba jest odpowiedzialna za wolne i otwarte oprogramowanie 12
   - 3.2. Ustalenie, czy wolne i otwarte oprogramowanie jest wprowadzane do obrotu w UE 13
     - 3.2.1. Pobieranie opłaty 13
     - 3.2.2. Monetyzacja innych usług lub żądanie przetwarzania danych osobowych 13
     - 3.2.3. Usługi wsparcia 14
     - 3.2.4. Darowizny 15
     - 3.2.5. Finansowanie wolnego i otwartego oprogramowania 15
     - 3.2.6. Podmioty nienastawione na zysk utworzone w celu osiągnięcia celów nienastawionych na zysk. 16
     - 3.2.7. Włączanie komponentów przez innych producentów 16
   - 3.3. Opiekunowie otwartego oprogramowania 16
     - 3.3.1. Stałe wsparcie i zapewnienie opłacalności wolnego i otwartego oprogramowania 17
   - 3.4. Współtwórcy i zastosowania na dalszym etapie łańcucha dostaw 18
   - 3.5. Przykładowe scenariusze 19
4. ISTOTNE MODYFIKACJE I CZĘŚCI ZAMIENNE 21
   - 4.1. Naprawy fizyczne 22
   - 4.2. Części zamienne 23
   - 4.3. Aktualizacje oprogramowania jako istotne modyfikacje 24

4.4. Konsekwencje istotnej modyfikacji 27
4.4.1. Istotne modyfikacje dokonane przez osobę inną niż pierwotny producent 28
4.4.2. Istotne modyfikacje dokonane przez pierwotnego producenta 29
5. OKRES WSPARCIA 29
5.1. Istotne modyfikacje i okres wsparcia 31
6. WAŻNE I KRYTYCZNE PRODUKTY Z ELEMENTAMI CYFROWYMI 32
6.1. Podstawowa funkcjonalność 33
6.2. Ocena zgodności ważnych i krytycznych produktów z elementami cyfrowymi 36
6.3. Konsekwencje dla domniemania zgodności 38
7. OCENA RYZYKA W CYBERPRZESTRZENI I ŁĄCZENIE PRODUKTÓW Z ELEMENTAMI CYFROWYMI Z KOMPONENTAMI 41
7.1. Ocena i zmniejszanie ryzyka w cyberprzestrzeni 41
7.2. Projektowanie, opracowywanie i wytwarzanie produktów z elementami cyfrowymi tak, by zapewniały odpowiedni poziom cyberbezpieczeństwa stosownie do ryzyka 42
7.3. Ocena ryzyka i należyta staranność w odniesieniu do zależności zewnętrznych i włączonych komponentów 42
7.4. Ponowne wykorzystanie ocen ryzyka i dokumentacji zgodności w odniesieniu do rodzin produktów z elementami cyfrowymi 44
8. ZDALNE PRZETWARZANIE DANYCH 44
8.1. Co uznaje się za rozwiązanie w zakresie zdalnego przetwarzania danych w odniesieniu do produktu z elementami cyfrowymi? 45
8.1.1. Pojęcie „na odległość” 46
8.1.2. Czy brak takiego przetwarzania danych spowodowałby, że produkt z elementami cyfrowymi nie będzie mógł wykonywać jednej ze swoich funkcji? 46
8.1.3. Czy oprogramowanie zostało zaprojektowane i opracowane przez producenta lub na jego odpowiedzialność? 47
8.2. Praktyczne i techniczne konsekwencje rozwiązań w zakresie zdalnego przetwarzania danych oraz korzystania z rozwiązań stron trzecich 49
8.3. Przypadki użycia rozwiązań w zakresie zdalnego przetwarzania danych 50
8.3.1. Aplikacja bankowości mobilnej 51
8.3.2. Inteligentny termostat 52
8.3.3. Czytnik książek elektronicznych 53
8.3.4. Robot przemysłowy 53
8.3.5. Sieć komórkowa 53
9. ELEMENTY DODATKOWE 54
9.1. Obowiązki w zakresie zgłaszania 54
9.2. Postępowanie w przypadku wykrycia podatności 56
9.2.1. Zgłaszanie na wyższym szczeblu łańcucha dostaw i udostępnianie poprawek zabezpieczeń 56
9.2.2. Znane podatności nadające się do wykorzystania 57
9.2.3. Skuteczne i regularne testy i przeglądy 58
9.3. Wzajemne powiązania z innymi przepisami 59
9.3.1. Rozporządzenie (UE) 2019/2144 i rozporządzenie (UE) nr 168/2013 59
9.3.2. Ważność certyfikatów badania typu UE (art. 69 ust. 1) 59

1. **WPROWADZENIE**

1.1. **Akt o cyberodporności**

1. 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) ([1]) weszło w życie dnia 10 grudnia 2024 r. Rozporządzenie ma na celu wzmocnienie podejścia UE do cyberbezpieczeństwa, zajęcie się kwestią cyberodporności na poziomie UE i poprawę funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych ram prawnych dotyczących zasadniczych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do wprowadzania produktów z elementami cyfrowymi do obrotu w UE, a także w całym cyklu życia produktu z elementami cyfrowymi.

2. Akt o cyberodporności opiera się na nowych ramach prawnych UE określonych w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającym rozporządzenie (EWG) nr 339/93 oraz decyzji Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylającej decyzję Rady 93/465/EWG ([2]).

3. Nadzór rynku i egzekwowanie przepisów są prowadzone przez krajowe organy nadzoru rynku. Produkty z elementami cyfrowymi, które wchodzą w zakres stosowania aktu o cyberodporności, objęte są rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniającym dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011. Komisja i Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) wspierają podmioty gospodarcze i państwa członkowskie w stosowaniu aktu o cyberodporności.

1.2. **Cel niniejszych wytycznych**

4. W art. 26 ust. 1 aktu o cyberodporności nakłada się na Komisję obowiązek opublikowania wytycznych, aby pomóc podmiotom gospodarczym w stosowaniu rozporządzenia, ze szczególnym naciskiem na ułatwienie zachowania zgodności mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom (MŚP). W art. 26 ust. 2 określono minimalne aspekty, które należy uwzględnić w wytycznych. Należą do nich: (i) zakres aktu o cyberodporności (w szczególności rozwiązania w zakresie zdalnego przetwarzania danych oraz wolnego i otwartego oprogramowania); (ii) pojęcie „okresów wsparcia"; (iii) wzajemne powiązania między aktem o cyberodporności a pozostałymi przepisami prawa UE; oraz (iv) pojęcie „istotnej modyfikacji".

5. 3 grudnia 2025 r. Komisja opublikowała zbiór często zadawanych pytań (FAQ), który ma pomóc podmiotom gospodarczym w przygotowaniu się do wdrożenia aktu o cyberodporności ([3]).

6. Niniejsze wytyczne mają pomóc podmiotom gospodarczym w przestrzeganiu przepisów aktu o cyberodporności oraz wspierać działania organów nadzoru rynku, organów notyfikujących i jednostek notyfikowanych, aby zapewnić zharmonizowane egzekwowanie przepisów aktu o cyberodporności w całej Unii. Niniejsze wytyczne nie mają na celu omówienia całego aktu o cyberodporności, lecz raczej przedstawienie wyjaśnień dotyczących uzasadnienia niektórych kluczowych przepisów i sposobu ich wdrożenia w praktyce. Niniejsze wytyczne dotyczą aktu o cyberodporności i nie mają zastosowania do innych aktów prawnych UE.

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

([2]) W programie prac Komisji na 2026 r. przewidziano przedstawienie „europejskiego aktu o produktach", aktualizującego nowe ramy prawne oraz przepisy dotyczące nadzoru rynku i normalizacji: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52025DC0870.

([3]) FAQ można pobrać za pośrednictwem portalu internetowego Komisji poświęconego wdrażaniu aktu o cyberodporności, ze specjalnej strony internetowej poświęconej FAQ.

7. Podczas przygotowywania niniejszych wytycznych przeprowadzono szeroko zakrojone konsultacje z zainteresowanymi stronami, w tym z grupą ekspertów ds. cyberbezpieczeństwa produktów z elementami cyfrowymi ([4]), oraz w ramach konsultacji publicznych, które odbyły się w dniach 3 marca – 13 kwietnia 2026 r. ([5])

8. Niniejsze wytyczne nie mają charakteru wiążącego dla podmiotów gospodarczych ani innych podmiotów podlegających aktowi o cyberodporności. Autorytatywnej wykładni aktu o cyberodporności może dokonywać wyłącznie Trybunał Sprawiedliwości Unii Europejskiej. Niemniej jednak w niniejszych wytycznych przedstawiono interpretację aktu o cyberodporności przyjętą przez Komisję w celu wsparcia przestrzegania przepisów i przyczynienia się do skutecznego wdrożenia rozporządzenia. Ponadto wytyczne zawierają szereg przykładów ilustrujących stosowanie konkretnych przepisów. Przykłady te nie mają jednak na celu zastąpienia indywidualnej oceny każdego przypadku, która zawsze będzie konieczna do uwzględnienia specyfiki każdej konkretnej sprawy.

9. Zgodnie z art. 26 aktu o cyberodporności Komisja może rozważyć wydanie dalszych wytycznych, w tym wytycznych skierowanych do producentów podlegających aktowi o cyberodporności i innemu unijnemu prawodawstwu harmonizacyjnemu lub innym powiązanym aktom prawnym Unii. Wytyczne te mogą na przykład dotyczyć kwestii wzajemnego oddziaływania między aktem o cyberodporności a rozporządzeniem (UE) 2024/1689 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (akt w sprawie AI) oraz rozporządzeniem (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego (rozporządzenie DORA).

2. **ZAKRES STOSOWANIA**

2.1. **Wprowadzenie do obrotu**

10. Akt o cyberodporności ma zastosowanie do produktów z elementami cyfrowymi, które są udostępniane na rynku UE. Pojęcie „udostępnienia na rynku" zdefiniowano w art. 3 pkt 22 aktu o cyberodporności jako „dostarczenie produktu z elementami cyfrowymi do celów dystrybucji lub używania na rynku Unii w ramach działalności handlowej, odpłatnie lub nieodpłatnie". Zgodnie z art. 3 pkt 21 produkt z elementami cyfrowymi zostaje wprowadzony do obrotu w UE w momencie jego udostępnienia po raz pierwszy.

11. Najnowsze wydanie „Niebieskiego przewodnika – wdrażanie unijnych przepisów dotyczących produktów" opublikowane w 2022 r. (zwanego dalej „Niebieskim przewodnikiem") ([6]) zawiera wytyczne ułatwiające zrozumienie unijnych przepisów dotyczących produktów i ich jednolite stosowanie w różnych sektorowych ramach prawnych dostosowanych do nowych ram prawnych, takich jak akt o cyberodporności. W Niebieskim przewodniku wskazano, że pojęcia „wprowadzania do obrotu" i „udostępniania" należy rozumieć jako odnoszące się „do każdego egzemplarza produktu, a nie typu produktu czy tego, czy został wyprodukowany jako pojedynczy egzemplarz czy w ramach serii" (sekcja 2.3).

12. W przypadku bardziej „tradycyjnych" produktów z elementami cyfrowymi objętych nowymi ramami prawnymi, takich jak sprzęt w postaci maszyn lub sprzęt radiowy z elementami cyfrowymi, pojęcie „wprowadzania do obrotu" jest dobrze ugruntowane, a Niebieski przewodnik zawiera dalsze wytyczne wyjaśniające, kiedy takie produkty uznaje się za wprowadzone do obrotu. „Przykłady podsumowujące" zawarte w sekcji 2.12 Niebieskiego przewodnika zawierają dalsze przykłady ilustrujące pojęcie „wprowadzania do obrotu".

13. Biorąc jednak pod uwagę charakter produktów niematerialnych z elementami cyfrowymi, takich jak samodzielne oprogramowanie, potrzebne są dalsze wytyczne dotyczące tego, kiedy takie produkty uznaje się za wprowadzone do obrotu. Po zakończeniu etapu produkcji oprogramowania i zaoferowaniu produktu z elementami cyfrowymi potencjalnym użytkownikom na rynku UE można uznać, że jego producent wyprodukował wiele kopii tego samego oprogramowania z elementami cyfrowymi i dostarczył je do dystrybucji lub użytkowania. W rzeczywistości, w przeciwieństwie do produktów materialnych z elementami cyfrowymi, samodzielne

([4]) Grupa ekspertów ds. cyberbezpieczeństwa produktów z elementami cyfrowymi w rejestrze grup ekspertów Komisji i podobnych zespołów.
([5]) Konsultacje publiczne w sprawie projektu wytycznych Komisji dotyczących aktu o cyberodporności.
([6]) Zawiadomienie Komisji „Niebieski przewodnik – wdrażanie unijnych przepisów dotyczących produktów 2022" 2022/C 247/01, Dz.U. C 247 z 29.6.2022, s. 1.

oprogramowanie nie podlega ograniczeniom związanym z produkcją fizyczną ani stanem zapasów: każda czynność udostępnienia oprogramowania do pobrania lub dystrybucji skutkuje utworzeniem nowej, identycznej kopii dla użytkownika. O ile ta wersja oprogramowania nie zostanie zmodyfikowana w sposób mający wpływ na zgodność z aktem o cyberodporności, uznaje się, że wprowadzenie do obrotu w UE miało miejsce w momencie pierwszej oferty dystrybucji lub wykorzystania. Możliwość późniejszego pobrania lub dystrybucji tej wersji oprogramowania z elementami cyfrowymi należy zatem uznać za przypadek udostępnienia tego oprogramowania z elementami cyfrowymi ([7]).

14. W związku z tym należy uznać, że samodzielne oprogramowanie z elementami cyfrowymi zostało wprowadzone do obrotu, gdy etap jego produkcji został zakończony, a oprogramowanie to zostało po raz pierwszy dostarczone do dystrybucji lub wykorzystania na rynku UE w ramach działalności handlowej. Należy uznać, że producent wprowadził do obrotu wiele kopii tego samego oprogramowania z elementami cyfrowymi w tym samym czasie. W związku z tym, chociaż wiele kopii tego samego oprogramowania pozostaje odrębnymi produktami z elementami cyfrowymi, uznaje się je za wprowadzone do obrotu w tym samym czasie, niezależnie od tego, kiedy posiadanie każdej pojedynczej kopii lub korzystanie z niej zostaje przeniesione na inną osobę fizyczną lub prawną. Jednocześnie, w przypadku gdy producent udostępnia oprogramowanie w różnych wariantach, które różnią się pod względem zawartych w nim komponentów, konfiguracji lub aktywowanych funkcji (na przykład buduje oprogramowanie dla różnych systemów operacyjnych lub łączy w pakiety o różnych zestawach funkcji), wariantów tych nie można uznać za wielokrotne kopie tego samego oprogramowania z elementami cyfrowymi. W związku z tym do celów wprowadzania do obrotu należy je traktować jako odrębne produkty z elementami cyfrowymi.

Przykład 1: W dniu 1 stycznia 2028 r. firma A dostarcza po raz pierwszy do dystrybucji za pośrednictwem swojej strony internetowej wersję 1.0.0 swojego oprogramowania X. W tym samym dniu klient 1 kupuje egzemplarz oprogramowania X w wersji 1.0.0. W dniu 15 stycznia 2028 r. klient 2 kupuje egzemplarz oprogramowania X w wersji 1.0.0. Oba egzemplarze oprogramowania X w wersji 1.0.0 zostały wprowadzone do obrotu w dniu 1 stycznia 2028 r.

15. Biorąc pod uwagę iteracyjny charakter opracowywania oprogramowania, należy doprecyzować, że kolejne wersje oprogramowania z elementami cyfrowymi uznaje się za nowo wprowadzone do obrotu, jeżeli wersje te kwalifikują się jako „istotna modyfikacja" oprogramowania z elementami cyfrowymi już wprowadzonego do obrotu, jak wskazano w motywie 41 aktu o cyberodporności. Wersje, które nie kwalifikują się jako istotne modyfikacje, nie wymagają od producenta przeprowadzenia nowej procedury oceny zgodności, a zatem nie zmieniają daty wprowadzenia tego oprogramowania do obrotu. Więcej wskazówek dotyczących pojęcia istotnych modyfikacji można znaleźć w sekcji *4 Istotne modyfikacje*.

Przykład 2: W dniu 1 stycznia 2028 r. firma A po raz pierwszy udostępnia do dystrybucji za pośrednictwem swojej strony internetowej wersję 1.0.0 oprogramowania X. W tym samym dniu klient 1 kupuje egzemplarz oprogramowania X w wersji 1.0.0. W dniu 15 stycznia 2028 r. firma A wydaje zaktualizowaną wersję 1.0.1 oprogramowania X, która nie stanowi istotnej modyfikacji. W dniu 30 stycznia 2028 r. klient 2 kupuje egzemplarz oprogramowania X w wersji 1.0.1. Oba egzemplarze oprogramowania X – w wersji 1.0.0 i 1.0.1 – uznaje się za wprowadzone do obrotu w dniu 1 stycznia 2028 r.

16. Wytyczne określone w pkt 13, 14 i 15 mają zastosowanie wyłącznie w przypadku, gdy produkt z elementami cyfrowymi stanowi samodzielne oprogramowanie. Nie ma to miejsca na przykład w przypadku, gdy oprogramowanie jest połączone ze sprzętem, jak omówiono w sekcji *2.4 Połączenie sprzętu i oprogramowania tworzące produkt z elementami cyfrowymi*.

2.2. **Oprogramowanie jako produkt z elementami cyfrowymi**

17. W art. 3 pkt 1 aktu o cyberodporności produkt z elementami cyfrowymi zdefiniowano jako „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". Takie produkty z elementami cyfrowymi wchodzą w zakres stosowania aktu o cyberodporności, jeżeli ich przeznaczenie lub racjonalnie przewidywalne wykorzystanie obejmuje bezpośrednie lub pośrednie logiczne lub fizyczne połączenie danych z urządzeniem lub siecią.

([7]) Zgodnie z art. 13 ust. 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.

18. Akt o cyberodporności może zatem obejmować szereg produktów z elementami cyfrowymi, w tym: (i) samodzielne oprogramowanie, takie jak aplikacje i programy komputerowe, dystrybuowane w formie cyfrowej lub fizycznej; (ii) sprzęt z wbudowanym oprogramowaniem (np. urządzenia internetu rzeczy, laptopy, tablety); (iii) samodzielny sprzęt (np. układy scalone, płyty główne); oraz (iv) dowolne kombinacje sprzętu komputerowego i oprogramowania dostarczanych oddzielnie, ale przeznaczonych do wspólnego działania.

19. Samodzielne oprogramowanie wchodzi zatem w zakres stosowania aktu o cyberodporności, jeżeli jest wprowadzane do obrotu jako produkt z elementami cyfrowymi. Pomocne jest rozróżnienie między oprogramowaniem z elementami cyfrowymi, które podlega aktowi o cyberodporności, a zdalnym świadczeniem usług, które nie wchodzi w zakres stosowania aktu o cyberodporności.

20. Aby oprogramowanie wchodziło w zakres stosowania aktu o cyberodporności, oprogramowanie z elementami cyfrowymi musi zostać dostarczone użytkownikowi, otrzymane przez tego użytkownika i uruchomione w elektronicznym systemie informacyjnym lub jako jego część po stronie użytkownika. Oprogramowanie, które jest pobierane, instalowane lub w inny sposób dostarczane użytkownikowi i które działa w elektronicznym systemie informacyjnym użytkownika, spełnia te kryteria, w tym na przykład gdy ma formę rozszerzenia przeglądarki lub aplikacji opracowanej przy użyciu technologii sieciowych, ale dostarczonej do działania lokalnego.

21. Natomiast oprogramowanie, które wykonuje się zdalnie i do którego użytkownik ma jedynie dostęp, nie stanowi – wyłącznie na tej podstawie – produktu z elementami cyfrowymi. W motywach 11 i 12 aktu o cyberodporności dokonano bowiem tego rozróżnienia, wyjaśniając, że przetwarzanie lub przechowywanie na odległość podlega aktowi o cyberodporności jedynie w zakresie, w jakim jest to niezbędne do wykonywania przez produkt z elementami cyfrowymi jego funkcji (tj. poprzez pojęcie zdalnego przetwarzania danych zdefiniowane w art. 3 pkt 2), a nie samo w sobie jako produkt z elementami cyfrowymi. Ma to zazwyczaj miejsce w przypadku aplikacji internetowych, w tym progresywnych aplikacji internetowych, do których dostęp uzyskuje się wyłącznie za pośrednictwem przeglądarki internetowej. To samo dotyczy stron internetowych: chociaż strony internetowe mogą, w ograniczonym zakresie, technicznie działać i być uruchamiane na urządzeniu użytkownika, z motywu 12 aktu o cyberodporności wynika, że same strony internetowe nie są uznawane za produkty z elementami cyfrowymi i są objęte zakresem aktu o cyberodporności tylko wtedy, gdy obsługują funkcjonalność produktu z elementami cyfrowymi, tj. w zakresie, w jakim kwalifikują się jako zdalne przetwarzanie danych (jak wyjaśniono bardziej szczegółowo w sekcji *8* i w szczególności *8.1.2 Czy brak takiego przetwarzania danych spowodowałby, że produkt z elementami cyfrowymi nie będzie mógł wykonywać jednej ze swoich funkcji?*).

Przykład 3: Aplikacja mobilna, którą użytkownik pobiera ze sklepu z aplikacjami i instaluje na smartfonie, jest dostarczana użytkownikowi i uruchamiana na urządzeniu użytkownika, a zatem stanowi produkt z elementami cyfrowymi. Jeżeli jest on wprowadzany do obrotu w ramach działalności handlowej, może wchodzić w zakres stosowania aktu o cyberodporności.

Przykład 4: Aplikacja dla komputerów stacjonarnych zbudowana z wykorzystaniem technologii internetowych, ale w pakiecie przeznaczonym do lokalnej instalacji, jest dostarczana użytkownikowi i działa na jego urządzeniu, a zatem stanowi produkt z elementami cyfrowymi. Jeżeli jest on wprowadzany do obrotu w ramach działalności handlowej, może wchodzić w zakres stosowania aktu o cyberodporności.

Przykład 5: Aplikacja internetowa, do której użytkownik ma dostęp wyłącznie za pośrednictwem przeglądarki internetowej, nie jest produktem z elementami cyfrowymi. O ile nie obsługuje funkcjonalności produktu z elementami cyfrowymi, nie wchodzi w zakres aktu o cyberodporności. Natomiast aplikacja dostarczana użytkownikowi jako lokalnie zainstalowany klient, która uruchamia się na urządzeniu użytkownika, jest produktem z elementami cyfrowymi. Jeżeli jest on wprowadzany do obrotu w ramach działalności handlowej, może wchodzić w zakres stosowania aktu o cyberodporności.

Jeżeli klient ten, w celu realizacji jednej lub kilku swoich funkcji, wykorzystuje przetwarzanie danych na odległość spełniające definicję zdalnego przetwarzania danych, to owo przetwarzanie danych na odległość stanowi również część produktu z elementami cyfrowymi.

Przykład 6: Strona internetowa, która jedynie przedstawia informacje odwiedzającym i nie obsługuje funkcjonalności produktu z elementami cyfrowymi, sama w sobie nie jest produktem z elementami cyfrowymi. Nie wchodzi ona zatem w zakres stosowania aktu o cyberodporności.

2.3. **Kod komputerowy**

22. Warto również wyjaśnić, czy kod źródłowy może stanowić oprogramowanie z elementami cyfrowymi. W akcie o cyberodporności zdefiniowano oprogramowanie jako „część elektronicznego systemu informacyjnego, która składa się z kodu komputerowego" (art. 3 pkt 4). Kod komputerowy może mieć formę (i) kodu maszynowego, który jest zbiorem instrukcji wykonywanych bezpośrednio przez procesor komputera, zapisanych w formacie binarnym; lub (ii) kodu źródłowego, tj. zestawu instrukcji i deklaracji napisanych w języku programowania, które muszą zostać skompilowane lub zinterpretowane, aby mogły zostać wykonane przez komputer. Definicja oprogramowania określona w akcie o cyberodporności obejmuje oba te rodzaje.

23. Odrębną kwestią jest to, czy dane udostępnienie kodu komputerowego jest równoznaczne z wprowadzeniem produktu z elementami cyfrowymi do obrotu w UE, co wymaga udostępnienia w ramach działalności handlowej. Często może tak nie być w przypadku kodu źródłowego. Na przykład osoba fizyczna lub prawna, która udostępnia wolny i otwarty kod komputerowy w publicznie dostępnych repozytoriach, zasadniczo nie jest uznawana za wprowadzającą ten kod do obrotu w UE do celów aktu o cyberodporności (jak omówiono bardziej szczegółowo w sekcji *3 Wolne i otwarte oprogramowanie*). Nieukończony kod udostępniany na etapie projektowania i opracowywania produktu z elementami cyfrowymi (np. do testowania lub przeglądu) również nie jest uznawany za wprowadzony do obrotu w rozumieniu aktu o cyberodporności, ponieważ etap jego produkcji nie został zakończony. Podobnie do celów aktu o cyberodporności za wprowadzenie do obrotu nie uznaje się również próbki kodu lub kodu demonstracyjnego dostarczonego w ramach materiałów instruktażowych lub szkoleniowych ([8]).

24. Z drugiej strony, w przypadku gdy producent dostarcza swoim klientom kod komputerowy jako produkt z elementami cyfrowymi, kod ten uznaje się za wprowadzony do obrotu, niezależnie od tego, czy jest to kod maszynowy, czy kod źródłowy ([9]).

Przykład 7: Firma A udziela firmie B licencji na kod źródłowy dostosowywanej do potrzeb platformy wewnętrznej i udostępnia ten kod źródłowy w postaci pliku tekstowego. Nawet jeśli ten kod źródłowy wymaga dalszego dostosowania i kompilacji przez firmę B przed jego użyciem, firma A wprowadza ten kod źródłowy do obrotu, a zatem podlega przepisom aktu o cyberodporności. Firma A nie ponosi odpowiedzialności za zgodność z przepisami aktu o cyberodporności w odniesieniu do późniejszych dostosowań i kompilacji tego kodu przez firmę B.

2.4. **Połączenie sprzętu i oprogramowania tworzące produkt z elementami cyfrowymi**

25. O tym, czy oprogramowanie stanowi część produktu z elementami cyfrowymi, należy decydować nie na podstawie sposobu lub momentu dostarczenia tego oprogramowania użytkownikowi, ale na podstawie tego, czy w świetle przeznaczenia produktu i jego racjonalnie przewidywalnego wykorzystania oprogramowanie to jest niezbędne do tego, aby produkt z elementami cyfrowymi spełniał swoje zamierzone funkcje. W przypadku gdy sprzęt komputerowy z elementami cyfrowymi jest zaprojektowany do współpracy z określonym oprogramowaniem dostarczanym przez tego samego producenta w celu wykonywania funkcji produktu, dany sprzęt i oprogramowanie razem stanowią produkt z elementami cyfrowymi. Oprogramowanie, które jest niezbędne do obsługi, konfigurowania, kontrolowania lub użytkowania produktu z elementami cyfrowymi zgodnie z jego przeznaczeniem, jest zatem częścią produktu z elementami cyfrowymi, nawet jeżeli uzyskuje się je za pośrednictwem odrębnego kanału (np. sklepu z aplikacjami, linku do pobierania danych lub innego kanału cyfrowego po wprowadzeniu do obrotu sprzętu komputerowego z elementami cyfrowymi). Jego wprowadzenie do obrotu następuje zatem w tym samym momencie co wprowadzenie do obrotu jednostek sprzętu komputerowego z elementami cyfrowymi.

Przykład 8: Drukarka sieciowa jest wprowadzana do obrotu jako sprzęt komputerowy z elementami cyfrowymi, natomiast sterowniki programowe wymagane do wysyłania zadań drukowania, konfigurowania urządzenia i zarządzania jego działaniem są udostępniane do pobrania ze strony internetowej producenta. Chociaż drukarka i sterowniki są dostarczane różnymi kanałami, razem stanowią jeden produkt z elementami cyfrowymi, ponieważ drukarka nie może spełniać swojego przeznaczenia bez sterowników.

Przykład 9: Wprowadza się do obrotu urządzenie ubieralne, które służy do monitorowania aktywności fizycznej, w celu pomiaru tętna i aktywności użytkownika, natomiast do wyświetlania pomiarów, historii oraz konfiguracji urządzenia niezbędna jest aplikacja na smartfony udostępniona przez producenta. Chociaż aplikację pobiera się oddzielnie przez sklep z aplikacjami, urządzenie ubieralne wraz z aplikacją razem stanowią jeden produkt z elementami cyfrowymi, ponieważ są zaprojektowane i przeznaczone do wspólnego działania w celu zapewnienia funkcjonalności produktu z elementami cyfrowymi.

([8]) Należy również przypomnieć, że art. 4 ust. 3 umożliwia producentom udostępnianie na rynku nieukończonego oprogramowania, które nie jest zgodne z rozporządzeniem, takiego jak wersje alfa, wersje beta lub kandydaci do wydania (ang. *release candidate*), pod warunkiem że nieukończone oprogramowanie zostanie udostępnione wyłącznie na okres niezbędny do jego przetestowania i uzyskania informacji zwrotnych.

([9]) Z drugiej strony należy zauważyć, że do celów prawa dotyczącego odpowiedzialności za produkt sam kod komputerowy nie stanowi produktu, a zatem producenci wprowadzający taki kod do obrotu nie mogą zostać pociągnięci do odpowiedzialności na podstawie dyrektywy (UE) 2024/2853 (dyrektywa w sprawie odpowiedzialności za produkty). W motywie 13 tej dyrektywy stwierdza się, że „[i]nformacji nie uznaje się jednak za produkt, a zatem przepisy dotyczące odpowiedzialności za produkt nie powinny mieć zastosowania do treści plików cyfrowych, takich jak pliki multimedialne, książki elektroniczne lub sam kod źródłowy oprogramowania". Nie wyklucza to możliwości pociągnięcia producentów do odpowiedzialności na mocy krajowego prawa deliktów.

2.5. **Połączenie danych**

26. Art. 2 ust. 1 stanowi, że akt o cyberodporności „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". Zakres stosowania aktu o cyberodporności nie wynika zatem z samej obecności elementów elektronicznych, lecz ze zdolności produktu z elementami cyfrowymi do wymiany informacji cyfrowych.

27. Chociaż pojęcia „połączenie logiczne" i „połączenie fizyczne" zdefiniowano w art. 3, w akcie o cyberodporności nie zdefiniowano pojęć „połączenie danych" ani „dane cyfrowe". Warto zatem przedstawić wykładnię tego, czym jest połączenie danych, aby wyjaśnić granicę zakresu stosowania aktu o cyberodporności. Granica ta jest szczególnie ważna dla odróżnienia produktów z elementami cyfrowymi, które wykorzystują jedynie sygnały elektryczne, od produktów, które uczestniczą w komunikacji cyfrowej i w związku z tym są narażone na ryzyko w cyberprzestrzeni.

28. W najprostszym ujęciu połączenie danych polega na przesyłaniu informacji w postaci binarnej, tj. jako sekwencji zer i jedynek. Samo włączanie i wyłączanie wyjścia (tj. 0/1) nie stanowi jeszcze połączenia danych, jeżeli stany te nie mają na celu reprezentowania danych lub nie są odczytywane przez wejście cyfrowe. Aby połączenie danych mogło mieć miejsce, stany binarne muszą być celowo zakodowane jako informacja przez źródło i musi istnieć możliwość ich dekodowania jako informacji w miejscu docelowym. Innymi słowy, musi istnieć nadawca, który celowo generuje symbole cyfrowe zgodnie z określonym schematem, oraz odbiorca zdolny do interpretowania tych symboli jako danych. W przypadku gdy sygnały elektryczne lub elektroniczne są wykorzystywane wyłącznie do uruchamiania lub zasilania danej funkcji, bez przekazywania informacji kodowanych cyfrowo, nie istnieje żadne połączenie danych w rozumieniu aktu o cyberodporności, w związku z czym produkt z elementami cyfrowymi nie wchodzi w zakres art. 2 ust. 1.

2.6. **Systemy złożone**

29. Produkty z elementami cyfrowymi objęte zakresem aktu o cyberodporności mogą składać się nie tylko z pojedynczych urządzeń lub komponentów oprogramowania, ale również ze złożonych systemów, w tym systemów składających się z wielu elementów sprzętu i oprogramowania, które działają razem w celu realizacji określonej funkcji. W przypadku gdy taki system jest wprowadzany do obrotu jako pojedynczy produkt z elementami cyfrowymi, stanowi on produkt z elementami cyfrowymi w rozumieniu aktu o cyberodporności.

30. Takie złożone systemy często charakteryzują się długimi cyklami projektowania i opracowywania z umowami zawartymi przed rozpoczęciem stosowania aktu o cyberodporności, a także długim okresem eksploatacji oraz wysokim stopniem złożoności technicznej i organizacyjnej. Systemy takie, które mają zostać wprowadzone do obrotu po rozpoczęciu stosowania aktu o cyberodporności, mogą wykorzystywać komponenty wprowadzone do obrotu przed rozpoczęciem stosowania aktu o cyberodporności, sprawdzone architektury lub powszechnie stosowane normy interoperacyjności, w tym normy, o których mowa w innych aktach prawnych UE lub ramach sektorowych. W rezultacie niektóre właściwości techniczne tych systemów mogą być trudne do zmodyfikowania lub modyfikacja ta musiałaby być nieproporcjonalna, bez wpływania jednocześnie na ich przeznaczenie, bezpieczeństwo, niezawodność lub interoperacyjność z istniejącą infrastrukturą.

31. Właściwości te same w sobie nie wykluczają złożonych systemów z zakresu stosowania aktu o cyberodporności. Ilustrują one raczej zastosowanie określonego w akcie podejścia opartego na analizie ryzyka, które umożliwia wykazanie zgodności na różne sposoby w zależności od właściwości i ograniczeń produktu z elementami cyfrowymi, zgodnie z art. 13 ust. 3 aktu o cyberodporności. Właściwości te stanowią część przeznaczenia i kontekstu operacyjnego tych systemów, a zatem są istotne przy ocenie zgodności z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa („zasadnicze wymagania"). W szczególności w motywie 55 wyraźnie przyznano, że niektóre zasadnicze wymagania mogą nie być w pełni zgodne z charakterem danego produktu z elementami cyfrowymi. Taka sytuacja może na przykład zaistnieć w przypadku, gdy zgodność podważyłaby obowiązkowe wymogi dotyczące interoperacyjności lub prawidłowe funkcjonowanie systemu.

32. W związku z tym producenci są zobowiązani do przeciwdziałania ryzyku w cyberprzestrzeni na podstawie oceny ryzyka w cyberprzestrzeni, o której mowa w art. 13 ust. 2. Jak wyjaśniono również w motywie 55, w niektórych przypadkach określone zasadnicze wymagania nie mają zastosowania lub nie mogą zostać spełnione poprzez

wdrożenie najnowocześniejszych środków bezpieczeństwa, na przykład ze względu na przeznaczenie systemu, które wymaga, aby produkt z elementami cyfrowymi współdziałał z istniejącymi zależnościami lub spełniał określone wymagania w zakresie interoperacyjności. W takich przypadkach producenci powinni zidentyfikować i udokumentować te szczególne ograniczenia, ocenić związane z nimi ryzyko oraz wdrożyć odpowiednie alternatywne lub kompensacyjne środki ograniczające ryzyko, tak aby nie osłabiać bezpieczeństwa produktu z elementami cyfrowymi. W tym celu zarówno dokumentacja techniczna, o której mowa w art. 31, jak i informacje i instrukcje dla użytkownika, o których mowa w załączniku II, odgrywają kluczową rolę w przejrzystym opisaniu zidentyfikowanych ograniczeń, związanego z nimi ryzyka w cyberprzestrzeni oraz wdrożonych środków ograniczających ryzyko. Zgodnie z obowiązkiem aktualizacji oceny ryzyka w okresie wsparcia producenci powinni również okresowo ponownie oceniać, czy takie ograniczenia nadal istnieją. W przypadku gdy takie ograniczenia można z czasem znieść lub zmniejszyć, producenci powinni odpowiednio zaktualizować produkt z elementami cyfrowymi, tak aby mógł on osiągnąć odpowiedni poziom cyberbezpieczeństwa ([10]).

Przykład 10: Producent wprowadza do obrotu produkt z elementami cyfrowymi, który komunikuje się z systemami zewnętrznymi za pomocą protokołu sieciowego. W ramach stosowania zasadniczych wymagań producent stwierdza na podstawie oceny ryzyka w cyberprzestrzeni, że zastosowanie bezpiecznego protokołu komunikacyjnego jest niezbędne do zapewnienia poufności i integralności danych wymienianych przez produkt z elementami cyfrowymi.

Jego przeznaczenie obejmuje jednak interoperacyjność z istniejącymi systemami, które obsługują jedynie starszy lub mniej bezpieczny protokół. W takich przypadkach producent może wdrożyć ten protokół, jeżeli jest to konieczne do osiągnięcia interoperacyjności, pod warunkiem że związane z tym ryzyko w cyberprzestrzeni zostanie zidentyfikowane i ograniczone za pomocą innych środków.

Jeżeli jest to technicznie wykonalne, aby produkt z elementami cyfrowymi obsługiwał zarówno protokół bezpieczny, jak i protokół mniej bezpieczny, oczekuje się, że producent wdroży protokół bezpieczny i włączy jego domyślne stosowanie. Mniej bezpieczny protokół byłby dozwolony tylko wtedy, gdy jest to wymagane do celów interoperacyjności.

Przykład 11: Producent systemu automatyki przemysłowej nabywa pewną liczbę mikrokontrolerów przed rozpoczęciem stosowania aktu o cyberodporności. Producent przeprowadza ocenę ryzyka w cyberprzestrzeni w odniesieniu do swojego systemu automatyki przemysłowej, który ma zostać wprowadzony do obrotu po rozpoczęciu stosowania aktu o cyberodporności. Na podstawie tej oceny ryzyka w cyberprzestrzeni producent nie identyfikuje konkretnego ryzyka w cyberprzestrzeni związanego ze stosowaniem jednego z tych mikrokontrolerów. Producent włącza go do swojego systemu automatyki przemysłowej i zapewnia, aby produkt z elementami cyfrowymi jako całość (system automatyki przemysłowej) spełniał zasadnicze wymagania.

2.7. **Produkty z elementami cyfrowymi zaprojektowane przed rozpoczęciem stosowania aktu o cyberodporności**

33. W niektórych przypadkach producent będzie wprowadzał do obrotu, po rozpoczęciu stosowania aktu o cyberodporności w dniu 11 grudnia 2027 r., egzemplarze produktu z elementami cyfrowymi wyprodukowane zgodnie z typem lub modelem zaprojektowanym i opracowanym przed datą rozpoczęcia stosowania aktu o cyberodporności. W takich przypadkach zgodność z tym rozporządzeniem niekoniecznie wymaga przeprojektowania tych egzemplarzy produktu z elementami cyfrowymi. Producent jest zobowiązany do przeprowadzenia oceny ryzyka w cyberprzestrzeni zgodnie z art. 13 ust. 2 aktu o cyberodporności w celu ustalenia, na podstawie przeznaczenia i racjonalnie przewidywalnego wykorzystania produktu z elementami cyfrowymi, które z zasadniczych wymagań określonych w załączniku I część I mają zastosowanie do tego produktu z elementami cyfrowymi oraz w jaki sposób wymagania te są wdrażane.

34. W przypadku gdy wynik tej oceny ryzyka wykaże, że produkt z elementami cyfrowymi zawiera już odpowiednie i skuteczne środki bezpieczeństwa eliminujące odpowiednie ryzyko, producent może oprzeć się na tych istniejących środkach w celu wykazania zgodności z aktem o cyberodporności. Akt o cyberodporności sam w sobie nie nakłada obowiązku wprowadzenia nowych zabezpieczeń ani przeprojektowania produktu z elementami cyfrowymi, jeżeli nie jest to konieczne do wyeliminowania zidentyfikowanego ryzyka.

([10]) Należy zauważyć, że uwagi zawarte w niniejszym punkcie mogą mieć zastosowanie, stosownie do przypadku, do wszystkich produktów z elementami cyfrowymi objętych zakresem aktu o cyberodporności, a nie tylko do „złożonych systemów".

35. Niemniej jednak producent nadal podlega obowiązkom określonym w akcie o cyberodporności. Obejmują one upewnienie się przed wprowadzeniem produktu z elementami cyfrowymi do obrotu, że przeprowadzono mającą zastosowanie procedurę oceny zgodności, sporządzono deklarację zgodności UE i umieszczono oznakowanie CE. Konieczność spełnienia tych wymogów nie zależy od tego, czy projekt produktu z elementami cyfrowymi wymagał modyfikacji w wyniku oceny ryzyka. W przypadku produktów z elementami cyfrowymi zaprojektowanych przed datą rozpoczęcia stosowania aktu o cyberodporności, ale wprowadzonych do obrotu po tej dacie, jeżeli producent nie jest w stanie wykazać, w jaki sposób uwzględniono ocenę ryzyka na etapie projektowania i opracowywania produktu z elementami cyfrowymi, obowiązek określony w art. 13 ust. 2 należy rozumieć jako zobowiązanie producentów do przeprowadzenia oceny ryzyka w cyberprzestrzeni i wykazania na tej podstawie, że produkt z elementami cyfrowymi obejmuje odpowiednie środki bezpieczeństwa mające na celu zminimalizowanie ryzyka w cyberprzestrzeni, zapobieganie incydentom i zminimalizowanie ich wpływu, w tym w odniesieniu do zdrowia i bezpieczeństwa użytkowników.

36. W związku z tym produkty z elementami cyfrowymi zaprojektowane przed rozpoczęciem stosowania aktu o cyberodporności mogą być wprowadzane do obrotu na podstawie aktu o cyberodporności bez konieczności ich przeprojektowywania, pod warunkiem że producent może wykazać w drodze oceny ryzyka w cyberprzestrzeni i dokumentacji technicznej, że produkt z elementami cyfrowymi osiąga odpowiedni poziom cyberbezpieczeństwa w świetle jego przeznaczenia i racjonalnie przewidywalnego wykorzystania oraz spełnia zasadnicze wymagania w zakresie cyberbezpieczeństwa.

37. Ponadto warto wyjaśnić kwestię stosowania obowiązków w zakresie oceny zgodności w odniesieniu do producentów produktów z elementami cyfrowymi, które są wprowadzane do obrotu po rozpoczęciu stosowania aktu o cyberodporności, ale produkowane zgodnie z typem lub modelem zaprojektowanym i opracowanym przed tą datą. Zgodnie z art. 13 ust. 12 producent jest zobowiązany do wykazania za pomocą odpowiedniej procedury oceny zgodności, że jego produkt z elementami cyfrowymi jest zgodny z mającymi zastosowanie zasadniczymi wymaganiami, oraz do włączenia dowodów w tym zakresie do dokumentacji technicznej produktu (załącznik VII pkt 6).

38. Stosowanie tych wymagań należy jednak interpretować w świetle oceny ryzyka w cyberprzestrzeni i profilu ryzyka w cyberprzestrzeni produktu z elementami cyfrowymi. W szczególności w przypadku produktów z elementami cyfrowymi zaprojektowanych przed datą rozpoczęcia stosowania aktu o cyberodporności (lecz wprowadzonych do obrotu po tej dacie) i podlegających procedurom oceny zgodności określonym w art. 32 ust. 1, jeżeli ocena ryzyka wykaże, że produkt z elementami cyfrowymi zawiera już odpowiednie i skuteczne środki bezpieczeństwa eliminujące ryzyko związane z tym produktem, obowiązku przedstawienia dowodów w ramach procedury oceny zgodności nie należy rozumieć jako wymogu przedstawienia przez producenta wyników badań obejmujących pierwotne etapy projektowania i opracowywania takich produktów z elementami cyfrowymi. Nie byłoby to konieczne, ponieważ nie przyczyniłoby się do zwiększenia bezpieczeństwa samego produktu z elementami cyfrowymi. W przypadku gdy badania mogą być jednak konieczne, od producentów nie oczekuje się przedstawienia dowodów potwierdzających badania przeprowadzone na wszystkich wariantach produktu, ale mogą oni grupować takie badania w ramach rodzin produktów z elementami cyfrowymi, co omówiono bardziej szczegółowo w sekcji *7.4 Ponowne wykorzystanie ocen ryzyka i dokumentacji zgodności w odniesieniu do rodzin produktów z elementami cyfrowymi*.

39. Niemniej jednak producent powinien przedstawić dowody potwierdzające, w jaki sposób przestrzega określonych w załączniku I część II procedur postępowania w przypadku wykrycia podatności, powinien aktualizować swoją ocenę ryzyka zgodnie z art. 13 ust. 3, a także wypełniać wszystkie inne obowiązki określone w akcie o cyberodporności, w tym poprzez dostarczanie użytkownikom informacji i instrukcji zgodnie z art. 13 ust. 18.

Przykład 12: Producent wprowadza do obrotu mikrokontroler, który został zaprojektowany i opracowany przed datą rozpoczęcia stosowania aktu o cyberodporności. Mikrokontroler ten jest przeznaczony do wbudowania w szereg produktów elektronicznych z elementami cyfrowymi, w tym produktów z elementami cyfrowymi wyposażonymi w funkcje łączności.

Przed wprowadzeniem do obrotu nowych egzemplarzy mikrokontrolera po rozpoczęciu stosowania aktu o cyberodporności producent przeprowadza ocenę ryzyka w cyberprzestrzeni zgodnie z art. 13 ust. 2. Na podstawie przeznaczenia mikrokontrolera i jego racjonalnie przewidywalnego wykorzystania producent identyfikuje istotne ryzyko w cyberprzestrzeni, takie jak nieuprawniony dostęp, manipulacja oprogramowaniem lub danymi oraz niewłaściwe wykorzystanie dostępnych interfejsów.

Wynik oceny ryzyka pokazuje, że mikrokontroler, zgodnie z pierwotnym projektem, już uwzględnia odpowiednie i skuteczne środki bezpieczeństwa przeciwdziałające zidentyfikowanemu ryzyku. Producent stwierdza zatem, że produkt z elementami cyfrowymi spełnia odpowiednie zasadnicze wymagania określone w załączniku I część I i że nie jest konieczna zmiana projektu ani wprowadzenie dodatkowych funkcji bezpieczeństwa.

W przypadku gdy nie jest możliwe wykazanie, w jaki sposób ocenę ryzyka w cyberprzestrzeni uwzględniono na początkowym etapie projektowania i opracowywania, producent dokumentuje aktualną ocenę ryzyka w cyberprzestrzeni i wyjaśnia, w jaki sposób istniejący projekt i środki ograniczają zidentyfikowane ryzyko. Producent nie jest zobowiązany do odtworzenia historycznej dokumentacji projektowej ani testowej, ponieważ nie przyczyniłoby się to do zwiększenia cyberbezpieczeństwa produktu z elementami cyfrowymi. W przypadku gdy kilka wariantów mikrokontrolera opiera się na tym samym projekcie i ma ten sam profil ryzyka w cyberprzestrzeni, producent może również opierać się na reprezentatywnych dowodach obejmujących odpowiednią rodzinę produktów.

Producent zapewnia również zgodność z wymaganiami dotyczącymi postępowania w przypadku wykrycia podatności określonymi w załączniku I część II, w tym poprzez utrzymywanie procesów mających na celu wyeliminowanie podatności i zaradzenie im oraz poprzez dokonywanie przeglądu oceny ryzyka w cyberprzestrzeni zgodnie z art. 13 ust. 3.

W takich okolicznościach mikrokontroler zaprojektowany przed datą rozpoczęcia stosowania aktu o cyberodporności może zostać wprowadzony do obrotu bez zmiany projektu, pod warunkiem że producent może wykazać w drodze oceny ryzyka w cyberprzestrzeni i dokumentacji technicznej, że ten mikrokontroler osiąga odpowiedni poziom cyberbezpieczeństwa w świetle swojego przeznaczenia i racjonalnie przewidywalnego wykorzystania oraz spełnia mające zastosowanie zasadnicze wymagania.

3. **WOLNE I OTWARTE OPROGRAMOWANIE**

40. Jak przypomniano w sekcji *2.1 Wprowadzanie do obrotu*, akt o cyberodporności ma zastosowanie do produktów z elementami cyfrowymi, które są udostępniane na rynku UE w ramach działalności handlowej po raz pierwszy (tj. „wprowadzane do obrotu"), a także do każdego późniejszego przypadku, który stanowi udostępnienie tego samego produktu z elementami cyfrowymi na rynku. W Niebieskim przewodniku (sekcja 2.2) wyjaśniono, że „działalność handlową" należy rozumieć jako dostarczanie towarów, za opłatą lub nieodpłatnie, w kontekście związanym z działalnością gospodarczą i można ją ocenić wyłącznie indywidualnie dla każdego przypadku przy uwzględnieniu regularności dostaw, charakterystyki produktu, intencji dostawcy itp.

41. Dostarczanie w ramach działalności handlowej charakteryzuje się szeregiem okoliczności, szczegółowo udokumentowanych w Niebieskim przewodniku i przywołanych w motywie 15 aktu o cyberodporności. Mogą one obejmować bezpośrednie pobieranie zapłaty, a także „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" (motyw 15) ([11]).

42. W akcie o cyberodporności uznano jednak specyfikę różnych sposobów opracowywania i upubliczniania „wolnego i otwartego oprogramowania" i przedstawiono pewne wytyczne, które mają pomóc w ustaleniu, czy wolne i otwarte oprogramowanie jest produktem z elementami cyfrowymi wprowadzanym do obrotu (tj. w ramach działalności handlowej) w rozumieniu aktu o cyberodporności. Jak wyjaśniono w motywie 18, „[p]rzy 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, „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".

([11]) Należy również przypomnieć, że chociaż często produkty z elementami cyfrowymi są monetyzowane (również) poprzez przetwarzanie danych osobowych, ochrona danych osobowych stanowi prawo podstawowe, a zatem danych osobowych nie można uznać za towar, jak wskazano w motywie 24 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych, *Dz.U. L 136 z 22.5.2019, s. 1*, ELI: http://data.europa.eu/eli/dir/2019/770/oj.

43. Warto zatem (i) wyjaśnić, czym jest wolne i otwarte oprogramowanie; (ii) określić, kiedy uznaje się, że wchodzi ono w zakres odpowiedzialności osoby fizycznej lub prawnej; oraz (iii) podać przykłady, które pomogą zainteresowanym stronom zrozumieć, kiedy dystrybucja wolnego i otwartego oprogramowania stanowi wprowadzenie do obrotu. W przypadku gdy wolne i otwarte oprogramowanie nie jest wprowadzane do obrotu, nie wchodzi w zakres stosowania aktu o cyberodporności, chyba że podmiot upubliczniający jest osobą prawną, która spełnia definicję „opiekuna oprogramowania otwartego" (zwanego dalej „opiekunem") zawartą w art. 3 pkt 14. W takim przypadku podlega on jedynie obowiązkom określonym w art. 24.

44. W art. 3 pkt 48 zdefiniowano wolne i otwarte oprogramowanie jako „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". Chociaż w niniejszych wytycznych nie wskazano konkretnych licencji wolnego i otwartego oprogramowania, które są zgodne z definicją określoną w art. 3 pkt 48, z brzmienia tego przepisu wynika, że jedynie oprogramowanie, które łącznie spełnia dwa warunki, kwalifikuje się jako wolne i otwarte oprogramowanie do celów aktu o cyberodporności: (i) oprogramowanie musi być udostępniane bezpłatnie i na otwartej licencji przyznającej pełny zestaw praw, o których mowa w art. 3 pkt 48; oraz (ii) jego kod źródłowy musi być powszechnie dostępny.

45. Wymóg, aby licencja zapewniała wszystkim prawo do „wolnego dostępu do niego, używania go, modyfikowania i redystrybucji", odzwierciedla tradycyjne rozumienie wolnego i otwartego oprogramowania, zgodnie z którym użytkownicy muszą mieć dostęp do kodu źródłowego, korzystać z niego bez nieuzasadnionych ograniczeń, modyfikować go i redystrybuować wersje oryginalne lub zmodyfikowane. Dostęp do kodu źródłowego jest zatem niezbędnym warunkiem wstępnym wykonywania pozostałych praw: bez dostępu do kodu źródłowego nie jest praktycznie możliwa modyfikacja lub istotne ponowne wykorzystanie oprogramowania.

46. Jednakże art. 3 pkt 48 wykracza poza odniesienie wyłącznie do warunków licencji, ponieważ wyraźnie wymaga, aby kod źródłowy „był powszechnie dostępny". Pojęcie „powszechnie dostępny" wskazuje, że kod źródłowy musi być publicznie dostępny (zarówno na wcześniejszym, jak i na dalszym etapie łańcucha dostaw) i nie może być dostarczany jedynie na zasadach ograniczonych lub warunkowych. W związku z tym oprogramowania dystrybuowanego bezpłatnie i na otwartej licencji, którego kod źródłowy jest udostępniany (lub może być udostępniany) wyłącznie klientom płacącym lub ograniczonej grupie użytkowników, nie należy uznawać za wolne i otwarte oprogramowanie w rozumieniu art. 3 pkt 48. Do celów aktu o cyberodporności za oprogramowanie kwalifikujące się jako wolne i otwarte należy zatem uznać wyłącznie oprogramowanie, którego kod źródłowy jest dostępny publicznie i które jest oferowane bezpłatnie i na otwartej licencji przyznającej pełny zbiór praw, o których mowa w art. 3 pkt 48.

3.1. **Ustalenie, czy dana osoba jest odpowiedzialna za wolne i otwarte oprogramowanie**

47. Akt o cyberodporności nakłada kluczowe obowiązki na podmioty gospodarcze, które dostarczają produkty z elementami cyfrowymi na rynek UE. Definiuje on producenta jako osobę fizyczną lub prawną, która dostarcza produkt z elementami cyfrowymi pod własną nazwą lub znakiem towarowym i czyni to w ramach działalności handlowej (wprowadzając go tym samym do obrotu). Podobnie importer to osoba fizyczna lub prawna mająca siedzibę w UE, która dostarcza produkt z elementami cyfrowymi osoby mającej siedzibę poza UE i czyni to w ramach działalności handlowej (wprowadzając go w ten sposób do obrotu). Obowiązki przewidziane dla opiekunów mają zastosowanie do osoby prawnej, która dostarcza wolne i otwarte oprogramowanie przeznaczone do działalności handlowej ([12]), ale nie wprowadza go do obrotu w rozumieniu aktu o cyberodporności.

48. W związku z tym, aby ustalić, czy osoba fizyczna lub prawna wprowadza wolne i otwarte oprogramowanie do obrotu w UE, należy najpierw wyjaśnić, czy ta osoba fizyczna lub prawna dostarcza rzeczywiście wolne i otwarte oprogramowanie. Aby prawidłowo określić mające zastosowanie obowiązki wynikające z aktu o cyberodporności, konieczne jest ustalenie, czy osoba fizyczna lub prawna rzeczywiście wykonuje działanie polegające na dostarczaniu wolnego i otwartego oprogramowania. Jak przypomniano w motywie 18, akt o cyberodporności 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.

([12]) Jest to warunek konieczny, ale niewystarczający, aby osoba prawna kwalifikowała się jako opiekun oprogramowania otwartego, ponieważ definicja określona w art. 3 pkt 14 ustanawia dodatkowe warunki, które musi spełnić osoba prawna, aby kwalifikowała się jako opiekun.

49. Biorąc pod uwagę specyfikę opracowywania wolnego i otwartego oprogramowania, które często obejmuje wielu współtwórców, opiera się na zdecentralizowanych modelach współpracy oraz charakteryzuje się rozdzieleniem funkcji wkładu i podejmowania decyzji, warto wyjaśnić, że wolne i otwarte oprogramowanie uznaje się za „podlegające odpowiedzialności" osób fizycznych lub prawnych, które je upubliczniają i sprawują zasadniczą kontrolę nad jego opracowywaniem, wydaniami i decyzjami dotyczącymi dystrybucji (często zwanych „osobami odpowiedzialnymi za utrzymanie"). Osoby, które tworzą kod źródłowy, ale nie sprawują kontroli nad wydaniami, planami działania ani decyzjami dotyczącymi zarządzania, uznaje się za „współtwórców"; w takich przypadkach wolne i otwarte oprogramowanie nie leży w zakresie ich odpowiedzialności, mimo że stworzyli do niego kod. Samo posiadanie uprawnień technicznych, takich jak dostęp do zatwierdzania zmian, nie wystarcza do stwierdzenia, że wolne i otwarte oprogramowanie znajduje się w zakresie odpowiedzialności tej osoby; odpowiedzialność spoczywa na tych, którzy upubliczniają wolne i otwarte oprogramowanie oraz sprawują nad nim kontrolę.

Przykład 13: Indywidualny programista lub pracownik firmy przesyła do projektu wolnego i otwartego oprogramowania zgłoszenie zmiany typu „pull request" lub „merge request" zawierające poprawkę zabezpieczeń lub nową funkcjonalność. Osoby utrzymujące projekt dokonują przeglądu kodu, akceptują go i włączają do głównej bazy kodu, a następnie uwzględniają go w nowym wydaniu oprogramowania. W tym scenariuszu osoba, która przesłała zgłoszenie „pull request", jest „współtwórcą" i nie podlega przepisom aktu o cyberodporności. Mimo że osoba ta stworzyła kod źródłowy, nie sprawuje ona zasadniczej kontroli nad rozwojem oprogramowania, jego wydaniami ani decyzjami dotyczącymi dystrybucji.

3.2. **Ustalenie, czy wolne i otwarte oprogramowanie jest wprowadzane do obrotu w UE**

50. Po ustaleniu, że za wolne i otwarte oprogramowanie odpowiada osoba fizyczna lub prawna, należy ustalić, czy osoba ta dostarcza je w ramach działalności handlowej, co stanowi wprowadzenie do obrotu.

3.2.1. *Pobieranie opłaty*

51. W przypadku gdy osoba fizyczna lub prawna, która dostarcza wolne i otwarte oprogramowanie, pobiera opłatę za samo oprogramowanie (np. pobierając opłatę za skompilowane pliki binarne), osoba ta wprowadza produkt z elementami cyfrowymi do obrotu. Osoba wprowadzająca wolne i otwarte oprogramowanie do obrotu jest zatem producentem w rozumieniu aktu o cyberodporności.

52. Często producenci wolnego i otwartego oprogramowania dostarczają bezpłatne wersje tego oprogramowania (często nazywane wersjami „społecznościowymi"), których baza kodu jest (niemal) identyczna z wersją płatną. Te produkty z elementami cyfrowymi stanowią jednak odrębne produkty: wersja płatna jest w jakiś sposób monetyzowana (np. poprzez pobieranie opłaty lub za pomocą innych środków, o których mowa w niniejszej sekcji) i w związku z tym uznaje się ją za wprowadzoną do obrotu, co powoduje powstanie obowiązków producenta. Wersja udostępniana bezpłatnie (lub wersja społecznościowa) nie jest przedmiotem monetyzacji i w związku z tym nie uznaje się jej za wprowadzoną do obrotu dla celów aktu o cyberodporności. Dotyczy to również sytuacji, w której wersja płatna jest „rozszerzoną" wersją komercyjną, która rozbudowuje bazę kodu wersji dostarczanej bezpłatnie lub włącza tę wersję do szerszego produktu z elementami cyfrowymi (jak ma to miejsce na przykład w modelu „open-core").

53. Jeżeli osoba dostarczająca wersję społecznościową jest osobą prawną, osoba ta podlega również obowiązkom nałożonym na opiekunów w odniesieniu do wersji, którą dostarcza bezpłatnie (wersji społecznościowej). Jeżeli podmiot jest osobą fizyczną, wersja dostępna bezpłatnie (wersja społecznościowa) nie wchodzi w zakres stosowania aktu o cyberodporności.

3.2.2. *Monetyzacja innych usług lub żądanie przetwarzania danych osobowych*

54. Osoba fizyczna lub prawna upubliczniająca wolne i otwarte oprogramowanie może również wprowadzać je do obrotu (tj. dostarczać je w ramach działalności handlowej), jeżeli dostarcza oprogramowanie, za pomocą którego zarabia na innych produktach z elementami cyfrowymi lub usługach cyfrowych, lub jeżeli wymaga jako warunku korzystania z oprogramowania przetwarzania danych osobowych z powodów innych niż wyłącznie poprawa bezpieczeństwa, kompatybilności lub interoperacyjności oprogramowania.

Przykład 14: Osoba fizyczna lub prawna upublicznia bezpłatną i otwartą aplikację pełniącą funkcję platformy handlowej. Aplikacja ta jest dostępna bez opłat i umożliwia użytkownikom dokonywanie za jej pośrednictwem zakupów towarów lub usług. Aplikacja umożliwia osobie, która ją upubliczniła, monetyzację innych produktów z elementami cyfrowymi oraz usług oferowanych za jej pośrednictwem (np. poprzez reklamy, prowizje lub opłaty abonamentowe). W związku z tym uznaje się, że aplikacja ta została wprowadzona do obrotu w ramach działalności handlowej.

Przykład 15: Osoba fizyczna lub prawna upublicznia bezpłatną i otwartą aplikację VPN. Aplikacja jest dostępna bezpłatnie, ale umożliwia użytkownikom płacenie za dostęp do dodatkowych serwerów lub dedykowanych adresów IP. Aplikacja ta umożliwia tej osobie monetyzację innych usług oferowanych za jej pośrednictwem, w związku z czym uznaje się ją za wprowadzoną do obrotu w ramach działalności handlowej.

Przykład 16: Osoba fizyczna lub prawna upublicznia bezpłatną i otwartą aplikację do śledzenia aktywności fizycznej. Aplikacja jest dostępna bezpłatnie, ale korzystanie z niej jest uzależnione od przetwarzania danych osobowych użytkowników do celów takich jak reklama ukierunkowana lub analityka niezwiązana z bezpieczeństwem, kompatybilnością lub interoperacyjnością oprogramowania. Ponieważ wymaganie takiego przetwarzania danych stanowi warunek korzystania z aplikacji, uznaje się, że została ona wprowadzona do obrotu w ramach działalności handlowej.

3.2.3. *Usługi wsparcia*

55. Sam fakt, że osoba fizyczna lub prawna upubliczniająca wolne i otwarte oprogramowanie oferuje również związane z nim płatne usługi wsparcia, nie oznacza sam w sobie, że produkt z elementami cyfrowymi jest dostarczany w ramach działalności handlowej. Usługi wsparcia mogą obejmować takie działania jak doradztwo, szkolenia lub profesjonalne usługi związane z użytkowaniem, dokumentacją, konfiguracją i wdrażaniem oprogramowania przez klienta.

56. Decydującym czynnikiem jest to, czy dostęp do samego wolnego i otwartego oprogramowania (tj. dostarczanie produktu z elementami cyfrowymi), w tym jego utrzymanie, jest uzależniony od wynagrodzenia, a nie od samego oferowania profesjonalnych usług związanych z bezpłatnie dostępnym produktem z elementami cyfrowymi, jak wskazano w motywie 18 aktu o cyberodporności („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"). W przypadku gdy wolne i otwarte oprogramowanie można bezpłatnie pobrać i zainstalować, a użytkownicy mogą opcjonalnie zdecydować się na zakup usług profesjonalnych oddzielnie, tego wolnego i otwartego oprogramowania nie uznaje się za wprowadzone do obrotu.

57. Natomiast w niektórych przypadkach dostęp do konkretnej wersji produktu z elementami cyfrowymi, w tym do pewnych korzyści, takich jak pomoc techniczna lub optymalizacja wydajności, jest uzależniony od uiszczenia wynagrodzenia. W takich przypadkach takie dostarczenie stanowi płatne udostępnienie produktu z elementami cyfrowymi dostarczonego w ramach działalności handlowej i w związku z tym uznaje się je za wprowadzenie do obrotu. Dotyczy to również sytuacji, w których płatne wydanie lub wersja dla przedsiębiorstw są udostępniane na podstawie umowy handlowej, niezależnie od tego, czy funkcjonalnie równoważne oprogramowanie jest również dostępne bezpłatnie na podstawie otwartej licencji.

Przykład 17: Osoba fizyczna lub prawna upublicznia bezpłatny i otwarty system operacyjny, oferując jednocześnie płatną wersję tego systemu, która obejmuje usługi wsparcia, takie jak pomoc techniczna lub optymalizacja wydajności. Płatną wersję systemu operacyjnego uznaje się za wprowadzoną do obrotu w ramach działalności handlowej.

Przykład 18: Osoba fizyczna lub prawna upublicznia bezpłatne i otwarte narzędzie wiersza poleceń. Narzędzie to jest ogólnodostępne i każdy może je pobrać i zainstalować. Ta osoba fizyczna lub prawna oferuje oddzielnie profesjonalne usługi, takie jak opcjonalne usługi doradcze w zakresie szkolenia użytkowników i wspierania ich w instalacji i korzystaniu z narzędzia. Takiego wolnego i otwartego oprogramowania nie uznaje się za wprowadzone do obrotu w rozumieniu aktu o cyberodporności.

58. W szczególności w przypadku osób fizycznych upubliczniających wolne i otwarte oprogramowanie, oferowanie pomocy technicznej bezpośrednio powiązanej z dostępem do produktu z elementami cyfrowymi nadal nie kwalifikowałoby się jako działalność handlowa, jeżeli, jak wskazano w motywie 15 aktu o cyberodporności, pobierana opłata służy jedynie odzyskaniu rzeczywistych kosztów. Takie rzeczywiste koszty obejmują różne koszty związane z projektowaniem, opracowywaniem i utrzymaniem tego oprogramowania, w tym uzasadnione koszty utrzymania danej osoby. W związku z tym osoby fizycznej upubliczniającej wolne i otwarte oprogramowanie i oferującej pomoc techniczną w celu pokrycia swoich kosztów i uzyskania sprawiedliwego wynagrodzenia nie można uznać, wyłącznie na tej podstawie, za osobę wprowadzającą to oprogramowanie do obrotu w UE.

59. Uznaje się, że osoba fizyczna lub prawna oferująca pomoc techniczną związaną z wolnym i otwartym oprogramowaniem, za które nie jest odpowiedzialna, nie wprowadza tego oprogramowania do obrotu, chyba że osoba ta znacząco zmodyfikuje wolne i otwarte oprogramowanie zgodnie z art. 22 w ramach świadczenia takiej pomocy.

Przykład 19: Usługodawca nie upublicznia wolnego i otwartego oprogramowania, lecz pomaga klientowi w zainstalowaniu go na serwerze lokalnym klienta. Czyni to bez dokonywania istotnej modyfikacji tego wolnego i otwartego oprogramowania. Uznaje się zatem, że usługodawca nie wprowadza wolnego i otwartego oprogramowania do obrotu.

3.2.4. *Darowizny*

60. Osoby fizyczne lub prawne upubliczniające projekty wolnego i otwartego oprogramowania rutynowo uwzględniają sposoby dobrowolnego przekazywania pieniędzy przez użytkowników tego oprogramowania w celu podziękowania wydawcy (wydawcom) projektu, a także zapewnienia aktywnego utrzymania projektu.

61. Jak wskazano w motywie 15 aktu o cyberodporności, „[p]rzyjmowanie darowizn bez zamiaru osiągnięcia zysku nie powinno być uznawane za działalność handlową". Samego faktu umieszczenia linku do platformy darowizn lub podobnych narzędzi do zbierania darowizn nie należy postrzegać jako zamiaru osiągnięcia zysku, nawet jeżeli kwota zebrana z darowizn przekracza zwykłe koszty związane z projektowaniem, opracowywaniem i dostarczaniem produktu z elementami cyfrowymi. Obejmuje to rozsądne wynagrodzenie dla współtwórców zatrudnionych przez osobę prawną lub rozsądne koszty utrzymania osoby fizycznej. Darowizny, ze względu na swój charakter, zmieniają się w czasie, dlatego przy ocenie, czy wolne i otwarte oprogramowanie finansowane wyłącznie przez darowizny jest uznane za wprowadzone do obrotu, należy zachować pewną elastyczność. Jest zatem mało prawdopodobne, aby wolne i otwarte oprogramowanie wspierane wyłącznie przez darowizny zostało uznane za wprowadzone do obrotu w rozumieniu aktu o cyberodporności.

Przykład 20: Osoba fizyczna lub prawna upublicznia narzędzie wolnego i otwartego oprogramowania w publicznym repozytorium internetowym, umożliwiając każdemu pobieranie, wykorzystywanie, modyfikowanie i dalsze rozpowszechnianie tego narzędzia bezpłatnie i na otwartej licencji. Wydawca zachęca użytkowników do dobrowolnego przekazywania darowizn za pośrednictwem platformy darowizn, aby wspierać dalszy rozwój i utrzymanie projektu. Dostęp do oprogramowania, jego kodu źródłowego i jego aktualizacji nie jest uzależniony od dokonania darowizny. Tego wolnego i otwartego oprogramowania nie uznaje się za dostarczone w ramach działalności handlowej i nie uznaje się go za wprowadzone do obrotu w rozumieniu aktu o cyberodporności.

62. Istnieją jednak przypadki, w których wolne i otwarte oprogramowanie wspierane przez darowizny można uznać za wprowadzone do obrotu. Ma to miejsce w przypadku gdy – na podstawie całościowej oceny okoliczności – darowizny są faktycznie równoważne z pobieraniem opłaty za dostęp do produktu z elementami cyfrowymi lub do niektórych jego funkcji. Może tak być w szczególności w przypadku, gdy dostęp do wolnego i otwartego oprogramowania, do jego podstawowych funkcji lub aktualizacji jest w praktyce uzależniony od dokonania darowizny lub gdy darowizny wiążą się z korzyściami umownymi lub wyłącznymi korzyściami wykraczającymi poza korzyści wynikające z przynależności do społeczności.

Przykład 21: Osoba fizyczna lub prawna upublicznia oprogramowanie z elementami cyfrowymi, bezpłatnie i na otwartej licencji, ale udostępnia wersje do pobrania i aktualizacje zabezpieczeń wyłącznie użytkownikom, którzy przekazują darowiznę. Użytkownicy, którzy nie dokonali darowizny, nie mają dostępu do aktualnej wersji oprogramowania.

W tym przypadku darowizny są faktycznym warunkiem dostępu do produktu z elementami cyfrowymi, a zatem stanowią pobieranie opłaty. To wolne i otwarte oprogramowanie uznaje się zatem za wprowadzone do obrotu w rozumieniu aktu o cyberodporności.

Przykład 22: Osoba fizyczna lub prawna udostępnia publicznie kod źródłowy wolnego i otwartego oprogramowania, ale dostarcza skompilowane pliki binarne, regularne aktualizacje oraz gwarantowane poprawki zabezpieczeń wyłącznie darczyńcom. W takim przypadku darowizny są powiązane z dostępem do istotnych aspektów produktu z elementami cyfrowymi i stanowią wynagrodzenie za dostarczenie tego produktu. To wolne i otwarte oprogramowanie uznaje się zatem za wprowadzone do obrotu w ramach działalności handlowej.

3.2.5. *Finansowanie wolnego i otwartego oprogramowania*

63. Sam fakt, że osoba trzecia opłaciła, sponsorowała lub w inny sposób sfinansowała opracowanie wolnego i otwartego oprogramowania, nie przesądza sam w sobie o tym, czy oprogramowanie to zostało wprowadzone do obrotu. Powszechną praktyką w ekosystemie wolnego i otwartego oprogramowania jest otrzymywanie przez poszczególnych programistów, fundacje lub społeczności finansowania od przedsiębiorstw, organów publicznych lub innych sponsorów w celu pracy nad konkretnymi funkcjami, usuwania błędów lub utrzymywania krytycznych komponentów. Finansowanie to może przybierać różne formy, w tym dotacji, programów nagród za znalezienie błędów, sponsoringu, umów o świadczenie usług lub płatnych prac programistycznych.

64. Jak już wspomniano, w motywie 18 aktu o cyberodporności wyjaśniono, że przy określaniu handlowego charakteru działalności nie należy brać pod uwagę samych tylko okoliczności, w jakich produkt z elementami cyfrowymi został opracowany, ani sposobu, w jaki jego opracowanie zostało sfinansowane.

65. W związku z tym, w przypadku gdy wolne i otwarte oprogramowanie jest ogólnie dostępne i wszyscy mogą bezpłatnie uzyskiwać do niego dostęp, używać go, modyfikować je i rozpowszechniać je, fakt, że podmiot komercyjny mógł zapłacić za ten projekt, nie powinien mieć wpływu na ustalenie, czy oprogramowanie to zostało wprowadzone do obrotu. W rzeczywistości, jeżeli wolne i otwarte oprogramowanie nie jest w inny sposób monetyzowane, nie należy go uznawać za wprowadzone do obrotu. W przypadku gdy przedsiębiorstwo, które sfinansowało opracowanie wolnego i otwartego oprogramowania (jak również każde inne przedsiębiorstwo), włącza je do swojego produktu z elementami cyfrowymi, przedsiębiorstwo to ma obowiązek dochować należytej staranności zgodnie z art. 13 ust. 5 aktu o cyberodporności.

Przykład 23: Indywidualny programista upublicznia projekt wolnego i otwartego oprogramowania i aktywnie go utrzymuje. Producent A zwraca się do programisty z prośbą o dodanie konkretnej funkcji do tego oprogramowania i finansuje te prace. Programista dodaje tę funkcję do bazy kodu wolnego i otwartego oprogramowania, udostępniając ją publicznie i zapewniając wszystkim bezpłatny dostęp do niego, możliwość używania go, modyfikowania i redystrybucji. Uznaje się, że indywidualny programista nie wprowadził tego wolnego i otwartego oprogramowania do obrotu. Jeżeli producent włącza wolne i otwarte oprogramowanie do swojego produktu z elementami cyfrowymi, musi dochować należytej staranności zgodnie z art. 13 ust. 5.

3.2.6. *Podmioty nienastawione na zysk utworzone w celu osiągnięcia celów nienastawionych na zysk*

66. W przypadku gdy osoba prawna upubliczniająca wolne i otwarte oprogramowanie jest organizacją nienastawioną na zysk, która „została założona w formie, która gwarantuje wykorzystanie całego zysku po odjęciu kosztów do osiągnięcia celów nienastawionych na zysk" (motyw 18 aktu o cyberodporności), wolne i otwarte oprogramowanie przez nią upubliczniane nie jest uznawane za wprowadzone do obrotu. W przypadku gdy ta osoba prawna odpowiada definicji „opiekuna", podlega odpowiednim obowiązkom (art. 24 aktu o cyberodporności).

Przykład 24: Osoba prawna udostępnia bezpłatną i otwartą przeglądarkę, która jest bezpośrednio monetyzowana za pośrednictwem partnerstw z wyszukiwarkami, ale cały jej zysk po odjęciu kosztów jest wykorzystywany na cele nienastawione na zysk. Przeglądarki tej nie uznaje się za wprowadzoną do obrotu w rozumieniu aktu o cyberodporności. Osoba prawna, która ją udostępnia, podlega obowiązkom mającym zastosowanie do opiekunów.

3.2.7. *Włączanie komponentów przez innych producentów*

67. W niektórych przypadkach wolne i otwarte oprogramowanie jest upubliczniane przez wyraźnie identyfikowalną osobę fizyczną lub prawną, ale to wolne i otwarte oprogramowanie jest „przeznaczone do włączenia przez innych producentów do ich własnych produktów z elementami cyfrowymi". W takich przypadkach takiego wolnego i otwartego oprogramowania nie uznaje się za wprowadzone do obrotu w UE, chyba że jest ono również monetyzowane przez osobę, która je upublicznia (tj. pierwotnego producenta), zgodnie z poprzednimi sekcjami niniejszych wytycznych.

68. W przypadku gdy wolne i otwarte oprogramowanie nie jest wprowadzane do obrotu, osoba prawna, która je upublicznia, podlegałaby obowiązkom opiekunów, jeżeli zapewnia stałe wsparcie, zgodnie z definicją „opiekuna".

Przykład 25: Osoba prawna upublicznia bibliotekę wolnego i otwartego oprogramowania służącą do tworzenia interfejsów użytkownika. Nie monetyzuje ona udostępniania tej biblioteki, ale włącza ją do jednego ze swoich produktów z elementami cyfrowymi (który z kolei jest wprowadzany do obrotu). Biblioteka nie jest uznawana za wprowadzoną do obrotu w rozumieniu aktu o cyberodporności, ale jest przeznaczona do włączenia do produktów z elementami cyfrowymi. Osoba prawna, która ją udostępnia, jest jej opiekunem.

Przykład 26: Osoba prawna wprowadza do obrotu system operacyjny, a także upublicznia biblioteki wolnego i otwartego oprogramowania, które mają służyć jako oprogramowanie wzorcowe dla użytkowników tego systemu operacyjnego. Osoba prawna nie monetyzuje bibliotek wolnego i otwartego oprogramowania, które są przeznaczone do włączenia do innych produktów z elementami cyfrowymi. Osoba prawna, która je upublicznia, jest opiekunem tych bibliotek wolnego i otwartego oprogramowania

3.3. **Opiekunowie otwartego oprogramowania**

69. W akcie o cyberodporności wprowadza się nową kategorię prawną „opiekuna otwartego oprogramowania" w świetle faktu, że „wiele produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie, które [upublicznia] się, lecz nie udostępnia na rynku w rozumieniu [aktu o cyberodporności], ma duże znaczenie dla cyberbezpieczeństwa" (motyw 19 aktu o cyberodporności).

70. W niektórych przypadkach wolne i otwarte oprogramowanie jest upubliczniane, ale nie jest udostępniane na rynku w rozumieniu aktu o cyberodporności przez osobę prawną, której „celem jest systematyczne i stałe wsparcie na rzecz opracowywania [wolnego i otwartego oprogramowania] [...] przeznaczonego do celów komercyjnych, oraz która zapewnia prawidłowe funkcjonowanie tych produktów" (art. 3 pkt 14 aktu o cyberodporności). W takich przypadkach osoba ta podlega obowiązkom spoczywającym na opiekunach.

71. Opiekuna definiuje się jako „osobę prawną inną niż producent”, ponieważ producent z definicji jest osobą fizyczną lub prawną, która wprowadza produkty z elementami cyfrowymi do obrotu („wprowadza je do obrotu”) pod własną nazwą lub własnym znakiem towarowym. Osoba prawna może pełnić rolę opiekuna wyłącznie w odniesieniu do produktów z elementami cyfrowymi kwalifikujących się jako wolne i otwarte oprogramowanie, które zostały upublicznione, ale nie zostały udostępnione na rynku w rozumieniu aktu o cyberodporności. Pojęcie opiekuna ma zatem zastosowanie do konkretnych przypadków wolnego i otwartego oprogramowania, które „ostatecznie [jest] przeznaczone do celów działalności handlowej, np. do wykorzystania w usługach komercyjnych lub w monetyzowanych produktach z elementami cyfrowymi” (motyw 19 aktu o cyberodporności ([13])), ale nie jest udostępniane na rynku w rozumieniu aktu o cyberodporności, i w odniesieniu do którego osoba prawna upubliczniająca to wolne i otwarte oprogramowanie zapewnia systematyczne wsparcie.

72. Pełnienie funkcji opiekuna konkretnego wolnego i otwartego oprogramowania nie oznacza, że dana osoba prawna jest siłą rzeczy również opiekunem innego wolnego i otwartego oprogramowania, które upublicznia. Podobnie fakt bycia producentem jednego konkretnego wolnego i otwartego oprogramowania nie oznacza, że osoba prawna nie może być opiekunem innego wolnego i otwartego oprogramowania. Obejmuje to dostarczanie „społecznościowych” wersji tego samego wolnego i otwartego oprogramowania, jak opisano w sekcji *3.2.1 Pobieranie opłaty*.

73. Osoba prawna może zatem jednocześnie być opiekunem jednego konkretnego wolnego i otwartego oprogramowania (gdy opiekun systematycznie zapewnia wsparcie w sposób ciągły i gwarantuje prawidłowe funkcjonowanie oprogramowania) oraz producentem innego konkretnego wolnego i otwartego oprogramowania (gdy wprowadza je do obrotu). Innymi słowy, ten sam podmiot prawny może być zobowiązany do pełnienia różnych ról w odniesieniu do różnych projektów wolnego i otwartego oprogramowania.

74. W odniesieniu do każdego konkretnego wolnego i otwartego oprogramowania, które upublicznia, osoba prawna będzie musiała ustalić, czy dane oprogramowanie uznaje się za wprowadzone do obrotu w rozumieniu aktu o cyberodporności. Jeżeli tak, czyni to podmiot prawny producentem oprogramowania. Jeżeli wolnego i otwartego oprogramowania nie uznaje się za wprowadzone do obrotu, osoba prawna może pełnić rolę opiekuna tego oprogramowania, o ile oprogramowanie jest przeznaczone do celów komercyjnych i o ile osoba prawna zapewnia jego utrzymanie zgodnie z definicją opiekuna ([14]).

3.3.1. *Stałe wsparcie i zapewnienie opłacalności wolnego i otwartego oprogramowania*

75. W motywie 19 wyjaśniono, że udzielanie stałego wsparcia na rzecz rozwoju produktu z elementami cyfrowymi może obejmować (między innymi): (i) hosting platform współpracy, na których opracowywane jest oprogramowanie, i zarządzanie tymi platformami; (ii) hosting kodu źródłowego lub oprogramowania; (iii) zarządzanie lub gospodarowanie produktami z elementami cyfrowymi kwalifikującymi się jako wolne i otwarte oprogramowanie; oraz (iv) kierowanie opracowywaniem takich produktów z elementami cyfrowymi.

76. Może tak być na przykład w przypadku podmiotu prawnego, który opracowuje wolne i otwarte oprogramowanie w celu włączenia do swoich produktów z elementami cyfrowymi, a następnie upublicznia je bez wprowadzania go do obrotu. Kwestię tę omówiono również w sekcji *3.2.7 Włączanie komponentów przez innych producentów*. W tym przypadku podmiot prawny nie jest producentem oprogramowania, ale może pełnić rolę jego opiekuna. Ponadto, jak wyjaśniono również w poprzednich sekcjach, podmiot prawny, który upublicznia wersję bezpłatną (lub społecznościową) i wersję monetyzowaną tego samego wolnego i otwartego oprogramowania, uznaje się za opiekuna wersji bezpłatnej (lub społecznościowej) i producenta wersji monetyzowanej.

77. Podobnie podmiot prawny, który monetyzuje wolne i otwarte oprogramowanie, ale jest podmiotem nienastawionym na zysk, którego zysk po odjęciu kosztów jest wykorzystywany do osiągnięcia celów nienastawionych na zysk (a zatem jego wolne i otwarte oprogramowanie nie jest wprowadzane do obrotu w rozumieniu aktu o cyberodporności, jak omówiono w sekcji *3.2.6 Podmioty nienastawione na zysk*), pełni rolę opiekuna upublicznianego przez siebie wolnego i otwartego oprogramowania.

78. Ponadto niektóre fundacje oferują platformy współpracy, które charakteryzują się różnymi formami zarządzania i umożliwiają producentom regularne wnoszenie wkładu w rozwój wolnego i otwartego oprogramowania lub są regularnie finansowane przez producentów. Takie fundacje należy uznać za opiekunów w odniesieniu do konkretnego wolnego i otwartego oprogramowania, które jest przeznaczone do celów komercyjnych i w odniesieniu do którego fundacja oferuje stałe wsparcie. Jak wyjaśniono w sekcji *3.3 Opiekunowie otwartego oprogramowania,* taka fundacja może jednak nie podlegać żadnym obowiązkom wynikającym z aktu o cyberodporności w odniesieniu do innego konkretnego wolnego i otwartego oprogramowania, które hostuje, w przypadkach gdy nie zapewnia systematycznego wsparcia dla konkretnego wolnego i otwartego oprogramowania, nie zapewnia jego opłacalności lub gdy konkretne oprogramowanie nie jest przeznaczone do celów komercyjnych.

([13]) Pojęcie to jest również objęte sformułowaniem „przeznaczone do celów komercyjnych” zawartym w definicji „opiekuna oprogramowania otwartego” ustanowionej w art. 3 pkt 14 aktu o cyberodporności.

([14]) Osoba prawna może również nie podlegać żadnym obowiązkom wynikającym z aktu o cyberodporności w przypadkach, gdy: (i) konkretne wolne i otwarte oprogramowanie nie jest wprowadzane do obrotu w rozumieniu aktu o cyberodporności; oraz (ii) osoba prawna nie spełnia definicji opiekuna w odniesieniu do tego konkretnego wolnego i otwartego oprogramowania.

79. Rodzaj „stałego wsparcia”, jakiego fundacje i podobne organizacje udzielają konkretnym projektom wolnego i otwartego oprogramowania, może się znacznie różnić. Na przykład niektóre podmioty prawne zapewniają jedynie wsparcie nietechniczne, takie jak zarządzanie marką projektów, ustanawianie zasad zarządzania, organizowanie wydarzeń społecznościowych lub zbieranie darowizn. Inne podmioty zapewniają również podstawową infrastrukturę informatyczną niezbędną do prowadzenia projektu, taką jak hosting repozytoriów kodu źródłowego, udostępnianie systemów kontroli wersji lub generowanie kluczy do podpisywania. Jeszcze inne idą o krok dalej w zakresie rodzaju wsparcia, które zapewniają, aktywnie wnosząc do projektu zasoby inżynieryjne, na przykład zatrudniając programistów, koordynując prace programistyczne, przeprowadzając przeglądy lub scalając kod, zarządzając wydaniami lub zajmując się zgłoszeniami podatności i poprawek zabezpieczeń. Chociaż wszystkie podmioty prawne, które kwalifikują się jako opiekunowie na podstawie aktu o cyberodporności, są zobowiązane do wypełniania obowiązków określonych w art. 24 ust. 1 i 2, zakres, w jakim obowiązki określone w art. 14 ust. 1, 3 i 8 mają zastosowanie do tych podmiotów prawnych, różni się w zależności od rodzaju udzielanego przez nie wsparcia, zgodnie z art. 24 ust. 3.

80. Na przykład opiekun, który zapewnia jedynie wsparcie nietechniczne, z definicji nie jest zaangażowany w opracowywanie produktu z elementami cyfrowymi, a zatem nie jest zobowiązany do zgłaszania aktywnie wykorzystywanych podatności. Opiekun ten nie udostępnia również żadnych sieci ani systemów informatycznych na potrzeby opracowywania takich produktów z elementami cyfrowymi, a zatem nie jest zobowiązany do zgłaszania poważnych incydentów ENISA i CSIRT ani użytkownikom, na których incydenty te mają wpływ. Niemniej jednak w przypadku, gdy opiekun dowie się o aktywnie wykorzystywanej podatności (np. za pośrednictwem zgłoszenia ze źródeł zewnętrznych, takich jak eksperci w obszarze bezpieczeństwa), powinien udostępnić informacje osobom odpowiedzialnym za utrzymanie produktu z elementami cyfrowymi, zgodnie ze swoją polityką cyberbezpieczeństwa. Osoby odpowiedzialne za utrzymanie produktów z elementami cyfrowymi lub opiekunowie powinni również rozważyć zgłaszanie podatności na zasadzie dobrowolności, zgodnie z art. 15.

81. Z drugiej strony, w przypadku gdy opiekun zapewnia bazową infrastrukturę informatyczną dla niektórych produktów z elementami cyfrowymi, jest on zobowiązany do powiadamiania ENISA i CSIRT, zgodnie z art. 14 ust. 3, o wszelkich poważnych incydentach związanych z tą infrastrukturą, które mają wpływ na bezpieczeństwo produktów z elementami cyfrowymi. W stosownych przypadkach ma on również obowiązek poinformować wszystkich użytkowników (np. za pomocą ogłoszenia ogólnego). Jak wskazano w poprzednim punkcie, chociaż opiekun nie jest zobowiązany do zgłaszania aktywnie wykorzystywanych podatności, o których się dowiedział, powinien wspierać prawidłowe postępowanie w przypadku podatności i rozważyć dobrowolne zgłaszanie zgodnie z art. 15.

82. Ponadto w przypadku gdy opiekun dostarcza również zasoby inżynieryjne do konkretnych produktów z elementami cyfrowymi, jest on zobowiązany do: (i) zgłaszania, zgodnie z art. 14 ust. 1, aktywnie wykorzystywanych podatności, o których się dowie; oraz (ii) w stosownych przypadkach poinformowania wszystkich użytkowników. W zakresie, w jakim opiekun pozostaje również w bezpośredniej relacji z użytkownikami, których dotyczy podatność, ma on również obowiązek poinformować ich bezpośrednio, zgodnie z art. 14 ust. 8.

83. W przypadku gdy podmiot zaprzestaje udzielania systematycznego wsparcia w sposób ciągły na rzecz konkretnego wolnego i otwartego oprogramowania, może on przestać spełniać definicję opiekuna i w związku z tym może nie podlegać już odpowiednim obowiązkom. W takich przypadkach zachęca się ten podmiot do wyraźnego informowania o zmianie swojego statusu w odniesieniu do danego wolnego i otwartego oprogramowania.

84. W niektórych sytuacjach podmiot, który pełnił funkcję opiekuna konkretnego projektu, może zdecydować się na bezpośrednią monetyzację tego projektu, wprowadzając tym samym produkt z elementami cyfrowymi do obrotu i powodując powstanie obowiązków producenta wynikających z aktu o cyberodporności. W takich okolicznościach podmiot ten kwalifikuje się jako producent produktu z elementami cyfrowymi od dnia, w którym wprowadza go do obrotu (ale nie w odniesieniu do wcześniejszych wersji, w przypadku których działał jako opiekun).

3.4. **Współtwórcy i zastosowania na dalszym etapie łańcucha dostaw**

85. Jak już wspomniano w sekcji *3.1 Ustalenie, czy dana osoba jest odpowiedzialna za wolne i otwarte oprogramowanie*, w akcie o cyberodporności wyjaśniono, że nie ma on 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” (motyw 18).

86. Producenci produktów z elementami cyfrowymi, którzy włączają komponenty wolnego i otwartego oprogramowania do tych produktów, również nie ponoszą odpowiedzialności za zgodność poszczególnych komponentów z aktem o cyberodporności, nawet jeżeli ci producenci wnoszą kod źródłowy na potrzeby utrzymywania tych komponentów.

87. Podobnie sam fakt, że producenci włączają komponenty wolnego i otwartego oprogramowania do własnych (monetyzowanych) produktów z elementami cyfrowymi, nie ma wpływu na status tego komponentu wolnego i otwartego oprogramowania w rozumieniu aktu o cyberodporności. Osoby odpowiedzialne za utrzymanie komponentów wolnego i otwartego oprogramowania, które nie są wprowadzane do obrotu, nie mają żadnych obowiązków wobec innych podmiotów, które mogą włączać takie komponenty do swoich produktów z elementami cyfrowymi. To, czy akt o cyberodporności ma zastosowanie do danego komponentu wolnego i otwartego oprogramowania, zależy wyłącznie od tego, czy osoba fizyczna lub prawna, która go upublicznia, wprowadza go do obrotu.

88. Producenci produktów z elementami cyfrowymi zawierających komponenty wolnego i otwartego oprogramowania są jednak zobowiązani do przestrzegania przepisów aktu o cyberodporności w odniesieniu do swoich własnych produktów z elementami cyfrowymi. Mają oni również obowiązek dołożenia należytej staranności, zgodnie z art. 13 ust. 5, w odniesieniu do komponentów wolnego i otwartego oprogramowania, które włączają do swoich produktów. Ponadto zgodnie z art. 13 ust. 6 są oni zobowiązani do zgłaszania podatności we włączonych komponentach oraz do dzielenia się rozwiązaniami w zakresie zabezpieczeń. Więcej wskazówek na ten temat można znaleźć w sekcji *9.2.1 Zgłaszanie na wyższym szczeblu łańcucha dostaw i udostępnianie poprawek zabezpieczeń*.

3.5. **Przykładowe scenariusze**

89. Przykłady wymienione poniżej są całkowicie hipotetyczne i mają na celu jedynie zilustrowanie różnych przypadków wyjaśnionych w powyższych sekcjach.

Przykład 27: Indywidualny programista A opracował wolne i otwarte oprogramowanie. Programista A upublicznia to oprogramowanie pod własną nazwą lub znakiem towarowym, ale nie pobiera opłat za jego użytkowanie. Oprogramowanie jest ogólnie dostępne i wszyscy mogą bezpłatnie uzyskiwać do niego dostęp, używać go, modyfikować je i rozpowszechniać. Programista A załącza również link do platformy służącej do gromadzenia dobrowolnych darowizn.

Firmy B, C i D włączają to wolne i otwarte oprogramowanie do swoich produktów z elementami cyfrowymi. Aby wesprzeć bieżące utrzymanie oprogramowania, firmy B, C i D przekazują dobrowolne darowizny na rzecz programisty A. Darowizny te umożliwiają programiście A aktywne utrzymywanie projektu.

To wolne i otwarte oprogramowanie nie jest wprowadzane do obrotu w rozumieniu aktu o cyberodporności. Programista A nie ma żadnych obowiązków wynikających z aktu o cyberodporności. Firmy B, C i D mają obowiązek dołożenia należytej staranności zgodnie z art. 13 ust. 5 przy włączaniu tego oprogramowania do swoich produktów z elementami cyfrowymi.

Przykład 28: Nienastawiona na zysk fundacja F upublicznia komponent wolnego i otwartego oprogramowania w celu włączenia go do innych komercyjnych produktów z elementami cyfrowymi. Fundacja F zobowiązuje się do zapewnienia stałego wsparcia dla tego wolnego i otwartego oprogramowania, aby zapewnić jego prawidłowe funkcjonowanie i wykorzystanie. Firmy A, B i C włączają to wolne i otwarte oprogramowanie do swoich produktów z elementami cyfrowymi. Firmy A i B dobrowolnie poświęcają część czasu swoich programistów na opracowanie i utrzymanie projektów wolnego i otwartego oprogramowania w ramach fundacji F, w tym również tego oprogramowania.

Ponieważ fundacja F jest podmiotem nienastawionym na zysk utworzonym w taki sposób, że jej zysk po odjęciu kosztów jest wykorzystywany do osiągnięcia celów nienastawionych na zysk, wolnego i otwartego oprogramowania nie uznaje się za wprowadzone do obrotu w rozumieniu aktu o cyberodporności. Fundacja F pełni rolę opiekuna oprogramowania i podlega odpowiednim obowiązkom określonym w art. 24. Przedsiębiorstwa A, B i C mają obowiązek dołożenia należytej staranności zgodnie z art. 13 ust. 5 przy włączaniu tego oprogramowania do własnych produktów z elementami cyfrowymi.

Przykład 29: Firma A opracowała komponent wolnego i otwartego oprogramowania w celu włączenia go do jej własnych produktów z elementami cyfrowymi. Upublicznia ona również to wolne i otwarte oprogramowanie oddzielnie pod własną nazwą lub znakiem towarowym i aktywnie je utrzymuje. Nie pobiera jednak opłat za jego używanie ani nie monetyzuje go w inny sposób. Firmy B, C i D włączają ten komponent wolnego i otwartego oprogramowania do swoich własnych produktów z elementami cyfrowymi i dobrowolnie poświęcają część czasu swoich programistów na jego utrzymanie.

Tego wolnego i otwartego oprogramowania nie uznaje się za wprowadzone do obrotu w rozumieniu aktu o cyberodporności. Firma A nie jest jego producentem, lecz opiekunem. Firmy B, C i D mają obowiązek dołożenia należytej staranności zgodnie z art. 13 ust. 5 przy włączaniu tego oprogramowania do własnych produktów z elementami cyfrowymi.

Przykład 30: Firma A upublicznia wolne i otwarte oprogramowanie pod własną nazwą lub znakiem towarowym i oferuje je w wersji płatnej, co obejmuje pewne korzyści, takie jak pomoc techniczna lub optymalizacja wydajności. Programiści z firm B, C i D wnoszą wkład w utrzymanie wolnego i otwartego oprogramowania, ale pozostaje ono pod kontrolą firmy A.

Firmę A uznaje się za producenta tego wolnego i otwartego oprogramowania ([15]). Firmy B, C i D nie podlegają obowiązkom wynikającym z aktu o cyberodporności w odniesieniu do tego konkretnego oprogramowania. Jeżeli włączają to wolne i otwarte oprogramowanie do swoich własnych produktów z elementami cyfrowymi, są zobowiązane do dołożenia należytej staranności zgodnie z art. 13 ust. 5.

Przykład 31: Firma A upublicznia wolne i otwarte oprogramowanie pod własną nazwą lub znakiem towarowym i zapewnia bieżące utrzymanie w celu zapewnienia jego długoterminowej funkcjonalności, aby umożliwić włączenie tego oprogramowania do produktów z elementami cyfrowymi innych firm. Firma A nie pobiera opłat za korzystanie z niego, nie przetwarza danych osobowych, które gromadzi za pośrednictwem produktu z elementami cyfrowymi, ani nie sprzedaje usług wsparcia związanych z upublicznianiem wolnego i otwartego oprogramowania.

Firma B wnosi wkład w postaci kodu i czasu pracy programistów na rzecz utrzymania wolnego i otwartego oprogramowania, ale nie zajmuje się jego komercyjną dystrybucją. Firma B oferuje usługi wsparcia technicznego niezależnie od dystrybucji wolnego i otwartego oprogramowania. Firmę A uznaje się za opiekuna tego wolnego i otwartego oprogramowania, podczas gdy firma B nie ma żadnych obowiązków wynikających z aktu o cyberodporności w odniesieniu do tego wolnego i otwartego oprogramowania.

Przykład 32: Komponent wolnego i otwartego oprogramowania jest upubliczniany przez podmiot nienastawiony na zysk utworzony w sposób zapewniający, aby cały przychód po odjęciu kosztów był wykorzystywany do osiągnięcia celów nienastawionych na zysk. Podmiot ten zapewnia stałe wsparcie w celu zapewnienia długoterminowego prawidłowego funkcjonowania projektu. Utrzymanie jest finansowane ze środków publicznych, takich jak dotacje na badania naukowe. Dodatkowe prace rozwojowe, w tym nowe funkcje, są finansowane z darowizn i w ramach konkretnych projektów realizowanych we współpracy z producentami, którzy włączają to wolne i otwarte oprogramowanie do swoich produktów z elementami cyfrowymi. Takie funkcje są włączane do bazy kodu wolnego i otwartego oprogramowania.

Podmiot nienastawiony na zysk, który upublicznia komponent wolnego i otwartego oprogramowania, uznaje się za opiekuna tego komponentu. Producent, który przyczynił się do opracowania niektórych funkcji, nie staje się producentem tego komponentu. Jeżeli producent włącza ten komponent wolnego i otwartego oprogramowania do swojego własnego produktu z elementami cyfrowymi, musi dochować należytej staranności zgodnie z art. 13 ust. 5.

Przykład 33: Podmiot nienastawiony na zysk utworzony w sposób zapewniający, aby cały zysk po odjęciu kosztów był wykorzystywany do osiągnięcia celów nienastawionych na zysk, upublicznia zestaw do opracowywania wolnego i otwartego oprogramowania (SDK) i zapewnia jego bieżące utrzymanie. Zestaw SDK jest ogólnie dostępny i wszyscy mogą bezpłatnie uzyskiwać do niego dostęp, używać go, modyfikować i rozpowszechniać. Finansowanie pochodzi ze składek członkowskich wpłacanych na rzecz podmiotu nienastawionego na zysk, a programiści zatrudnieni przez organizacje członkowskie przyczyniają się do rozwoju zestawu SDK, tworząc kod i inne zasoby. Producenci wykorzystują zestaw SDK jako komponent do tworzenia innych produktów z elementami cyfrowymi.

Podmiot nienastawiony na zysk, który upublicznia ten zestaw SDK, pełni rolę jego opiekuna. Członkowie fundacji nie ponoszą odpowiedzialności za zgodność zestawu SDK z aktem o cyberodporności. W przypadku gdy producenci wykorzystują zestaw SDK do budowy własnego produktu z elementami cyfrowymi, muszą dochować należytej staranności zgodnie z art. 13 ust. 5.

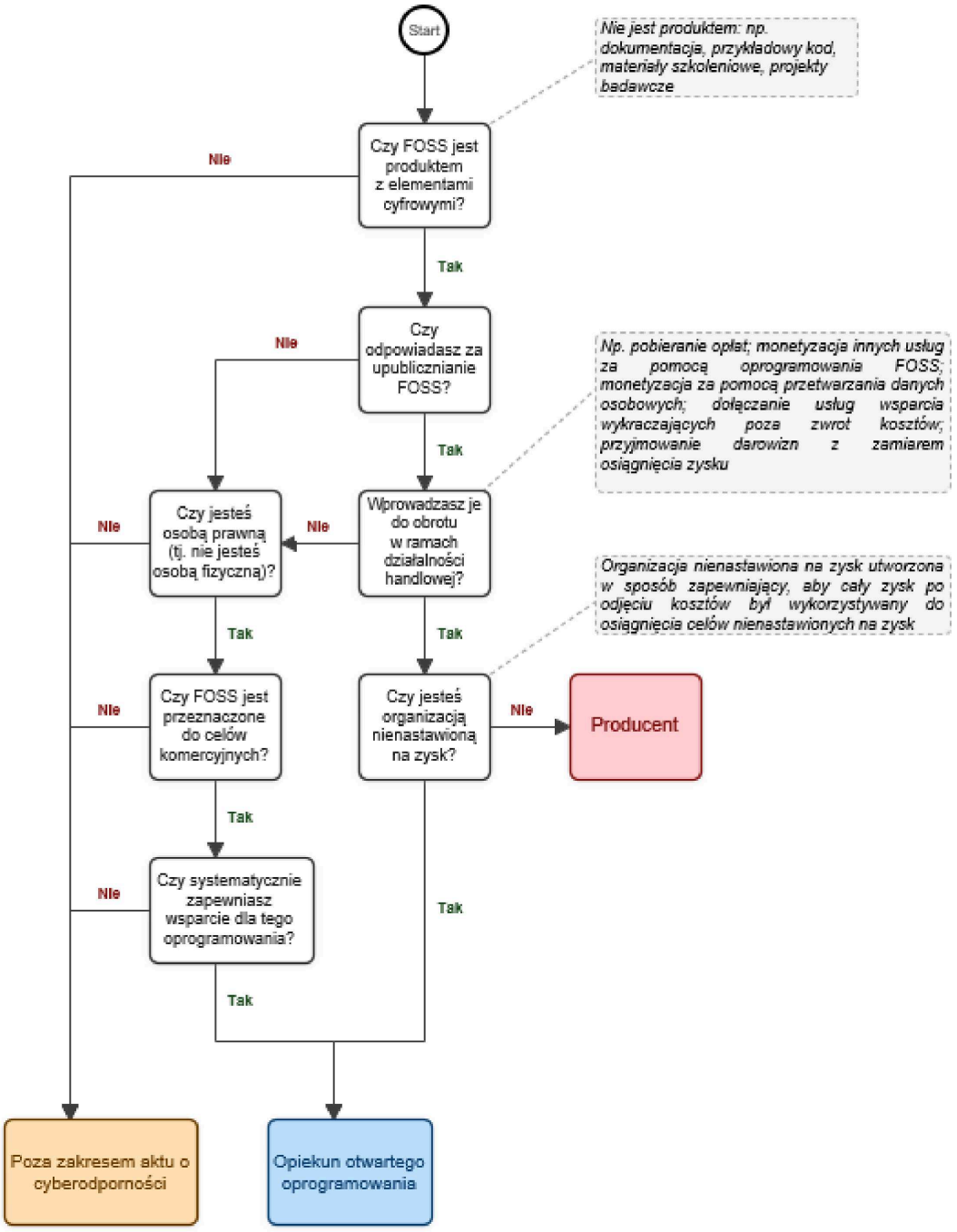
Przykład 34: Indywidualny programista upublicznia bibliotekę wolnego i otwartego oprogramowania w publicznym repozytorium pakietów dla danego języka programowania i aktywnie ją utrzymuje. W dokumentacji pakietu programista dodaje link umożliwiający przekazywanie darowizn. Producent pobiera tę bibliotekę z repozytorium bezpłatnie i włącza ją do własnego produktu z elementami cyfrowymi.

Indywidualny programista i repozytorium pakietów nie mają żadnych obowiązków wynikających z aktu o cyberodporności. Producent, który włącza tę bibliotekę, musi dochować należytej staranności zgodnie z art. 13 ust. 5.

([15]) Chyba że firma A jest podmiotem nienastawionym na zysk utworzonym w sposób zapewniający, aby cały zysk po odjęciu kosztów był wykorzystywany do osiągnięcia celów nienastawionych na zysk, w którym to przypadku firma ta byłaby opiekunem tego wolnego i otwartego oprogramowania.

Rys. 1:

Schematyczne przedstawienie zakresu stosowania aktu o cyberodporności w odniesieniu do wolnego i otwartego oprogramowania (FOSS)



4. ISTOTNE MODYFIKACJE I CZĘŚCI ZAMIENNE

90. W art. 3 pkt 30 aktu o cyberodporności „istotną modyfikację” zdefiniowano jako zmianę w produkcie z elementami cyfrowymi po jego wprowadzeniu do obrotu, która (i) wpływa na zgodność produktu z elementami cyfrowymi z zasadniczymi wymaganiami określonymi w załączniku I część I; lub (ii) powoduje zmianę przeznaczenia, w odniesieniu do którego oceniono produkt z elementami cyfrowymi.

91. Pojęcie istotnej modyfikacji ma znaczenie dla ustalenia obowiązków wynikających z aktu o cyberodporności w szeregu przypadków, w tym w następujących przypadkach:

a) zgodnie z art. 21 importer lub dystrybutor, który dokonuje istotnej modyfikacji produktu z elementami cyfrowymi już wprowadzonego do obrotu, uważany jest za producenta;

b) zgodnie z art. 22 każda osoba fizyczna lub prawna, która dokonuje istotnej modyfikacji produktu z elementami cyfrowymi i udostępnia go na rynku, uważana jest za jego producenta;

c) zgodnie z art. 69 ust. 2 każda osoba fizyczna lub prawna, która po dniu 11 grudnia 2027 r. dokonuje istotnej modyfikacji produktu z elementami cyfrowymi wprowadzonego do obrotu przed dniem 11 grudnia 2027 r. i wprowadza go do obrotu, uważana jest za jego producenta;

d) w przypadku producentów produktów z elementami cyfrowymi wprowadzonych do obrotu po dniu 11 grudnia 2027 r. – w celu ustalenia, czy produkt z elementami cyfrowymi musi zostać poddany nowej procedurze oceny zgodności ze względu na zmiany wprowadzone po tej dacie, w szczególności w świetle iteracyjnego charakteru opracowywania oprogramowania.

92. W związku z tym ważne jest, aby zapewnić wytyczne pomagające podmiotom gospodarczym zrozumieć, kiedy modyfikacje sprzętu lub oprogramowania kwalifikują się jako istotne modyfikacje.

4.1. **Naprawy fizyczne**

93. Jak stwierdzono w motywie 42 aktu o cyberodporności, „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, niekoniecznie skutkuje to istotną modyfikacją produktu, na przykład jeśli nie zmienia przeznaczenia ani funkcji oraz jeśli nie wpływa 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 wymaganiami określonymi w niniejszym rozporządzeniu”. Jest to zgodne z sekcją 2.1 Niebieskiego przewodnika, w której przypomniano, że „produkt, w którym po oddaniu do użytku dokonano poważnych zmian lub napraw, musi zostać uznany za nowy produkt, jeżeli: i) jego oryginalne działanie, zastosowanie lub typ zostały zmienione, a nie zostało to przewidziane we wstępnej ocenie ryzyka; ii) w stosunku do odpowiedniego unijnego prawodawstwa harmonizacyjnego zmienił się charakter zagrożenia lub wzrósł poziom ryzyka; oraz (iii) produkt został udostępniony (lub oddany do użytku, jeśli zakres obowiązujących przepisów obejmuje również oddanie do użytku). Oceny należy dokonywać w odniesieniu do poszczególnych przypadków, w szczególności biorąc pod uwagę cel przepisów prawa i typ produktów objętych omawianymi przepisami prawa”.

94. Operacje odnowienia, konserwacji lub naprawy, które skutkują fizycznymi modyfikacjami produktów z elementami cyfrowymi już wprowadzonych do obrotu, niekoniecznie oznaczają istotne modyfikacje. Należy zatem przeprowadzić indywidualną ocenę w celu ustalenia, czy taka fizyczna zmiana wpływa na zgodność produktu z elementami cyfrowymi z zasadniczymi wymaganiami określonymi w załączniku I część I lub powoduje zmianę przeznaczenia produktu objętego oceną ryzyka w cyberprzestrzeni.

95. Wymiana wadliwych lub zużytych części na części, które mają lepsze parametry (np. ze względu na postęp techniczny lub fakt, że stara część nie jest już produkowana), sama w sobie nie powoduje istotnej modyfikacji naprawionego produktu z elementami cyfrowymi. Wymiana powoduje istotną modyfikację tylko wtedy, gdy zmiana wydajności lub sposób działania naprawionego produktu z elementami cyfrowymi (i) wpływa na jego zgodność z zasadniczymi wymaganiami lub (ii) skutkuje zmianą przeznaczenia, która nie została objęta oceną ryzyka.

Przykład 35: Producent serwera komputerowego przeprowadza naprawę, wymieniając uszkodzoną pamięć RAM na nową, o lepszej wydajności. Nie ma to wpływu na zgodność serwera z zasadniczymi wymaganiami. Serwer działa lepiej, ale jego nowa wydajność pozostaje zgodna z zamierzonym zastosowaniem serwera uwzględnionym w ocenie ryzyka w cyberprzestrzeni. Serwera nie uważa się za istotnie zmodyfikowany.

4.2. **Części zamienne**

96. Art. 2 ust. 6 aktu o cyberodporności stanowi, że części zamienne przeznaczone do wymiany identycznych komponentów i wytwarzane zgodnie z tymi samymi specyfikacjami co te komponenty nie podlegają aktowi o cyberodporności. W motywie 29 stwierdza się ponadto, że odstępstwo to dotyczy zarówno części zamiennych do produktów z elementami cyfrowymi udostępnionych przed rozpoczęciem stosowania aktu o cyberodporności, jak i części zamiennych, które zostały już poddane procedurze oceny zgodności określonej w rozporządzeniu.

97. Odstępstwo przewidziane w art. 2 ust. 6 aktu o cyberodporności należy rozumieć jako mające zastosowanie wyłącznie w przypadku, gdy część zamienna jest dostarczana specjalnie w celu naprawy lub przedłużenia trwałości produktu z elementami cyfrowymi już wprowadzonego do obrotu (przed dniem 11 grudnia 2027 r. lub po tym dniu). W przypadku gdy produkt z elementami cyfrowymi jest dostarczany jako produkt samodzielny, bez żadnego związku z konserwacją lub naprawą wcześniej istniejącego produktu z elementami cyfrowymi, jest on wprowadzany do obrotu w rozumieniu aktu o cyberodporności i nie powinien być uznawany za część zamienną objętą zakresem art. 2 ust. 6. Cel konserwacji lub naprawy powinien jasno wynikać z kontekstu dostawy, na przykład przez identyfikację produktu z elementami cyfrowymi lub rodziny produktów w zamówieniu lub ofercie handlowej lub przez dostawę za pośrednictwem kanałów posprzedażnych lub usługowych. Dowody potwierdzające w tym zakresie powinny być również dostępne dla organów nadzoru rynku. Fakt, że produkt z elementami cyfrowymi mógłby z technicznego punktu widzenia być wykorzystany do zastąpienia danego komponentu, nie jest sam w sobie wystarczający, aby objąć go zakresem odstępstwa w przypadku braku takich elementów.

98. W związku z tym, w przypadku gdy część zamienna jest identyczna z komponentem zawartym już w produkcie z elementami cyfrowymi, który został wprowadzony do obrotu przed datą rozpoczęcia stosowania aktu o cyberodporności albo który został wprowadzony do obrotu zgodnie z aktem o cyberodporności, ta część zamienna sama nie podlega aktowi o cyberodporności.

99. Ocena, czy część zamienną należy uznać za identyczną z komponentem, powinna koncentrować się na jej funkcjonalnej roli w produkcie z elementami cyfrowymi oraz na właściwościach, które mogą mieć znaczenie dla cyberbezpieczeństwa. Chociaż zawsze konieczna jest indywidualna ocena każdego przypadku, różnice, które nie mają wpływu na charakterystykę bezpieczeństwa komponentu lub jego profil ryzyka w cyberprzestrzeni, same w sobie nie uniemożliwiają objęcia tej części zamiennej zakresem art. 2 ust. 6 aktu o cyberodporności.

100. Natomiast różnice we właściwościach komponentu istotnych z punktu widzenia cyberbezpieczeństwa, takich jak algorytmy, protokoły, mechanizmy kryptograficzne, funkcje kontroli dostępu lub inne właściwości istotne z punktu widzenia bezpieczeństwa, mogą oznaczać, że nowej części nie można uznać za identyczną z komponentem, który ma zastąpić.

101. W przypadku gdy część zamienna nie jest identyczna z oryginalnym komponentem, ta część zamienna sama w sobie stanowi produkt z elementami cyfrowymi i w związku z tym podlega aktowi o cyberodporności. W takich przypadkach zgodność z zasadniczymi wymaganiami należy oceniać w świetle przeznaczenia komponentu zamiennego. Szczególnie istotna jest funkcja komponentu zamiennego polegająca na zapewnieniu kompatybilności lub interoperacyjności z istniejącym produktem z elementami cyfrowymi, w tym w przypadku gdy produkt ten jest produktem z elementami cyfrowymi wprowadzonym do obrotu przed rozpoczęciem stosowania aktu o cyberodporności. W przypadku gdy ze względu na to przeznaczenie lub ograniczenia techniczne nie można racjonalnie spełnić niektórych zasadniczych wymagań, producent musi uwzględnić to w ocenie ryzyka w cyberprzestrzeni i wdrożyć odpowiednie alternatywne lub kompensacyjne środki zmniejszające ryzyko, aby nie osłabiać bezpieczeństwa produktu z elementami cyfrowymi. Jak omówiono również w sekcji *2.6 Systemy złożone*, zarówno dokumentacja techniczna, jak i informacje i instrukcje dla użytkownika odgrywają kluczową rolę w przejrzystym opisaniu zidentyfikowanych ograniczeń, związanego z nimi ryzyka w cyberprzestrzeni oraz wdrożonych środków ograniczających ryzyko. Jak wyjaśniono w sekcji *4.1 Naprawy fizyczne*, zastąpienie wadliwych części lub zużytych elementów częściami o lepszych parametrach samo w sobie nie powoduje istotnej modyfikacji naprawionego produktu z elementami cyfrowymi.

Przykład 36: Producent wprowadził do obrotu w UE sterowniki podłączone do sieci. W jednym przypadku sterownik został wprowadzony do obrotu w 2026 r., przed datą rozpoczęcia stosowania aktu o cyberodporności. W drugim przypadku sterownik został wprowadzony do obrotu w 2028 r., zgodnie z aktem o cyberodporności. W 2028 r. w obu typach sterowników dochodzi do awarii modułu komunikacji cyfrowej. Producent dostarcza jako część zamienną moduł zastępczy, który jest identyczny i wyprodukowany zgodnie z tymi samymi specyfikacjami, co moduł oryginalny.

W obu przypadkach moduł zastępczy wchodzi w zakres wyłączenia określonego w art. 2 ust. 6. Część zamienna sama w sobie nie podlega przepisom aktu o cyberodporności, mimo że jest produktem z elementami cyfrowymi, ponieważ zastępuje identyczny komponent w produkcie z elementami cyfrowymi. Naprawa nie stanowi istotnej modyfikacji produktu z elementami cyfrowymi.

Przykład 37: W 2026 r., przed datą rozpoczęcia stosowania aktu o cyberodporności, producent wprowadził do obrotu w UE podłączony do sieci sterownik przemysłowy. W 2028 r. dochodzi do awarii mikroprocesora komunikacyjnego w tym sterowniku. Ponieważ producent nie wytwarza już tego układu, dostarcza jako część zamienną nowszy mikroprocesor o równoważnej funkcjonalności, ale z inną implementacją kryptograficzną i zaktualizowanym mechanizmem bezpiecznego rozruchu, aby zachować kompatybilność i zapewnić dalsze działanie urządzenia.

W tym przypadku nie można uznać, że mikroprocesor zastępczy jest identyczny, ponieważ różnice w implementacji kryptograficznej i mechanizmie bezpiecznego rozruchu wpływają na właściwości tego mikroprocesora w zakresie cyberbezpieczeństwa. W związku z tym nie podlega on wyłączeniu przewidzianemu w art. 2 ust. 6 i stanowi produkt z elementami cyfrowymi podlegający przepisom aktu o cyberodporności. Zgodność części zamiennej należy oceniać w świetle jej przeznaczenia, w tym jej roli w zapewnianiu interoperacyjności z produktem z elementami cyfrowymi wprowadzonym do obrotu przed rozpoczęciem stosowania aktu o cyberodporności.

Przykład 38: W 2028 r. producent wprowadza do obrotu sterownik inteligentnego budynku zgodnie z aktem o cyberodporności. W 2029 r. dochodzi do awarii modułu łączności bezprzewodowej w tym sterowniku. Ponieważ producent nie produkuje już tego modułu, dostarcza on jako część zamienną nowy moduł, który pełni tę samą funkcję przy użyciu tych samych protokołów komunikacyjnych i mechanizmów bezpieczeństwa, ale opiera się na innym chipsecie i posiada zaktualizowane oprogramowanie układowe, które nie zmienia właściwości, które mogą być istotne dla cyberbezpieczeństwa.

W takim przypadku moduł zastępczy można uznać za identyczny. Moduł ten podlega zatem wyłączeniu, o którym mowa w art. 2 ust. 6, i nie podlega przepisom aktu o cyberodporności.

102. Wyłączenie dotyczące części zamiennych ma zastosowanie niezależnie od tego, czy dana część zamienna zastępuje komponent w produkcie z elementami cyfrowymi, czy też zastępuje kompletny produkt z elementami cyfrowymi, który sam stanowi część większego produktu, w tym w przypadku gdy ten większy produkt z elementami cyfrowymi składa się z kilku zintegrowanych komponentów, pod warunkiem że część zamienna jest dostarczana konkretnie jako część zamienna, jak wyjaśniono w poprzednich punktach.

Przykład 39: W 2027 r. producent wprowadza do obrotu system automatyki przemysłowej, którego jednym z komponentów jest programowalny sterownik logiczny (PLC). W 2031 r. dochodzi do awarii jednostki centralnej (CPU) sterownika PLC. Producent oferuje dwie możliwości naprawy: (i) dostawę zamiennej jednostki centralnej, którą można uznać za identyczną z pierwotnie zainstalowaną jednostką centralną; lub (ii) dostawę kompletnego zastępczego sterownika PLC, który można uznać za identyczny z pierwotnie zainstalowanym sterownikiem. W każdym przypadku część zamienna jest dostarczana za pośrednictwem kanału obsługi posprzedażnej producenta jako część zamienna, a system automatyki przemysłowej, dla którego jest ona przeznaczona, jest wyraźnie określony. W obu przypadkach część zamienna wchodzi w zakres wyłączenia określonego w art. 2 ust. 6, niezależnie od tego, czy dotyczy komponentu wewnątrz sterownika PLC, czy też sterownika jako całości.

4.3. **Aktualizacje oprogramowania jako istotne modyfikacje**

103. Opracowywanie oprogramowania ma charakter iteracyjny, a oprogramowanie z elementami cyfrowymi, które już wprowadzono do obrotu, jest często i na bieżąco aktualizowane. W tym kontekście warto przedstawić bardziej szczegółowe wytyczne pozwalające ustalić, kiedy oprogramowanie należy uznać za znacząco zmodyfikowane. Wytyczne te mają w szczególności pomóc producentom oprogramowania z elementami cyfrowymi, którzy wprowadzają zmiany we własnych produktach, w ustaleniu, czy zmiany te stanowią istotną modyfikację.

104. W motywie 39 wskazano, że produkt z elementami cyfrowymi jest istotnie zmodyfikowany, jeżeli zmiana wpływa na poziom ryzyka w cyberprzestrzeni i jeżeli takie zmienione lub dodatkowe ryzyko nie zostało uwzględnione przez producenta w jego ocenie ryzyka, a w konsekwencji we wdrażaniu zasadniczych wymagań. Producent powinien zatem ocenić indywidualnie dla każdego przypadku, czy aktualizacja oprogramowania wprowadza nowe lub zwiększone ryzyko w cyberprzestrzeni oraz czy takie ryzyko zostało już uwzględnione w jego ocenie ryzyka.

105. W przypadku gdy producent wprowadza do produktu z elementami cyfrowymi nowe funkcje, które skutkują zmianą przeznaczenia produktu jako całości, prawdopodobne jest, że producent nie uwzględnił takich zmian w swojej ocenie ryzyka. W takich okolicznościach zmiana zasadniczo kwalifikowałaby się jako istotna modyfikacja.

Przykład 40: Producent wprowadza do obrotu tablicę wskaźników, która gromadzi dane z maszyn i wyświetla trendy i alerty, nie mając jednak możliwości sterowania tymi maszynami. Następnie producent opracowuje nową wersję tej tablicy wskaźników, wprowadzając funkcje umożliwiające sterowanie maszynami, w tym przez regulację parametrów operacyjnych oraz ponowne uruchamianie maszyn po wystąpieniu awarii. W wyniku tych zmian przeznaczenie tego panelu wykroczyło poza zakres przewidziany w ocenie ryzyka, przechodząc od narzędzia służącego do orientacji sytuacyjnej do produktu z elementami cyfrowymi przeznaczonego do sprawowania kontroli operacyjnej nad innymi urządzeniami. Tablica wskaźników została zatem istotnie zmodyfikowana.

Przykład 41: Producent wprowadza do obrotu aplikację konsumencką przeznaczoną do organizowania i wyświetlania danych osobistych, takich jak e-maile, wiadomości lub dokumenty, oraz do obsługi podstawowych funkcji wyszukiwania i filtrowania. Następnie producent wprowadza aktualizację, która umożliwia aplikacji automatyczną analizę treści użytkownika w celu generowania profili behawioralnych i podejmowania zautomatyzowanych decyzji mających wpływ na ustalanie priorytetów, ukrywanie lub rekomendowanie treści bez interwencji użytkownika. W wyniku tej zmiany przeznaczenie oprogramowania zmienia się z narzędzia do zarządzania informacjami kontrolowanego przez użytkownika na zautomatyzowany system podejmowania decyzji, czego nie przewidziano w ocenie ryzyka. Aplikacja została zatem istotnie zmodyfikowana.

106. Jednocześnie możliwe jest jednak, że producent stopniowo wprowadza nowe funkcje, które już uwzględniono w jego ocenie ryzyka lub które same w sobie nie zmieniają profilu ryzyka w cyberprzestrzeni produktu z elementami cyfrowymi. Może to mieć miejsce na przykład w sytuacji, gdy producent przewidział rozwój tych funkcji, opisał już i ocenił związane z nimi ryzyko oraz wdrożył odpowiednie środki ograniczające ryzyko w celu zapewnienia ciągłej zgodności z zasadniczymi wymaganiami. Może tak być również w przypadku, gdy nowe funkcje nie wprowadzają zmian powodujących pojawienie się nowego lub zwiększonego ryzyka. Aktualizacji tego rodzaju nie należy zatem uznawać za istotne modyfikacje, ponieważ nie zwiększają one ryzyka w cyberprzestrzeni, a co za tym idzie – nie zmieniają sposobu spełnienia zasadniczych wymagań.

Przykład 42: Aplikacja do przesyłania wiadomości jest początkowo udostępniana z funkcjonalnością ograniczoną do przesyłania wiadomości prywatnych („jeden na jeden"). Ocena ryzyka przeprowadzona przez producenta obejmuje późniejsze wprowadzenie wiadomości grupowych, w tym na przykład bardziej złożone przekierowywanie komunikatów. W kolejnej aktualizacji producent dodaje funkcję czatu grupowego wraz ze sterownikami administratora i narzędziami do moderacji, które zostały już przewidziane i ocenione w pierwotnym projekcie. Aktualizacja wprowadza funkcje, które wchodzą w zakres pierwotnego przewidzianego zastosowania i oceny ryzyka. W związku z tym aplikacja do przesyłania wiadomości nie została istotnie zmodyfikowana.

Przykład 43: Wprowadza się do obrotu system monitorowania produkcji z włączonymi tablicami wskaźników przeznaczonymi wyłącznie do odczytu, podczas gdy w architekturze systemu obecne są funkcje automatycznego sterowania, ale pozostają one wyłączone. Ocena ryzyka przeprowadzona przez producenta wyraźnie obejmuje przyszłe uruchomienie pętli sterowania automatycznego, w tym ryzyko w cyberprzestrzeni wynikające ze sterowania w pętli zamkniętej, a także zabezpieczenia, takie jak mechanizmy ręcznego przejęcia kontroli przez operatora i stany awaryjne. W późniejszej aktualizacji producent włącza funkcje automatycznego sterowania i aktywuje zabezpieczenia zgodnie z pierwotną oceną. System monitorowania produkcji nie został zatem istotnie zmodyfikowany.

107. Z drugiej strony nawet ograniczone lub pozornie mało znaczące nowe funkcje mogą powodować znaczne ryzyko w cyberprzestrzeni, które ma wpływ na zgodność z zasadniczymi wymaganiami. Ocena istotnej modyfikacji nie powinna zatem opierać się na skali lub złożoności zmiany, ale na jej potencjalnych niekorzystnych skutkach dla profilu ryzyka w cyberprzestrzeni produktu z elementami cyfrowymi, a w konsekwencji na realizacji zasadniczych wymagań.

Przykład 44: Producent wprowadza aktualizację aplikacji, dodając funkcję „pamiętaj mnie", czyli funkcję trwałego logowania, która lokalnie przechowuje tokeny uwierzytelniające, aby zwiększyć wygodę użytkownika. Chociaż funkcja ta ma ograniczony zakres, wprowadza nowe zagrożenia związane z kradzieżą tokenów, nieuprawnionym dostępem i przejęciem sesji, których nie uwzględniono w ocenie ryzyka. Aktualizacja ma zatem wpływ na zgodność z zasadniczymi wymaganiami. Aplikacja została istotnie zmodyfikowana.

Przykład 45: Producent dodaje nową funkcję rejestrowania i diagnostyki do istniejącego oprogramowania z elementami cyfrowymi, umożliwiając eksport szczegółowych logów systemowych do celów rozwiązywania problemów. Chociaż funkcja ta wydaje się mało znacząca, skutkuje gromadzeniem i przechowywaniem wrażliwych danych operacyjnych w niezaszyfrowanym formacie, co stwarza ryzyko ujawnienia danych, które nie zostało wcześniej ocenione ani ograniczone. Zmiana może zatem mieć znaczący wpływ na profil ryzyka w cyberprzestrzeni produktu z elementami cyfrowymi. Oprogramowanie z elementami cyfrowymi zostało istotnie zmodyfikowane.

108. Zgodnie z motywem 39 aktu o cyberodporności aktualizacji zabezpieczeń zasadniczo nie należy uznawać za istotne modyfikacje, ponieważ ich głównym celem jest zmniejszenie poziomu ryzyka w cyberprzestrzeni produktu z elementami cyfrowymi. Aktualizacji zabezpieczeń, która nie zmienia przeznaczenia danego produktu i nie wprowadza nowych ryzyk w cyberprzestrzeni, nie należy zatem uznawać za istotną modyfikację, nawet jeżeli aktualizacja ta może wprowadzić istotne zmiany techniczne. Obejmuje to przypadki, w których niektóre funkcje są modyfikowane lub ograniczane wyłącznie w celu ograniczenia stwierdzonych podatności i zapewnienia ciągłej zgodności z zasadniczymi wymaganiami.

Przykład 46: Producent wdraża aktualizację zabezpieczeń w celu wyeliminowania podatności w bazie kodu produktu z elementami cyfrowymi przez skorygowanie błędu walidacji danych wejściowych, który mógłby prowadzić do przepełnienia bufora, lub przez usunięcie błędu logicznego umożliwiającego obejście uwierzytelniania poprzez niewłaściwą walidację tokena sesji. Aktualizacja ta modyfikuje wewnętrzną implementację oprogramowania, nie wpływając na przeznaczenie tego produktu ani nie powodując nowego narażenia. Taka aktualizacja ma na celu wyłącznie ograniczenie ryzyka w cyberprzestrzeni. Aktualizacji zabezpieczeń nie należy uznawać za istotną modyfikację.

Przykład 47: Producent wprowadza aktualizację zabezpieczeń, która wzmacnia istniejące konfiguracje zabezpieczeń, np. poprzez zaostrzenie reguł zapory sieciowej, wyłączenie nieużywanych portów sieciowych, zmianę zasad dotyczących domyślnego hasła administratora lub wprowadzenie obowiązku uwierzytelniania wieloskładnikowego, jeżeli taka funkcja była już dostępna lub przewidziana. Chociaż aktualizacja ta może wpływać na sposób, w jaki użytkownicy konfigurują produkt z elementami cyfrowymi lub uzyskują do niego dostęp, nie zmienia ona jego przeznaczenia i służy wyłącznie poprawie stanu bezpieczeństwa. Aktualizacji zabezpieczeń nie należy uznawać za istotną modyfikację.

Przykład 48: Producent wprowadza do obrotu oprogramowanie z elementami cyfrowymi, które zabezpiecza komunikację za pomocą konfigurowalnej platformy szyfrującej obsługującej wiele algorytmów kryptograficznych i rozmiarów kluczy, zgodnie z opisem zawartym w dokumentacji technicznej produktu oraz w ocenie ryzyka. Ocena ryzyka obejmuje wszystkie opcje kryptograficzne przewidziane w produkcie z elementami cyfrowymi i przewiduje przyszłe wycofanie niektórych algorytmów. Ocena ryzyka obejmuje również środki ograniczające ryzyko, takie jak elastyczność kryptograficzna, wewnętrzne zarządzanie kluczami i testowanie zgodności. W odpowiedzi na pojawiające się wytyczne kryptograficzne producent wdraża aktualizację zabezpieczeń, która dezaktywuje wycofany algorytm i aktywuje silniejszą, już obsługiwaną alternatywę, nie wprowadzając przy tym nowych zależności zewnętrznych ani nie zmieniając przepływów danych. Ponieważ aktualizacja wdraża środek bezpieczeństwa, który przewidziano i oceniono jako część pierwotnego projektu, a także nie wprowadza nowego ryzyka w cyberprzestrzeni, aktualizacji zabezpieczeń nie należy uznawać za istotną modyfikację.

109. Z kolei aktualizacja zabezpieczeń może kwalifikować się jako istotna modyfikacja, jeżeli – niezależnie od jej celu w zakresie bezpieczeństwa – skutkuje ona modyfikacją przeznaczenia produktu z elementami cyfrowymi w stopniu wykraczającym poza pierwotnie przewidziane ramy lub wprowadza nowe lub zwiększone ryzyko w cyberprzestrzeni. Może to mieć miejsce na przykład wtedy, gdy aktualizacja istotnie zmienia granice produktu lub strukturę zależności w sposób nieprzewidziany w ocenie ryzyka, np. poprzez istotną zmianę przepływów danych lub dodanie nowych interfejsów dostępnych z zewnątrz.

Przykład 49: Producent wprowadza do obrotu oprogramowanie z elementami cyfrowymi przeznaczone do zapewnienia lokalnego szyfrowania plików w odniesieniu do danych przechowywanych na urządzeniu użytkownika, które umożliwia użytkownikom szyfrowanie i odszyfrowywanie plików na żądanie. Po wykryciu podatności w procesie szyfrowania producent wdraża aktualizację zabezpieczeń, która usuwa funkcję lokalnego szyfrowania i zamiast tego wymaga, aby wszystkie pliki były przesyłane do usługi zdalnego szyfrowania obsługiwanej przez producenta, przechowywane w tej usłudze i przetwarzane przez nią. W wyniku tej zmiany produkt z elementami cyfrowymi nie realizuje już lokalnego szyfrowania zgodnie z pierwotnym zamierzeniem, lecz funkcjonuje jako usługa zdalnego szyfrowania i przetwarzania danych. Chociaż aktualizację wprowadza się ze względów bezpieczeństwa, zasadniczo zmienia ona przeznaczenie tego produktu w sposób nieprzewidziany w ocenie ryzyka, a zatem kwalifikuje się jako istotna modyfikacja.

Przykład 50: Producent wprowadza do obrotu oprogramowanie z elementami cyfrowymi, które w celu zabezpieczenia komunikacji między komponentami produktu z elementami cyfrowymi wykorzystuje ustalony protokół szyfrowania oraz wewnętrznie zarządzany cykl życia klucza. W odpowiedzi na nowo zidentyfikowane słabości kryptograficzne producent wprowadza aktualizację zabezpieczeń, która zastępuje istniejący mechanizm szyfrowania innym protokołem wymagającym korzystania z zewnętrznej usługi zarządzania kluczami obsługiwanej przez podmiot zewnętrzny. W wyniku tej zmiany zależności i przepływy danych w odniesieniu do produktu z elementami cyfrowymi ulegają istotnej zmianie, co powoduje wprowadzenie nowych interfejsów zewnętrznych oraz zależność od usług stron trzecich, których nie uwzględniono w ocenie ryzyka. Chociaż aktualizacja jest podyktowana względami bezpieczeństwa, wprowadza nowe ryzyko w cyberprzestrzeni, a zatem kwalifikuje się jako istotna modyfikacja.

110. Jak stwierdzono w pkt 104 powyżej, to, czy aktualizacja oprogramowania stanowi istotną modyfikację, należy oceniać indywidualnie dla każdego przypadku. Przeprowadzając tę ocenę, producenci mogą rozważyć, między innymi, czy aktualizacja oprogramowania:

a) wprowadza nowe wektory zagrożeń, takie jak dodatkowe interfejsy, kanały komunikacji, środowiska uruchomieniowe lub zależności zewnętrzne, za pośrednictwem których zagrożenia mogą się urzeczywistnić;

b) umożliwia nowe scenariusze ataków, w tym na przykład nowe sposoby, w jakie mogłoby realnie dojść do nieuprawnionego dostępu, manipulacji, ingerencji lub niewłaściwego wykorzystania produktu z elementami cyfrowymi lub przetwarzanych przez niego danych;

c) zmienia prawdopodobieństwo wcześniej zidentyfikowanych scenariuszy ataku, na przykład poprzez zmniejszenie nakładu pracy lub wiedzy specjalistycznej wymaganej do ich wykorzystania, zwiększenie narażenia na niezaufane podmioty lub osłabienie istniejących zabezpieczeń;

d) zmienia potencjalny wpływ wcześniej zidentyfikowanych scenariuszy ataku, w tym na przykład zakres danych lub funkcji, których dotyczy incydent, dotkliwość skutków operacyjnych, skutków dla bezpieczeństwa lub skutków gospodarczych, a także zdolność do wykrywania i powstrzymywania incydentu lub odtworzenia po incydencie.

111. W niektórych przypadkach aktualizacja oprogramowania nie wprowadza nowych wektorów zagrożeń, nie umożliwia nowych scenariuszy ataku i nie zmienia w istotny sposób prawdopodobieństwa wystąpienia lub wpływu wcześniej zidentyfikowanych scenariuszy ataku. Może to wskazywać, że aktualizacja nie wprowadza nowego lub zwiększonego ryzyka w cyberprzestrzeni, pod warunkiem że założenia i środki ograniczające ryzyko, na których opiera się ocena ryzyka, pozostają aktualne i skuteczne. Jest zatem prawdopodobne, że aktualizacja nie kwalifikuje się jako istotna modyfikacja.

112. Z drugiej strony aktualizacja oprogramowania może wprowadzić nowe wektory zagrożeń, umożliwić realizację nowych scenariuszy ataków lub istotnie zmienić prawdopodobieństwo wystąpienia lub wpływ istniejących scenariuszy ataków. W takich przypadkach producent powinien ponownie ocenić ryzyko w cyberprzestrzeni związane z produktem z elementami cyfrowymi i ustalić, czy zasadnicze wymagania są nadal spełniane, w tym czy aktualizacja wprowadza nowe lub zwiększone ryzyko, którego nie przewidziano w ocenie ryzyka.

113. To, czy aktualizacja oprogramowania kwalifikuje się jako istotna modyfikacja, jest istotne przy ustalaniu, czy mają zastosowanie określone obowiązki wynikające z aktu o cyberodporności, jak określono w pkt 91. Niezależnie od tej kwalifikacji producenci pozostają jednak odpowiedzialni za zapewnienie bezpieczeństwa aktualizacji oprogramowania i swojego produktu z elementami cyfrowymi w okresie wsparcia, zgodnie z wymogami dotyczącymi postępowania w przypadku wykrycia podatności określonymi w części II załącznika I do aktu o cyberodporności. Ponadto niezależnie od tego, czy aktualizacje oprogramowania kwalifikują się jako istotne modyfikacje, producenci są zobowiązani do zapewnienia dokładności, kompletności i ciągłej aktualizacji oceny ryzyka i dokumentacji technicznej, zgodnie z art. 13 ust. 7 i art. 31 ust. 2.

4.4. **Konsekwencje istotnej modyfikacji**

114. Konsekwencje istotnej modyfikacji dokonanej przez podmiot inny niż pierwotny producent produktu z elementami cyfrowymi już wprowadzonego do obrotu uwzględniono w art. 21 i 22 aktu o cyberodporności. Art. 21 dotyczy importerów i dystrybutorów, natomiast art. 22 dotyczy każdej osoby fizycznej lub prawnej innej niż producent, importer lub dystrybutor.

115. W przypadku gdy istotną modyfikację przeprowadza pierwotny producent produktu z elementami cyfrowymi, konsekwencje wynikają z ogólnie przyjętego pojęcia istotnej modyfikacji, o którym mowa w motywie 41 aktu o cyberodporności, i omówiono je bardziej szczegółowo w sekcji 2.1 Niebieskiego przewodnika. Sekcja ta stanowi, że produkt, który został poddany istotnym zmianom lub gruntownemu przeglądowi po wprowadzeniu do obrotu, należy uznać za nowy produkt, jeżeli zmieniono jego pierwotną wydajność, przeznaczenie lub typ, zmienił się charakter zagrożenia lub wzrósł poziom ryzyka, a produkt z elementami cyfrowymi jest udostępniany na rynku.

116. Ogólnie przyjętą konsekwencją jest zatem to, że w przypadku gdy modyfikacja produktu z elementami cyfrowymi kwalifikuje się jako istotna modyfikacja, a zmodyfikowany produkt z elementami cyfrowymi jest udostępniany na rynku, do celów aktu o cyberodporności należy go traktować jako nowy produkt z elementami cyfrowymi. W związku z tym udostępnienie na rynku produktu poddanego istotnej modyfikacji stanowi nowe wprowadzenie do obrotu. Ma to zastosowanie niezależnie od tego, czy istotną modyfikację przeprowadza pierwotny producent, czy inna osoba. Aby zapewnić, aby akt o cyberodporności był stosowany w sposób jednolity i proporcjonalny w odniesieniu do różnych kategorii podmiotów, które mogą dokonywać istotnych modyfikacji, w poniższych podsekcjach odniesiono się do wynikających z tego obowiązków osoby dokonującej istotnej modyfikacji przy wprowadzaniu do obrotu istotnie zmodyfikowanego produktu z elementami cyfrowymi. Konsekwencje dla okresu wsparcia produktu z elementami cyfrowymi omówiono w sekcji *5 Okres wsparcia*.

4.4.1. *Istotne modyfikacje dokonane przez osobę inną niż pierwotny producent*

117. Zgodnie z art. 21 i 22, w przypadku gdy istotna modyfikacja produktu z elementami cyfrowymi już wprowadzonego do obrotu jest dokonywana przez osobę fizyczną lub prawną inną niż producent produktu z elementami cyfrowymi, osobę, która dokonuje istotnej modyfikacji i udostępnia zmodyfikowany produkt z elementami cyfrowymi na rynku, uznaje się za producenta zmodyfikowanego produktu z elementami cyfrowymi, niezależnie od tego, czy osoba ta była zaangażowana w pierwotny projekt lub wprowadzenie tego produktu do obrotu.

118. W art. 22 doprecyzowano ponadto, że osoba dokonująca modyfikacji podlega obowiązkom określonym w art. 13 i 14 wyłącznie w odniesieniu do części produktu z elementami cyfrowymi, której dotyczy istotna modyfikacja, w przypadku gdy modyfikacja ta nie ma wpływu na cyberbezpieczeństwo produktu z elementami cyfrowymi jako całości.

119. W przypadku gdy istotna modyfikacja wpływa na zgodność z zasadniczymi wymaganiami, ale nie wpływa negatywnie na cyberbezpieczeństwo produktu z elementami cyfrowymi jako całości, osoba dokonująca modyfikacji podlega przepisom art. 13 (w tym obowiązkowi zapewnienia zgodności z zasadniczymi wymaganiami i przeprowadzenia procedury oceny zgodności) i art. 14 (obowiązki w zakresie zgłaszania) wyłącznie w odniesieniu do tej części produktu z elementami cyfrowymi, która została istotnie zmodyfikowana ([16]). Ponadto obowiązki pierwotnego producenta wynikające z aktu o cyberodporności nadal mają zastosowanie do wprowadzonego do obrotu oryginalnego produktu z elementami cyfrowymi, co zapewnia ciągłość postępowania w przypadku wykrycia podatności i zgodność w odniesieniu do niezmienionych części.

120. Przypadku istotnej modyfikacji nie należy mylić z przypadkami integracji, w których dana osoba włącza komponenty (w tym, w stosownych przypadkach, modyfikując je) do nowego produktu z elementami cyfrowymi, który sama wprowadza do obrotu. W takich przypadkach osoba integrująca nie modyfikuje produktu z elementami cyfrowymi już wprowadzonego do obrotu przez innego producenta; wprowadza ona raczej do obrotu nowy produkt z własnymi elementami cyfrowymi. Osoba integrująca jest producentem tego nowego produktu z elementami cyfrowymi w rozumieniu aktu o cyberodporności i jest zobowiązana do przestrzegania rozporządzenia w całości w odniesieniu do produktu z elementami cyfrowymi jako całości. Jeżeli producent włącza komponenty, które wchodzą w zakres aktu o cyberodporności, do swojego produktu, może on wykorzystywać działania zapewniające zgodność podejmowane przez producentów tych komponentów, aby ułatwić sobie samemu zapewnienie zgodności z aktem o cyberodporności.

Przykład 51: Przedsiębiorstwo nabywa gotowe moduły mikrokontrolerów i elementy łączności od dostawców zewnętrznych, opracowuje własne oprogramowanie układowe i pakiet czujników, a następnie montuje je w połączony z siecią produkt z elementami cyfrowymi służący do monitorowania upraw rolnych, który wprowadza do obrotu pod własną nazwą. Chociaż przedsiębiorstwo zmodyfikowało podstawowe moduły mikrokontrolerów i połączyło je z innymi komponentami, nie dokonuje istotnej modyfikacji produktu z elementami cyfrowymi już wprowadzonego do obrotu; wprowadza raczej do obrotu nowy produkt z elementami cyfrowymi. Przedsiębiorstwo jest producentem urządzenia do monitorowania upraw rolnych w rozumieniu aktu o cyberodporności i jest zobowiązane do przestrzegania przepisów rozporządzenia w odniesieniu do tego produktu jako całości.

([16]) Zgodnie z sekcją 2.1 Niebieskiego przewodnika „nie jest wymagane powtarzanie testów i tworzenie nowej dokumentacji w odniesieniu do aspektów, na które modyfikacja nie miała wpływu. Osoba fizyczna lub prawna, która dokonuje lub dokonała zmian w produkcie, musi wykazać, że nie wszystkie elementy dokumentacji produktu wymagają aktualizacji. Osoba fizyczna lub prawna, która dokonuje lub dokonała zmian w produkcie, jest odpowiedzialna za zgodność zmodyfikowanego produktu i sporządza deklarację zgodności, nawet jeśli korzysta z istniejących testów i dokumentacji produktu”.

121. W przypadku gdy istotna modyfikacja dokonana przez osobę inną niż pierwotny producent ma negatywny wpływ na cyberbezpieczeństwo produktu z elementami cyfrowymi jako całości, na przykład dlatego, że modyfikacja nie jest już ukierunkowana ani ograniczona do konkretnego komponentu lub podsystemu, zmodyfikowany produkt z elementami cyfrowymi udostępniony na rynku należy traktować jako nowy produkt z elementami cyfrowymi podlegający w całości przepisom aktu o cyberodporności. W takich przypadkach zmienił się ogólny profil ryzyka w cyberprzestrzeni tego produktu, a modyfikacji nie można ocenić bez uwzględnienia produktu z elementami cyfrowymi jako całości. Osoba dokonująca modyfikacji podlega obowiązkom producenta określonym w art. 13 i 14 w odniesieniu do zmodyfikowanego produktu z elementami cyfrowymi jako całości.

4.4.2. *Istotne modyfikacje dokonane przez pierwotnego producenta*

122. W przypadku gdy istotną modyfikację przeprowadza pierwotny producent, w tym w kontekście iteracyjnego opracowywania oprogramowania z elementami cyfrowymi, do celów aktu o cyberodporności producent ten pozostaje producentem. Produkt z elementami cyfrowymi, który został poddany istotnej modyfikacji, należy jednak uznać za nowo wprowadzony do obrotu.

123. Zgodnie z sekcją 2.1 Niebieskiego przewodnika pierwotny producent wprowadzający do obrotu istotnie zmodyfikowany produkt z elementami cyfrowymi może ponownie wykorzystać istniejącą dokumentację i wyniki testów w odniesieniu do tych aspektów produktu z elementami cyfrowymi, na które istotna modyfikacja nie ma wpływu. W szczególności w przypadku gdy producent wprowadza do obrotu istotnie zmodyfikowane wersje tego samego produktu z elementami cyfrowymi, procedura oceny zgodności powinna koncentrować się na istotnie zmodyfikowanych częściach produktu z elementami cyfrowymi. Podobnie w przypadku przeprowadzania oceny zgodności przez osobę trzecią jednostka oceniająca zgodność powinna skoncentrować swoją ocenę na istotnie zmodyfikowanych częściach. W przypadku niezmienionych części produktu z elementami cyfrowymi może ponownie wykorzystać istniejącą dokumentację i wyniki testów.

124. Względy proporcjonalności określone w poprzedniej podsekcji mają również zastosowanie do istotnych modyfikacji przeprowadzonych przez pierwotnego producenta produktu z elementami cyfrowymi wprowadzonego do obrotu przed dniem 11 grudnia 2027 r. Taka istotna modyfikacja dokonana przez pierwotnego producenta nie wymaga sama w sobie od producenta zapewnienia pełnej zgodności całego produktu z elementami cyfrowymi wprowadzonego do obrotu przed tą datą z aktem o cyberodporności, chyba że modyfikacja ta negatywnie wpływa na cyberbezpieczeństwo produktu z elementami cyfrowymi jako całości. W przypadku gdy modyfikacja nie ma wpływu na cyberbezpieczeństwo produktu z elementami cyfrowymi jako całości, obowiązki pierwotnego producenta w odniesieniu do tej modyfikacji powinny ograniczać się do części, które zostały istotnie zmodyfikowane.

5. **OKRES WSPARCIA**

125. Art. 13 ust. 8 aktu o cyberodporności nakłada na producentów obowiązek określenia okresu wsparcia, w trakcie którego zapewniają skuteczne i zgodne z zasadniczymi wymaganiami określonymi w załączniku I część II postępowanie w przypadku wykrycia podatności tego produktu lub jego komponentów. Okres wsparcia odzwierciedla czas, przez który produkt z elementami cyfrowymi ma być użytkowany (przewidywany czas użytkowania), i powinien być ustalany w świetle kryteriów określonych w art. 13 ust. 8, w szczególności uzasadnionych oczekiwań użytkowników, charakteru produktu z elementami cyfrowymi, w tym jego przeznaczenia, a także odpowiedniego prawa Unii określającego cykl życia produktów z elementami cyfrowymi ([17]). Ogólnie rzecz biorąc, kryteria te należy uwzględniać w sposób zapewniający proporcjonalność przy określaniu okresu wsparcia.

([17]) Dodatkowe kryteria, które można uwzględnić zgodnie z art. 13 ust. 8, obejmują 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 w ramach aktu o cyberodporności (grupę ADCO) i Komisję.

126. W art. 13 ust. 8 wymaga się ponadto, aby okres wsparcia wynosił co najmniej pięć lat, chyba że oczekuje się, że produkt z elementami cyfrowymi będzie użytkowany krócej niż pięć lat, w którym to przypadku okres wsparcia odpowiada przewidywanemu czasowi użytkowania. Minimalny okres wsparcia pełni zatem jedynie funkcję zabezpieczającą, zapewniając, aby podatności były usuwane przez wystarczająco długi czas, a jednocześnie umożliwiając producentom uwzględnienie produktów z elementami cyfrowymi o rzeczywiście krótszym przewidywanym czasie użytkowania. W motywie 60 przedstawiono więcej wytycznych w tym zakresie, wyjaśniając, że produkty z elementami cyfrowymi, co do których można zasadnie oczekiwać, że będą używane dłużej niż pięć lat, powinny odpowiednio mieć dłuższe okresy wsparcia. Okres wsparcia wynoszący pięć lat nie powinien zatem być traktowany jako domyślny dla wszystkich produktów z elementami cyfrowymi. Zamiast tego producent powinien określić odpowiedni okres wsparcia w świetle kryteriów, o których mowa w art. 13 ust. 8.

127. W art. 13 ust. 19 nakłada się na producentów obowiązek podania w momencie zakupu, w jasny i zrozumiały sposób, daty zakończenia okresu wsparcia (co najmniej miesiąc i rok). Wymaga się w nim również, aby producenci wyświetlali użytkownikom powiadomienie informujące ich, że zakończył się okres wsparcia, jeżeli jest to technicznie wykonalne ze względu na charakter produktu z elementami cyfrowymi. Obowiązek ten ma na celu zapewnienie użytkownikom przejrzystości w sprawie okresu, przez jaki mogą liczyć na wsparcie w zakresie bezpieczeństwa.

128. W przypadku oprogramowania z elementami cyfrowymi, które jest często opracowywane i udostępniane w sposób iteracyjny i w przypadku którego z biegiem czasu mogą być często wprowadzane do obrotu wersje poddane istotnym modyfikacjom, okres wsparcia należy rozumieć w kontekście tego modelu rozwoju. Każda istotnie zmodyfikowana wersja wprowadzonego do obrotu oprogramowania z elementami cyfrowymi musi mieć deklarowany okres wsparcia zgodny z art. 13 ust. 8. Obejmuje to minimalny okres wsparcia wynoszący co najmniej pięć lat, chyba że przewidywany czas korzystania z tej wersji jest wyraźnie krótszy, co wyjaśniono również w motywie 60. W sekcji *5.1 Istotne modyfikacje i okres wsparcia* wyjaśniono ponadto, że jeżeli istotna modyfikacja nie prowadzi do zmian czynników, które pierwotnie określały przewidywany czas użytkowania produktu z elementami cyfrowymi, nie ma to wpływu na pierwotny okres wsparcia (tj. również w przypadkach, gdy pozostały okres wsparcia jest krótszy niż pięć lat).

129. W art. 13 ust. 10 zapewniono elastyczność w odniesieniu do oprogramowania z elementami cyfrowymi, umożliwiając producentom, pod pewnymi warunkami, zapewnienie zgodności z wymogiem dotyczącym postępowania w przypadku wykrycia podatności określonym w załączniku I część II pkt 2 (reagowanie na podatności i ich eliminowanie) wyłącznie w odniesieniu do wersji oprogramowania z elementami cyfrowymi, która jako ostatnia została wprowadzona do obrotu. Jest to dozwolone, jeżeli użytkownicy wcześniej wprowadzonych wersji mają bezpłatny dostęp do wersji ostatnio wprowadzonej do obrotu i nie ponoszą dodatkowych kosztów związanych z dostosowaniem środowiska sprzętowego i oprogramowania, w którym korzystają z pierwotnej wersji tego produktu.

130. Do celów art. 13 ust. 10 pojęcie „dodatkowych kosztów" należy interpretować w sposób praktyczny i proporcjonalny, z uwzględnieniem normalnych i oczekiwanych praktyk w zakresie konserwacji i eksploatacji oprogramowania. Nie obejmuje to uzasadnionego nakładu pracy związanego z wdrażaniem aktualizacji oprogramowania lub utrzymaniem bezpiecznego środowiska operacyjnego, takiego jak czas pracy personelu, rutynowe testy, dostosowania konfiguracji lub aktualizacje zależności oprogramowania bazowego, które są niezbędne do wyeliminowania komponentów wycofanych z eksploatacji lub znanych luk w zabezpieczeniach. Natomiast „dodatkowe koszty" odnoszą się do obciążeń, które wykraczają poza to, czego można zwykle oczekiwać w kontekście aktualizacji oprogramowania, takich jak obowiązkowy zakup nowego sprzętu, wymiana infrastruktury lub zasadnicze zmiany w środowisku operacyjnym.

131. W przypadku stale zmieniającego się oprogramowania z elementami cyfrowymi producenci mogą wprowadzać do obrotu kolejne istotnie zmodyfikowane wersje w stosunkowo krótkich odstępach czasu i oczekiwać, że użytkownicy będą regularnie aktualizować to oprogramowanie. W takich przypadkach zadeklarowany okres wsparcia dla każdej istotnie zmodyfikowanej wersji musi być zgodny z art. 13 ust. 8 w momencie wprowadzenia jej do obrotu. Innymi słowy, producent musi zadeklarować nowy okres wsparcia dla tej istotnie zmodyfikowanej wersji. Producenci mogą jednak oprzeć się na art. 13 ust. 10, aby zaprzestać reagowania na podatności i ich eliminowania w odniesieniu do wcześniejszych wersji, gdy użytkownicy będą mogli bezpłatnie i bez ponoszenia

dodatkowych kosztów, o których mowa powyżej, przejść na nowszą wersję, nawet jeśli spowoduje to skrócenie faktycznego okresu wsparcia dla tych starszych wersji ([18]). Producent nadal podlega innym wymaganiom dotyczącym postępowania w przypadku wykrycia podatności określonym w załączniku I część II, a także obowiązkom w zakresie zgłaszania określonym w art. 14. Jak wyjaśniono również w motywie 40, wymagania te obejmują między innymi, w odniesieniu do wszystkich kolejnych, istotnie zmodyfikowanych wersji wprowadzonego do obrotu oprogramowania z elementami cyfrowymi: (i) utrzymywanie polityki skoordynowanego ujawniania podatności; oraz (ii) środki ułatwiające wymianę informacji na temat potencjalnych podatności ([19]).

Przykład 52: Producent wprowadza model smartfona do obrotu w UE i deklaruje okres wsparcia wynoszący X lat od daty wprowadzenia do obrotu, podczas którego zapewni aktualizacje zabezpieczeń w celu wyeliminowania podatności. W tym okresie producent udostępnia regularne aktualizacje oprogramowania i istotnie zmodyfikowane wersje systemu operacyjnego, które użytkownicy mogą instalować bezpłatnie bez konieczności zakupu nowego sprzętu.

Producent może, zgodnie z art. 13 ust. 10, reagować na podatności i eliminować je w najnowszej wersji systemu operacyjnego udostępnionej dla danego modelu smartfona, pod warunkiem że wcześniejsze wersje można aktualizować bezpłatnie i bez dodatkowych kosztów. Przez cały okres wsparcia producent nadal podlega innym wymaganiom dotyczącym postępowania w przypadku wykrycia podatności, takim jak skoordynowane ujawnianie podatności i środki wymiany informacji.

Przykład 53: Producent wprowadza do obrotu oprogramowanie z elementami cyfrowymi skierowane do przedsiębiorstw i co kilka miesięcy udostępnia jego istotnie zmodyfikowane wersje, odzwierciedlające poprawę bezpieczeństwa, nowe funkcje i kompatybilność ze zaktualizowanymi systemami operacyjnymi i platformami. Każda wersja jest wprowadzana do obrotu z zadeklarowanym okresem wsparcia zgodnie z art. 13 ust. 8. Producent oczekuje, że użytkownicy będą regularnie aktualizować oprogramowanie w ramach normalnego użytkowania, i zapewnia bezpłatny dostęp do najnowszej wersji. Zastosowanie aktualizacji może wymagać racjonalnego wysiłku operacyjnego, takiego jak testowanie lub dostosowanie konfiguracji, ale nie wymaga poniesienia dodatkowych kosztów, takich jak zakup nowego sprzętu lub zasadnicze zmiany infrastruktury. W tym kontekście producent może oprzeć się na art. 13 ust. 10, aby zaprzestać reagowania na podatności i ich eliminowania w odniesieniu do wcześniejszych wersji, gdy użytkownicy będą mogli zaktualizować wersję do najnowszej, a jednocześnie nadal spełniać pozostałe wymagania dotyczące postępowania w przypadku wykrycia podatności w odniesieniu do wszystkich kolejnych istotnie zmodyfikowanych wersji.

5.1. **Istotne modyfikacje i okres wsparcia**

132. Jak określono w sekcji 4.4 *Konsekwencje istotnej modyfikacji*, w przypadku gdy modyfikacja produktu z elementami cyfrowymi kwalifikuje się jako istotna modyfikacja, a zmodyfikowany produkt z elementami cyfrowymi jest udostępniany na rynku, do celów aktu o cyberodporności należy go traktować jako nowy produkt, a udostępnienie na rynku istotnie zmodyfikowanego produktu z elementami cyfrowymi stanowi nowe wprowadzenie do obrotu. Warto zatem wyjaśnić, jaki wpływ to nowe wprowadzenie do obrotu ma na okres wsparcia w przypadku produktu z elementami cyfrowymi poddanego istotnej modyfikacji.

133. Okres wsparcia dla istotnie zmodyfikowanego produktu z elementami cyfrowymi należy określić przez odniesienie do przewidywanego czasu użytkowania tego produktu w świetle kryteriów określonych w art. 13 ust. 8 aktu o cyberodporności. Istotna modyfikacja powinna zatem wymagać ponownej oceny pod kątem tych kryteriów, ale nie prowadzi ona automatycznie do zresetowania, a nawet przedłużenia okresu wsparcia. Istotną kwestią jest to, czy istotna modyfikacja wpływa na czynniki, które pierwotnie determinowały przewidywany czas użytkowania tego produktu, a tym samym pierwotny okres wsparcia.

([18]) Należy przypomnieć, że w art. 13 ust. 19 nakłada się na producentów obowiązek, jeżeli jest to technicznie wykonalne ze względu na charakter produktu z elementami cyfrowymi, wyświetlania użytkownikom powiadomienia informującego ich, że zakończył się okres wsparcia ich produktu z elementami cyfrowymi. W związku z tym oczekuje się, że w przypadku zaprzestania reagowania na podatności i ich eliminowania we wcześniejszych wersjach użytkownicy, którzy nie zaktualizowali swojej wersji do najnowszej, zostaną o tym poinformowani, jeżeli jest to technicznie wykonalne.

([19]) Należy zauważyć, że w przypadku gdy użytkownicy mogą przejść na najnowszą wersję oprogramowania bez dodatkowych kosztów, producenci mogą jednak zdecydować się na dalsze reagowanie na podatności i ich eliminowanie we wcześniejszych wersjach tego oprogramowania, w tym za opłatą lub na podstawie innych uzgodnień handlowych. Akt o cyberodporności nie wymaga od producentów bezpłatnego dostarczania aktualizacji zabezpieczeń dla takich wcześniejszych wersji.

134. W przypadku gdy istotna modyfikacja nie ma wpływu na te czynniki, kryteria określone w art. 13 ust. 8 nadal wskazują taki sam przewidywany czas użytkowania jak pierwotnie ustalony, a okres wsparcia zmodyfikowanego produktu z elementami cyfrowymi powinien być dostosowany do pozostałego przewidywanego czasu użytkowania produktu w postaci, w jakiej został on pierwotnie wprowadzony do obrotu. Zazwyczaj ma to miejsce w sytuacji, gdy przewidywany czas użytkowania był określony przede wszystkim przez czynniki, których modyfikacja nie zmienia, takie jak fizyczna trwałość komponentów sprzętu, jeżeli istotna modyfikacja dotyczy wyłącznie funkcji oprogramowania lub usług zaplecza.

Przykład 54*: Producent wprowadza do obrotu odkurzacz automatyczny o przewidywanym czasie użytkowania wynoszącym X lat, określonym na podstawie charakteru produktu z elementami cyfrowymi, w tym trwałości fizycznej i charakterystyki zużycia elementów sprzętowych, oraz z uwzględnieniem uzasadnionych oczekiwań użytkowników co do cyklu życia tego produktu. Producent ustala okres wsparcia technicznego na X lat. Po upływie Y lat producent udostępnia aktualizację oprogramowania, która kwalifikuje się jako istotna modyfikacja, dodając nowe tryby czyszczenia i funkcje nawigacyjne. Aktualizacja oprogramowania nie ma wpływu na fizyczną trwałość sprzętu ani nie zmienia uzasadnionych oczekiwań użytkowników co do cyklu życia tego produktu. Kryteria określone w art. 13 ust. 8 nadal wskazują zatem taki sam przewidywany czas użytkowania. Okres wsparcia dla zmodyfikowanego produktu z elementami cyfrowymi jest zgodny z pozostałym przewidywanym czasem użytkowania, który został pierwotnie określony.*

Przykład 55: Producent wprowadza do obrotu złożony produkt w postaci maszyny przemysłowej z elementami cyfrowymi z zapleczem w chmurze, które stanowi rozwiązanie do zdalnego przetwarzania danych. Przewidywany czas użytkowania wynosi X lat i jest określany w oparciu o uzasadnione oczekiwania użytkowników oraz charakter produktu z elementami cyfrowymi, takie jak fizyczna trwałość sprzętu maszyny i przewidywane zużycie. Okres wsparcia ustalono tak, aby odpowiadał temu przewidywanemu okresowi użytkowania wynoszącemu X lat. Po upływie Y lat producent przebudowuje zaplecze w chmurze (rozwiązanie do zdalnego przetwarzania danych), wprowadzając nowe interfejsy API i przepływy danych w sposób, który kwalifikuje się jako istotna modyfikacja produktu z elementami cyfrowymi, ale nie zmienia charakteru tego produktu ani nie wpływa na oczekiwania użytkowników. Kryteria określone w art. 13 ust. 8 nadal wskazują zatem taki sam przewidywany czas użytkowania. Okres wsparcia dla zmodyfikowanego produktu z elementami cyfrowymi jest zgodny z pozostałym przewidywanym czasem użytkowania, który został pierwotnie określony.

135. W przypadku gdy istotna modyfikacja wpływa na czynniki, które pierwotnie determinowały przewidywany czas użytkowania produktu z elementami cyfrowymi, producent powinien ponownie obliczyć okres wsparcia, aby odzwierciedlić nowy przewidywany czas użytkowania, stosując odpowiednio kryteria określone w art. 13 ust. 8. Może tak być na przykład w przypadku modyfikacji sprzętu służących modernizacji, które wydłużają okres eksploatacji tego produktu, lub znacznego przeprogramowania lub przepisania podstawowego oprogramowania tego produktu, co w znacznym stopniu zmienia jego przewidywany czas użytkowania ([20]).

Przykład 56: Producent wprowadza do obrotu programowalny sterownik logiczny (PLC) o przewidywanym czasie użytkowania wynoszącym X lat, określonym przede wszystkim na podstawie charakteru produktu z elementami cyfrowymi i trwałości sprzętu, na którym opiera się urządzenie. Okres wsparcia ustala się odpowiednio do tego czasu. Kilka lat po pierwszym wprowadzeniu do obrotu producent dokonuje istotnej modyfikacji polegającej na zastąpieniu wbudowanej platformy obliczeniowej sterownika PLC, w tym procesora, pamięci i środowiska uruchomieniowego, nową generacją komponentów zaprojektowanych na znacznie dłuższy okres eksploatacji. W wyniku tej modyfikacji zmieniają się uzasadnione oczekiwania użytkowników i charakter produktu z elementami cyfrowymi: użytkownik sterownika PLC może obecnie zasadnie oczekiwać, że sterownik będzie nadal produktywnie użytkowany po pierwotnie zadeklarowanym przewidywanym czasie użytkowania, przy wsparciu nowej platformy obliczeniowej. Kryteria określone w art. 13 ust. 8 wskazują zatem na dłuższy przewidywany czas użytkowania, a producent odpowiednio ponownie oblicza okres wsparcia dla tego konkretnego sterownika PLC.

6. **WAŻNE I KRYTYCZNE PRODUKTY Z ELEMENTAMI CYFROWYMI**

136. Art. 7 ust. 1 aktu o cyberodporności stanowi, że produkty z elementami cyfrowymi, które posiadają podstawową funkcjonalność kategorii produktów określonej w załączniku III do rozporządzenia, uznaje się za „ważne produkty z elementami cyfrowymi". W załączniku III dokonano dalszego podziału ważnych produktów z elementami cyfrowymi na klasę I i II. Podobnie art. 8 ust. 1 stanowi, że produkty z elementami cyfrowymi, które posiadają podstawową funkcjonalność kategorii produktów określonej w załączniku IV do aktu o cyberodporności, uznaje się za „produkty krytyczne z elementami cyfrowymi" ([21]).

([20]) Należy przypomnieć, że – jak wskazano w sekcji 4.*1 Naprawy fizyczne* – działań związanych z odnawianiem, konserwacją lub naprawą zasadniczo nie uznaje się za istotne modyfikacje.

([21]) W rozporządzeniu wykonawczym Komisji (UE) 2025/2392 określono opis techniczny kategorii ważnych i krytycznych produktów.

137. Klasyfikacja produktu z elementami cyfrowymi jako ważnego lub krytycznego lub, przeciwnie, jako należącego do kategorii „domyślnej" ([22]) ma znaczenie przy określaniu procedury oceny zgodności, której producent musi przestrzegać zgodnie z art. 32, zanim będzie mógł wprowadzić ten produkt z elementami cyfrowymi do obrotu. Co istotne, w przypadku produktów z elementami cyfrowymi należących do kategorii domyślnej zawsze można stosować procedurę kontroli wewnętrznej zgodnie z modułem A („samoocena") ([23]). Ważne produkty z elementami cyfrowymi klasy I lub II oraz produkty krytyczne z elementami cyfrowymi podlegają bardziej rygorystycznym procedurom oceny zgodności. Nie obejmuje to wprowadzanych do obrotu ważnych produktów z elementami cyfrowymi klasy I lub II kwalifikujących się jako wolne i otwarte oprogramowanie, w przypadku których zgodnie z art. 32 ust. 5 producenci mogą stosować procedury przewidziane dla kategorii domyślnej.

138. Pojęcie podstawowej funkcjonalności ma zatem zasadnicze znaczenie dla producenta przy określaniu mającego zastosowanie systemu oceny zgodności. Pojęcie to nie zostało jednak wyraźnie zdefiniowane w akcie o cyberodporności. Produkty z elementami cyfrowymi mogą pełnić szereg funkcji, z których część może mieć charakter pomocniczy w stosunku do podstawowej funkcjonalności tego produktu, i nie powinny one mieć wpływu na klasyfikację produktu jako domyślnego, ważnego klasy I, ważnego klasy II lub krytycznego. W związku z tym wskazane jest przedstawienie dodatkowych wytycznych, aby pomóc producentom w prawidłowym przeprowadzaniu odpowiednich procedur oceny zgodności oraz ułatwić organom nadzoru rynku zapewnienie zharmonizowanego egzekwowania aktu o cyberodporności w całej UE.

6.1. **Podstawowa funkcjonalność**

139. Podstawowa funkcjonalność produktu z elementami cyfrowymi odnosi się do głównych cech i możliwości technicznych tego produktu, bez których nie byłby on w stanie spełniać swojego przeznaczenia. Można ją ocenić w świetle konkretnego kontekstu i warunków użytkowania tego produktu, biorąc pod uwagę między innymi informacje podawane przez producenta w instrukcji obsługi, materiałach promocyjnych lub sprzedażowych oraz oświadczeniach, a także w dokumentacji technicznej.

Przykład 57: Oprogramowanie z elementami cyfrowymi zapewnia warstwę abstrakcji nad sprzętem, na którym jest zainstalowane, i zarządza wykonywaniem komponentów oprogramowania. Jego główne funkcje obejmują inicjalizację sprzętu i urządzeń peryferyjnych, zarządzanie procesami i pamięcią, kontrolę wejścia-wyjścia, szeregowanie zadań, alokację zasobów oraz udostępnianie usług systemowych i interfejsów programowania aplikacji (API), za pośrednictwem których aplikacje wchodzą w interakcję ze sprzętowymi i programowymi zasobami urządzenia. W dokumentacji technicznej wskazano, że produkt z elementami cyfrowymi koordynuje zasoby obliczeniowe, wymusza konfigurację systemu i zapewnia standaryzowane interfejsy dla modułów oprogramowania i podłączonych urządzeń peryferyjnych. Producent podkreśla, że te możliwości pozwalają platformie pełnić rolę centralnego środowiska oprogramowania, w którym aplikacje mogą działać w sposób niezawodny. Produkt z elementami cyfrowymi posiada podstawową funkcjonalność systemu operacyjnego, zgodnie z opisem w załączniku I pkt 11 do rozporządzenia wykonawczego (UE) 2025/2392.

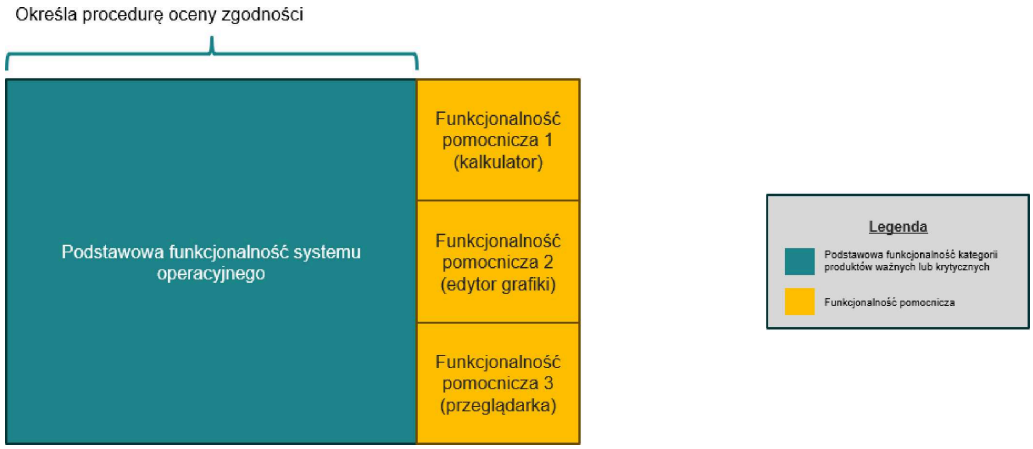
140. Funkcjonalność produktu z elementami cyfrowymi rzadko ogranicza się wyłącznie do jego podstawowej funkcjonalności, ponieważ produkty z elementami cyfrowymi często – jeśli nie zawsze – pełnią dodatkowe funkcje, które nie przyczyniają się do realizacji podstawowej funkcjonalności produktu. Może to również obejmować włączenie komponentów, które same posiadają funkcjonalność innego ważnego lub krytycznego produktu z elementami cyfrowymi. Fakt, że produkt z elementami cyfrowymi pełni funkcje inne niż funkcje wyszczególnione w opisach technicznych ważnych lub krytycznych produktów z elementami cyfrowymi lub dodatkowe w stosunku do tych funkcji, sam w sobie nie uniemożliwia jednak posiadania przez produkt jednej z takich podstawowych funkcjonalności.

([22]) Termin kategoria „domyślna" nie jest terminem zdefiniowanym w akcie o cyberodporności. Termin ten, użyty w niniejszym dokumencie, odnosi się do produktów z elementami cyfrowymi, które nie posiadają podstawowej funkcjonalności kategorii produktu określonej w załącznikach III lub IV do aktu o cyberodporności i które w związku z tym podlegają systemowi oceny zgodności określonemu w art. 32 ust. 1.

([23]) Producent może jednak zawsze zdecydować się na zastosowanie bardziej rygorystycznej procedury oceny zgodności, jak określono w art. 32 ust. 1.

Rys. 2:

Ilustracja pokazująca, jak o wyborze mającej zastosowanie procedury oceny zgodności decyduje funkcjonalność podstawowa, a nie funkcjonalności pomocnicze



141. Produkt z elementami cyfrowymi może posiadać zdolność do pełnienia funkcji charakterystycznych dla kategorii produktów ważnych lub krytycznych, ale mimo to jego podstawowa funkcjonalność może różnić się od funkcjonalności produktów należących do tej kategorii. W takich przypadkach produkt z elementami cyfrowymi nie kwalifikuje się jako ważny lub krytyczny produkt z elementami cyfrowymi. Jak wyraźnie stwierdzono w art. 7 ust. 1 aktu o cyberodporności w odniesieniu do ważnych produktów z elementami cyfrowymi (i stosując tę samą logikę w przypadku produktów krytycznych z elementami cyfrowymi), sama integracja ważnego lub krytycznego produktu z elementami cyfrowymi nie sprawia, że produkt z elementami cyfrowymi staje się ważnym lub krytycznym produktem z elementami cyfrowymi.

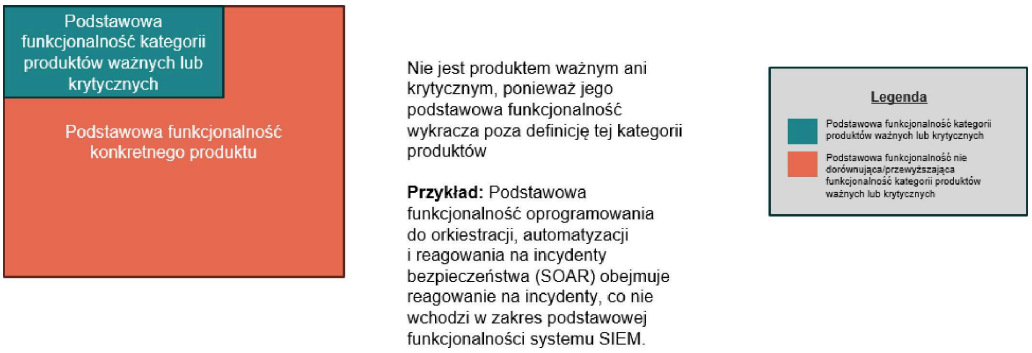
Przykład 58: Smartfon posiada system operacyjny zapewniający funkcje opisane w załączniku I pkt 11 do rozporządzenia wykonawczego (UE) 2025/2392. Podczas gdy system operacyjny umożliwia zarządzanie zasobami sprzętowymi i korzystanie z aplikacji, smartfon jako całość posiada inną podstawową funkcjonalność (np. umożliwia użytkownikom komunikację oraz dostęp do informacji i usług). Sama obecność systemu operacyjnego nie oznacza, że smartfon posiada podstawową funkcjonalność systemu operacyjnego.

142. Niektóre produkty z elementami cyfrowymi mogą być podobne do produktów z kategorii ważnych lub krytycznych albo należeć do tej samej ogólnej rodziny produktów, jednak ich podstawowa funkcjonalność może znacznie przekraczać podstawową funkcjonalność tej kategorii lub znacznie odbiegać od niej. Nie ma to miejsca w przypadku, gdy produkt z elementami cyfrowymi zawiera dodatkowe funkcje, które jedynie uzupełniają lub wzmacniają podstawową funkcjonalność, która sama odpowiada funkcjonalności produktów z kategorii ważnych lub krytycznych; w takich przypadkach produkt z elementami cyfrowymi zachowuje podstawową funkcjonalność tej kategorii i jest odpowiednio klasyfikowany. Ocena ta powinna opierać się na głównych cechach i możliwościach technicznych tego produktu, rozpatrywanych obiektywnie w świetle jego przeznaczenia, a nie na sposobie, w jaki produkt z elementami cyfrowymi jest opisywany lub wprowadzany do obrotu, jeżeli opis ten nie odzwierciedla rzeczywistych właściwości technicznych produktu.

Przykład 59: Oprogramowanie do orkiestracji, automatyzacji i reagowania na incydenty bezpieczeństwa (SOAR) często ma zdolność do pełnienia funkcji produktów z elementami cyfrowymi w kategorii „systemy zarządzania informacjami i zdarzeniami zabezpieczeń (SIEM)", takich jak gromadzenie danych z wielu źródeł, analizowanie i korelowanie tych danych oraz prezentowanie ich jako informacji możliwych do zastosowania do celów związanych z bezpieczeństwem. Podstawowa funkcjonalność oprogramowania znacznie przekracza jednak funkcjonalność SIEM, obejmując usługi takie jak reagowanie na incydenty jako podstawowe elementy jego zdolności technicznych. W związku z tym zasadniczo nie uznaje się, że oprogramowanie SOAR posiada podstawową funkcjonalność systemów SIEM.

Rys. 3:

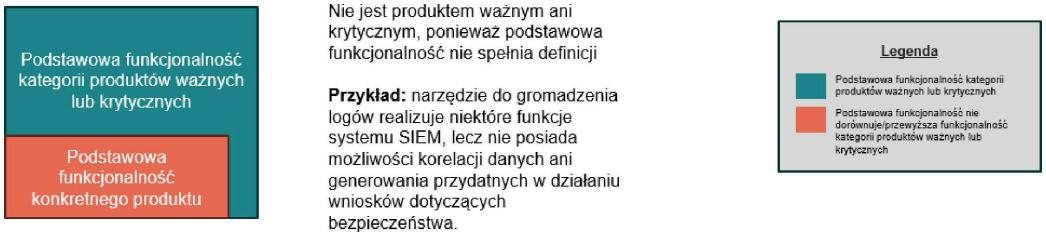
Ilustracja przedstawiająca sytuację, w której podstawowa funkcjonalność produktu z elementami cyfrowymi znacznie wykracza poza definicję kategorii produktów ważnych lub krytycznych



Przykład 60: Niektóre narzędzia do gromadzenia i wizualizacji rejestrów umożliwiają pobieranie danych z rejestrów i prezentowanie podstawowych pulpitów nawigacyjnych przedstawiających zdarzenia systemowe. Chociaż narzędzia te mogą wspierać działania w zakresie monitorowania bezpieczeństwa, ich podstawowa funkcjonalność nie dorównuje funkcjonalności systemów SIEM, ponieważ nie przeprowadzają one korelacji danych ani nie dostarczają przydatnych informacji dotyczących bezpieczeństwa. W związku z tym zasadniczo nie uznaje się, że takie narzędzia posiadają podstawową funkcjonalność systemów SIEM.

Rys. 4:

Ilustracja przedstawiająca podstawową funkcjonalność produktu z elementami cyfrowymi, która znacznie odbiega od definicji kategorii produktów ważnych lub krytycznych

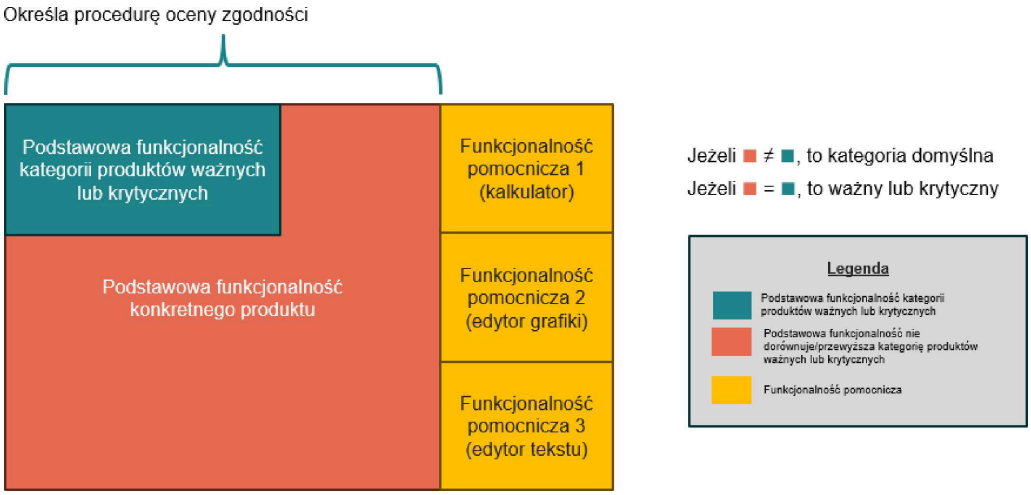


143. Producent nie może błędnie przedstawiać podstawowej funkcjonalności swojego produktu z elementami cyfrowymi w taki sposób, aby uniknąć objęcia systemem oceny zgodności mającym zastosowanie do ważnych lub krytycznych produktów z elementami cyfrowymi, np. poprzez nadmierne podkreślanie lub bagatelizowanie roli niektórych funkcji, tak aby produkt znacznie przekraczał daną podstawową funkcjonalność lub jej nie spełniał. Miałoby to miejsce na przykład w przypadku wyraźnych niespójności między materiałami promocyjnymi, instrukcją obsługi i dokumentacją techniczną.

144. Produkt z elementami cyfrowymi może posiadać nie więcej niż jedną podstawową funkcjonalność do celów określenia mającego zastosowanie systemu oceny zgodności. Zgodnie z załącznikiem VII do aktu o cyberodporności w dokumentacji technicznej produktu producenci są zobowiązani do opisania przeznaczenia swojego produktu z elementami cyfrowymi oraz procedury oceny zgodności, którą zastosowali. Należy zatem jasno określić podstawową funkcjonalność produktu. Umożliwia to prawidłową identyfikację mającego zastosowanie systemu oceny zgodności i umożliwia organom nadzoru rynku nadzorowanie i sprawdzanie, czy rozporządzenie jest prawidłowo stosowane.

Rys. 5:

Ilustracja sposobu, w jaki podstawowa funkcjonalność konkretnego produktu z elementami cyfrowymi określa klasę produktu, a tym samym mającą zastosowanie procedurę oceny zgodności



145. Niektóre produkty z elementami cyfrowymi są wprowadzane do obrotu jako pojedyncze produkty z elementami cyfrowymi, ale składają się z odrębnych modułów o odrębnych funkcjach. Jeżeli producent również udostępnia te moduły na rynku oddzielnie, na przykład w przypadku, gdy są one oferowane do odrębnego zakupu, na podstawie licencji lub w ramach subskrypcji, moduły te same w sobie stanowią samodzielne produkty z elementami cyfrowymi. W związku z tym należy je klasyfikować na podstawie ich odpowiednich podstawowych funkcjonalności (a zatem powinny one podlegać odpowiedniemu systemowi oceny zgodności na podstawie podstawowej funkcjonalności każdego modułu). Pozostaje to bez uszczerbku dla modułów dostarczanych wyłącznie jako komponenty zintegrowanego produktu z elementami cyfrowymi i nieudostępnianych oddzielnie; w takich przypadkach podstawową funkcjonalność określa się na poziomie zintegrowanego produktu z elementami cyfrowymi.

Przykład 61: Producent wprowadza do obrotu ujednolicony pakiet zabezpieczeń łączący wiele modułów, w tym SIEM, system wykrywania włamań i moduł analityczny. Producent oferuje również te moduły w ramach oddzielnych subskrypcji. W tym scenariuszu każdy moduł stanowi odrębny produkt z elementami cyfrowymi i jest klasyfikowany na podstawie swojej własnej podstawowej funkcjonalności. Moduł SIEM podlega systemowi oceny zgodności dla ważnych produktów z elementami cyfrowymi klasy I, ponieważ jego podstawowa funkcjonalność odpowiada funkcjonalności „Systemy zarządzania informacjami i zdarzeniami zabezpieczeń (SIEM)". System wykrywania włamań podlega systemowi oceny zgodności dla ważnych produktów z elementami cyfrowymi klasy II, ponieważ jego podstawowa funkcjonalność odpowiada funkcjonalności „Zapory sieciowe, systemy wykrywania włamań lub zapobiegania włamaniom". Moduł analityczny podlega systemowi oceny zgodności dla „domyślnych" produktów z elementami cyfrowymi, ponieważ jego podstawowa funkcjonalność nie odpowiada funkcjonalności produktów z kategorii ważnych lub krytycznych.

146. Niezgodność z obowiązkami określonymi w art. 32 aktu o cyberodporności może skutkować nałożeniem administracyjnych kar pieniężnych zgodnie z art. 64 ust. 3.

6.2. Ocena zgodności ważnych i krytycznych produktów z elementami cyfrowymi

147. Po określeniu podstawowej funkcjonalności swojego produktu z elementami cyfrowymi producent musi przeprowadzić jedną z mających zastosowanie procedur oceny zgodności. Producent musi zapewnić, aby produkt z elementami cyfrowymi jako całość spełniał zasadnicze wymagania, biorąc pod uwagę, w stosownych przypadkach, bezpieczeństwo włączonych do niego komponentów lub funkcji.

148. Bardziej rygorystyczna procedura oceny zgodności z udziałem strony trzeciej (zgodnie z modułem B+C, modułem H lub programami certyfikacji cyberbezpieczeństwa) jest obowiązkowa w przypadku ważnych produktów z elementami cyfrowymi klasy II (z wyjątkiem produktów kwalifikujących się jako wolne i otwarte oprogramowanie zgodnie z art. 32 ust. 5) oraz w przypadku produktów krytycznych z elementami cyfrowymi ([24]). Natomiast ważne produkty z elementami cyfrowymi klasy I (z wyjątkiem produktów kwalifikujących się jako wolne i otwarte oprogramowanie zgodnie z art. 32 ust. 5) muszą zostać poddane procedurze oceny zgodności przeprowadzanej przez stronę trzecią tylko wtedy, gdy producent nie zastosował odpowiednich norm zharmonizowanych, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej* (zwanych dalej „normami zharmonizowanymi"), wspólnych specyfikacji lub europejskich programów certyfikacji cyberbezpieczeństwa co najmniej na „istotnym" poziomie uzasadnienia, lub zastosował je tylko częściowo ([25]).

149. W związku z tym, aby ważny produkt z elementami cyfrowymi klasy I kwalifikował się do procedury kontroli wewnętrznej, (i) należy zastosować wszystkie mające zastosowanie wymogi odpowiedniej normy zharmonizowanej; oraz (ii) zakres normy musi obejmować co najmniej wszystkie rodzaje ryzyka w cyberprzestrzeni związane z podstawową funkcjonalnością tego produktu.

150. Zakres produktu z elementami cyfrowymi może być szerszy niż zakres przewidziany w odpowiedniej normie zharmonizowanej, a takie dodatkowe funkcje mogą stwarzać inne lub dodatkowe ryzyko w cyberprzestrzeni. Producent jest zawsze zobowiązany do przeprowadzenia oceny ryzyka zgodnie z art. 13 ust. 2 i w związku z tym powinien sprawdzić, czy wdrożenie normy zharmonizowanej obejmuje wszystkie rodzaje ryzyka związane z produktem z elementami cyfrowymi. W przypadku gdy wdrożenie normy nie obejmuje wszystkich rodzajów ryzyka, producent powinien zapewnić za pomocą innych środków, aby jego produkt z elementami cyfrowymi był zgodny z zasadniczymi wymaganiami.

151. W związku z tym, jeżeli producent ważnego produktu z elementami cyfrowymi klasy I zastosował odpowiednią normę zharmonizowaną, która obejmuje ryzyko związane z podstawową funkcjonalnością tego produktu, może zdecydować się na skorzystanie z procedury kontroli wewnętrznej w celu wykazania zgodności swojego produktu. W ramach swoich działań w zakresie oceny zgodności producent będzie nadal zobowiązany do wykazania, że uwzględniono wszystkie rodzaje ryzyka mające zastosowanie do jego produktu z elementami cyfrowymi. W związku z tym, jeżeli istnieje rozbieżność między zakresem normy zharmonizowanej a zakresem produktu z elementami cyfrowymi jako całości, producent nadal musi udokumentować, jakie dodatkowe środki wprowadził w celu przeciwdziałania tym rodzajom ryzyka.

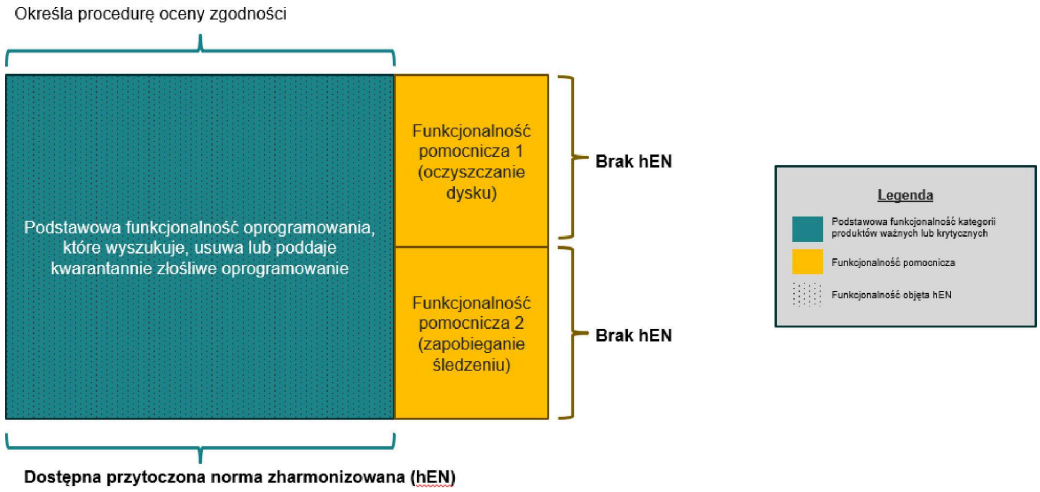
Przykład 62: Oprogramowanie antywirusowe posiada podstawową funkcjonalność oprogramowania, które wyszukuje, usuwa lub poddaje kwarantannie złośliwe oprogramowanie, jak opisano w załączniku I pkt 4 do rozporządzenia wykonawczego (UE) 2025/2392. Ten produkt z elementami cyfrowymi posiada również dodatkowe cechy, a mianowicie funkcję czyszczenia dysku i funkcję przeciwdziałania śledzeniu, chroniącą użytkownika podczas poruszania się w sieci. Producent przeprowadza ocenę ryzyka obejmującą produkt z elementami cyfrowymi w całości, w tym podstawową funkcjonalność programu antywirusowego, funkcję czyszczenia dysku oraz funkcję zapobiegania śledzeniu. Stosuje on normę zharmonizowaną obejmującą ryzyko związane z podstawową funkcjonalnością programu antywirusowego oraz dodatkowe środki w celu przeciwdziałania ryzyku wynikającemu z dodatkowych funkcji. Producent może korzystać z procedury kontroli wewnętrznej na potrzeby oceny zgodności, obejmującej produkt z elementami cyfrowymi jako całość, w tym funkcję czyszczenia dysku i funkcję zapobiegania śledzeniu.

([24]) Dotyczy to również korzystania z europejskiego systemu certyfikacji cyberbezpieczeństwa co najmniej na „istotnym" poziomie uzasadnienia, ponieważ wymagany jest udział zewnętrznej jednostki certyfikującej.

([25]) W celu zachowania zwięzłości pozostała część niniejszej sekcji odnosi się wyłącznie do norm zharmonizowanych, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*. Te same wytyczne mają jednak również zastosowanie do wspólnych specyfikacji przyjętych zgodnie z art. 27 ust. 2 oraz do europejskich programów certyfikacji cyberbezpieczeństwa w przypadkach określonych przez Komisję w drodze aktów delegowanych zgodnie z art. 27 ust. 9.

Rys. 6:

Ilustracja sposobu, w jaki zastosowanie przywołanej normy zharmonizowanej obejmującej wyłącznie podstawową funkcjonalność decyduje o mającej zastosowanie procedurze oceny zgodności



152. Dotyczy to również sytuacji, w której produkt z elementami cyfrowymi zawiera dodatkową funkcję, która sama w sobie jest funkcją innego ważnego lub krytycznego produktu z elementami cyfrowymi. W rzeczywistości to podstawowa funkcja produktu z elementami cyfrowymi jako całości, a nie funkcja włączonych komponentów rozpatrywanych oddzielnie, decyduje o tym, czy produkt z elementami cyfrowymi należy do kategorii produktów ważnych czy krytycznych (a zatem o mającym zastosowanie systemie oceny zgodności). Na przykład jeżeli produkt z elementami cyfrowymi posiada podstawową funkcjonalność ważnego produktu z elementami cyfrowymi klasy I, produkt ten jako całość podlega systemowi oceny zgodności mającemu zastosowanie do ważnych produktów z elementami cyfrowymi klasy I, nawet jeżeli zawiera komponent, który sam w sobie jest produktem krytycznym z elementami cyfrowymi. W takich przypadkach, gdy producent stosuje normę zharmonizowaną obejmującą ryzyko związane z podstawową funkcjonalnością tego produktu, może on skorzystać z procedury kontroli wewnętrznej.

Przykład 63: Sprzęt komputerowy z elementami cyfrowymi posiada podstawową funkcjonalność routera, zgodnie z opisem w załączniku I pkt 12 do rozporządzenia wykonawczego (UE) 2025/2392. Ten produkt z elementami cyfrowymi obejmuje również dodatkowe funkcje, w tym zdolności zapory sieciowej, ponieważ zawiera komponent zapory sieciowej. Producent przeprowadza ocenę ryzyka obejmującą produkt z elementami cyfrowymi w całości, w tym podstawową funkcjonalność routera i funkcjonalność zapory sieciowej. Stosuje on normę zharmonizowaną obejmującą ryzyko związane z podstawową funkcjonalnością routera oraz dodatkowe środki w celu przeciwdziałania ryzyku wynikającemu z dodatkowych funkcji. Na przykład producent może zastosować normę zharmonizowaną dotyczącą zapór sieciowych w celu uwzględnienia ryzyka związanego z funkcjonalnością zapory sieciowej. Producent może skorzystać z procedury kontroli wewnętrznej na potrzeby oceny zgodności, obejmującej produkt z elementami cyfrowymi jako całość, w tym funkcjonalność zapory sieciowej.

6.3. Konsekwencje dla domniemania zgodności

153. Art. 27 ust. 1 aktu o cyberodporności stanowi, że 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 aktu o cyberodporności objęte tymi normami lub ich częściami ([26]). W art. 27 ust. 5

([26]) Jak wyraźnie stwierdzono w sekcji 4.1.2.2 Niebieskiego przewodnika, „w prawodawstwie harmonizacyjnym dotyczącym ryzyka [...] producenci zawsze – nawet gdy stosują normy zharmonizowane, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej* – muszą ocenić wszystkie rodzaje ryzyka związane z ich produktem, aby ustalić stosowne zasadnicze (lub inne) wymagania. Po dokonaniu takiej oceny producent może zdecydować się na zastosowanie specyfikacji technicznych określonych w normach zharmonizowanych, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, aby wdrożyć »środki zmniejszania ryzyka«, które są określone w normach zharmonizowanych".

rozszerzono to samo domniemanie zgodności na produkty z elementami cyfrowymi i procedury wprowadzone przez producenta, które są zgodne ze wspólnymi specyfikacjami przyjętymi przez Komisję w drodze aktów wykonawczych, a w art. 27 ust. 8 ustanowiono domniemanie zgodności w odniesieniu do produktów z elementami cyfrowymi i procedur wprowadzonych przez producenta, dla których wydano unijną deklarację zgodności lub certyfikat w ramach europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego na podstawie rozporządzenia (UE) 2019/881, jeżeli zostało to określone w aktach delegowanych zgodnie z art. 27 ust. 9 ([27]).

154. W związku z tym w przypadku gdy producent zastosował normę zharmonizowaną, do której odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, korzysta on z domniemania zgodności w odniesieniu do rodzajów ryzyka objętych tą normą. Może tak być na przykład w przypadku, gdy norma zharmonizowana, do której się odwołuje, odnosi się do wszystkich rodzajów ryzyka związanych z podstawową funkcjonalnością produktu z elementami cyfrowymi i nie ma żadnych dodatkowych funkcjonalności, które stwarzają ryzyko w cyberprzestrzeni. Oczekuje się na przykład, że norma zharmonizowana dotycząca routerów uwzględni co najmniej ryzyko związane z podstawową funkcjonalnością tych produktów z elementami cyfrowymi. Jeżeli taki produkt nie zawiera żadnych dodatkowych funkcjonalności lub jeżeli te dodatkowe funkcjonalności nie stwarzają ryzyka nieuwzględnionego w normie, produkt z elementami cyfrowymi może korzystać z domniemania zgodności.

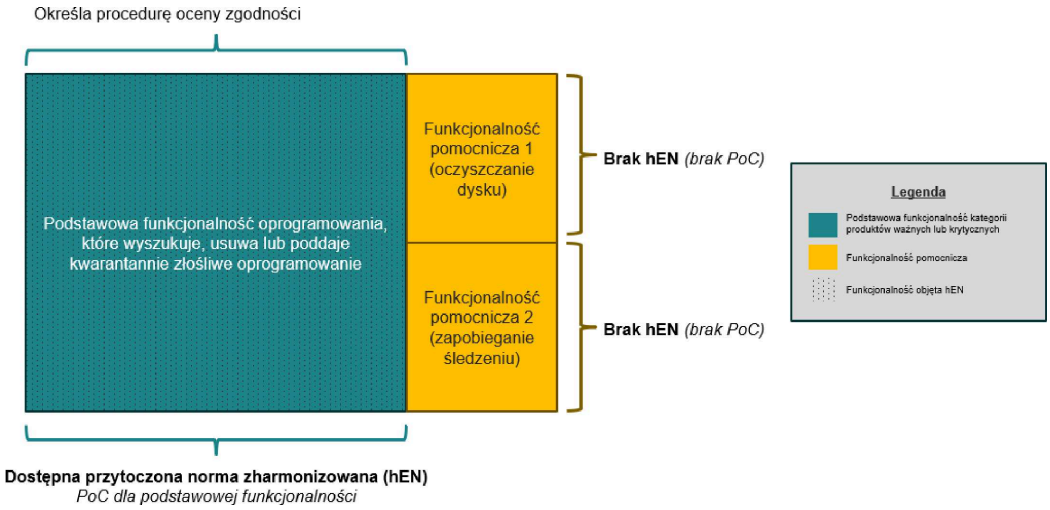
155. W przypadkach omówionych w pkt 151 i 152 producent może zastosować procedurę kontroli wewnętrznej, ponieważ norma zharmonizowana obejmuje rodzaje ryzyka związane z podstawową funkcjonalnością produktu z elementami cyfrowymi. Produkty z elementami cyfrowymi opisane w tych przykładach mogą jednak wykraczać poza zakres norm zharmonizowanych, a dodatkowe funkcjonalności mogą stwarzać ryzyko w cyberprzestrzeni, którego nie uwzględnia dana norma zharmonizowana. Te produkty z elementami cyfrowymi mogą zatem nie korzystać z domniemania zgodności w odniesieniu do tych dodatkowych funkcjonalności.

Przykład 64: Oprogramowanie antywirusowe posiada podstawową funkcjonalność oprogramowania, które wyszukuje, usuwa lub poddaje kwarantannie złośliwe oprogramowanie, a ryzyko związane z tą podstawową funkcjonalnością jest objęte normą zharmonizowaną. Ten produkt z elementami cyfrowymi zawiera również dodatkowe funkcjonalności, a mianowicie funkcję czyszczenia dysku i funkcjonalność zapobiegania śledzeniu, chroniącą użytkownika podczas poruszania się w sieci, których ryzyko nie jest objęte normą zharmonizowaną. W przypadku zastosowania normy zharmonizowanej producent może skorzystać z procedury kontroli wewnętrznej w celu dokonania oceny zgodności. Będzie on korzystał z domniemania zgodności w odniesieniu do ryzyka związanego z podstawową funkcjonalnością tego produktu, ale nie w odniesieniu do ryzyka związanego z dodatkowymi funkcjami.

([27]) Podobnie jak powyżej, dla zachowania zwięzłości, pozostała część niniejszej sekcji odnosi się wyłącznie do norm zharmonizowanych, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*. Te same wytyczne mają jednak również zastosowanie do wspólnych specyfikacji i europejskich programów certyfikacji cyberbezpieczeństwa.

Rys. 7:

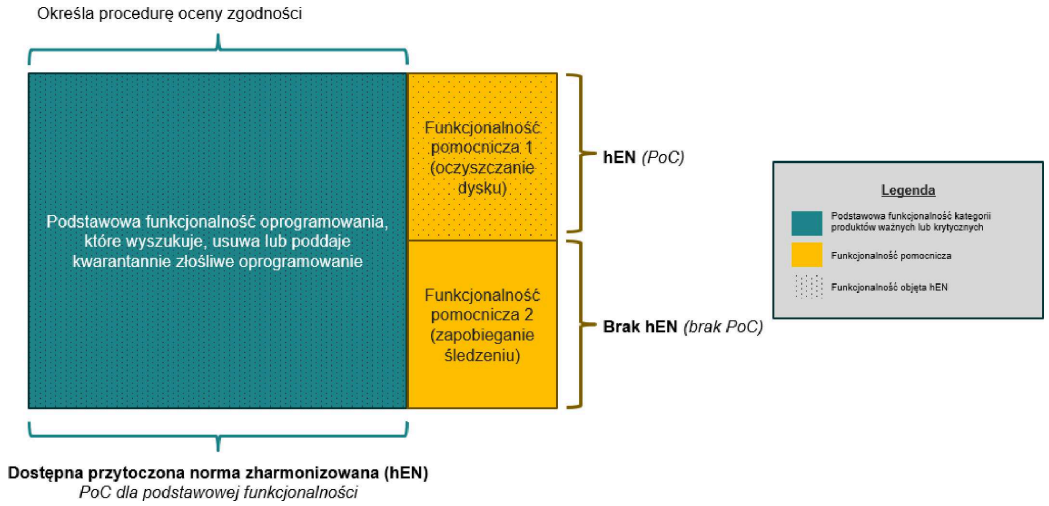
Norma zharmonizowana przyznaje domniemanie zgodności w odniesieniu do podstawowej funkcjonalności, ponieważ odnosi się do wszystkich rodzajów ryzyka związanych z tą podstawową funkcjonalnością, ale nie dotyczy to funkcjonalności pomocniczych



Przykład 65: W tym samym scenariuszu, co w poprzednim przykładzie, zaktualizowano normę zharmonizowaną, aby uwzględnić również ryzyko związane z jedną z dodatkowych funkcjonalności, a mianowicie funkcją czyszczenia dysku, ale nie z drugą (tj. funkcją zapobiegania śledzeniu). W przypadku zastosowania normy zharmonizowanej producent może skorzystać z procedury kontroli wewnętrznej w celu dokonania oceny zgodności. Będzie on korzystał z domniemania zgodności w odniesieniu do ryzyka związanego z podstawową funkcjonalnością tego produktu oraz z funkcją czyszczenia dysku, ale nie w odniesieniu do ryzyka związanego z funkcjonalnością zapobiegania śledzeniu.

Rys. 8:

Norma zharmonizowana przyznaje domniemanie zgodności w odniesieniu do funkcjonalności podstawowej i funkcjonalności pomocniczej 1, ponieważ odnosi się do wszystkich rodzajów ryzyka związanych z tymi dwiema funkcjonalnościami, ale nie dla funkcjonalności pomocniczej 2



7. **OCENA RYZYKA W CYBERPRZESTRZENI I ŁĄCZENIE PRODUKTÓW Z ELEMENTAMI CYFROWYMI Z KOMPONENTAMI**

7.1. **Ocena i zmniejszanie ryzyka w cyberprzestrzeni**

156. Ocena ryzyka w cyberprzestrzeni, o której mowa w art. 13 ust. 2 aktu o cyberodporności, wymaga od producentów zidentyfikowania istotnego ryzyka i oceny jego potencjalnych skutków dla produktu z elementami cyfrowymi. Producenci muszą również wdrożyć odpowiednie środki w celu przeciwdziałania temu ryzyku, zgodnie z zasadniczymi wymaganiami określonymi w załączniku I.

157. W ramach zarządzania ryzykiem w organizacji ryzyko ocenia się zazwyczaj na podstawie kryteriów akceptacji wynikających z wewnętrznych celów organizacji lub jej gotowości do podejmowania ryzyka. Natomiast zgodnie z aktem o cyberodporności rezydualne ryzyko w cyberprzestrzeni należy oceniać w świetle wymogu, zgodnie z którym produkt z elementami cyfrowymi wprowadzany do obrotu musi zapewniać odpowiedni poziom cyberbezpieczeństwa stosownie do ryzyka, biorąc pod uwagę jego przeznaczenie i racjonalnie przewidywalne wykorzystanie.

158. W związku z tym wewnętrzna tolerancja ryzyka producenta, strategia handlowa lub same względy kosztowe nie mają znaczenia dla ustalenia, czy ryzyko zostało uwzględnione. Do celów art. 13 ust. 2 i 3 producenci muszą być w stanie ustalić, czy zidentyfikowane ryzyko w cyberprzestrzeni zostało w wystarczającym stopniu uwzględnione poprzez wdrożenie zasadniczych wymagań określonych w załączniku I część I, w świetle przewidzianego zastosowania, racjonalnie przewidywalnego wykorzystania i warunków użytkowania, w tym, w stosownych przypadkach, środowiska operacyjnego (na przykład docelowych użytkowników produktu z elementami cyfrowymi) oraz aktywów, które mają być chronione, z uwzględnieniem oczekiwanego czasu użytkowania produktu z elementami cyfrowymi.

159. Rezydualne ryzyko w cyberprzestrzeni stanowi nieodłączny wynik oceny ryzyka i zmniejszania ryzyka. Uznaje się, że w praktyce nie można całkowicie wyeliminować ryzyka w cyberprzestrzeni. Istnienie ryzyka rezydualnego nie oznacza jednak, że producent może zaakceptować jakiekolwiek ryzyko według własnego uznania. Produkt z elementami cyfrowymi może zostać wprowadzony do obrotu tylko wtedy, gdy ryzyko rezydualne, po podjęciu odpowiednich środków, zostało w wystarczającym stopniu uwzględnione poprzez wdrożenie zasadniczych wymagań, z uwzględnieniem przeznaczenia i racjonalnie przewidywalnego wykorzystania produktu z elementami cyfrowymi.

160. Zgodnie z art. 13 ust. 3 w przypadku zidentyfikowania ryzyka w cyberprzestrzeni producenci są zobowiązani do przeciwdziałania mu za pomocą odpowiednich środków, w tym na poziomie produktu. W zależności od okoliczności może to obejmować na przykład zmniejszenie powierzchni ataku, wdrożenie zabezpieczeń technicznych, ograniczenie lub dostosowanie funkcjonalności lub dokładniejsze określenie przeznaczenia produktu z elementami cyfrowymi. Producenci mogą również podejmować działania mające na celu kształtowanie racjonalnie przewidywalnego wykorzystania produktu z elementami cyfrowymi, na przykład poprzez informowanie o ryzyku, wytyczne dla użytkownika lub projektowanie interfejsu użytkownika, aby ukierunkować zachowania użytkowników na bezpieczne wzorce użytkowania.

161. Akt o cyberodporności nie przewiduje przeniesienia ryzyka w cyberprzestrzeni ani odpowiedzialności na użytkowników lub osoby trzecie w celu zrekompensowania niedociągnięć w projekcie produktu lub uzasadnienia pozostawienia ryzyka w cyberprzestrzeni bez uwzględnienia. Obowiązek wprowadzenia do obrotu bezpiecznego produktu z elementami cyfrowymi oraz wykazania zgodności z zasadniczymi wymaganiami spoczywa na producencie.

162. Informacje i instrukcje przekazywane użytkownikom mogą być wykorzystywane do wspierania bezpiecznego wdrożenia i eksploatacji produktu z elementami cyfrowymi, w tym w przypadku gdy producent postanowił ograniczyć przeznaczenie tego produktu do zaufanych środowisk, a także do informowania użytkowników o ryzyku rezydualnym w sposób odpowiedni do charakteru produktu z elementami cyfrowymi i jego docelowych użytkowników.

Przykład 66: Producent opracowuje czujnik przemysłowy przeznaczony do stosowania w zaufanych środowiskach. Aby czujnik mógł prawidłowo spełniać swoją funkcję, producent nie wdraża środków ochrony przed fizycznymi atakami na sam czujnik. Aby ograniczyć powiązane ryzyko zidentyfikowane w ocenie ryzyka, producent ogranicza przeznaczenie czujnika do stosowania wyłącznie w zaufanych środowiskach, w których uniemożliwia się nieuprawniony fizyczny dostęp do produktu z elementami cyfrowymi. Informacje i instrukcje dla użytkowników zawierają jasne informacje na temat tych ograniczeń w korzystaniu z czujnika, w sposób odpowiedni do charakteru produktu z elementami cyfrowymi i jego docelowych użytkowników.

Przykład 67: Producent opracowuje aplikację do użytku profesjonalnego na zarządzanych komputerach stacjonarnych i urządzeniach mobilnych. Aplikacja przetwarza lokalnie przechowywane dane wrażliwe i treści tworzone przez użytkowników. Podczas oceny ryzyka producent identyfikuje ryzyko nieuprawnionego dostępu do takich danych, jeżeli są one przechowywane w postaci zwykłego tekstu na urządzeniu. Zamiast zaprojektować i wdrożyć własny mechanizm szyfrowania w samej aplikacji, producent decyduje się na wykorzystanie funkcji szyfrowania i zarządzania kluczami zapewnianych na miejscu przez system operacyjny, na którym ma działać aplikacja, ponieważ wbudowane usługi kryptograficzne tego systemu operacyjnego są dopracowane i regularnie aktualizowane.

163. W przypadku gdy w ocenie ryzyka w cyberprzestrzeni zidentyfikowano ryzyko, któremu nie można odpowiednio zaradzić za pomocą odpowiednich środków, zgodność z aktem o cyberodporności może wymagać zmian w projekcie, funkcjonalności lub przeznaczeniu produktu z elementami cyfrowymi. Względy związane wyłącznie z kosztami lub komercyjną wykonalnością nie stanowią wystarczającej podstawy do pozostawienia takiego ryzyka bez odpowiedzi, jeżeli uniemożliwiłoby to spełnienie zasadniczych wymagań przez produkt z elementami cyfrowymi.

7.2. Projektowanie, opracowywanie i wytwarzanie produktów z elementami cyfrowymi tak, by zapewniały odpowiedni poziom cyberbezpieczeństwa stosownie do ryzyka

164. Zasadnicze wymaganie w zakresie cyberbezpieczeństwa, o którym mowa w części I pkt 1 załącznika I do aktu o cyberodporności, stanowi, że produkty z elementami cyfrowymi projektuje się, opracowuje i produkuje tak, by zapewniały odpowiedni poziom cyberbezpieczeństwa stosownie do ryzyka.

165. To zasadnicze wymaganie ma na celu uwzględnienie wszystkich rodzajów ryzyka w cyberprzestrzeni, które zidentyfikowano w ramach oceny ryzyka w cyberprzestrzeni. W szczególności obejmuje to ryzyko w cyberprzestrzeni, które nie zostało w inny sposób odpowiednio uwzględnione w ramach wdrażania zasadniczych wymagań części I załącznika I innych niż określone w pkt 1. To zasadnicze wymaganie różni się od obowiązku prawnego dotyczącego przeprowadzenia oceny ryzyka w cyberprzestrzeni, którą należy przeprowadzić zgodnie z art. 13 ust. 2.

166. W przypadku gdy wszelkie istotne ryzyko w cyberprzestrzeni związane z produktem z elementami cyfrowymi jest zmniejszane poprzez wdrożenie odpowiednich środków mających na celu spełnienie mających zastosowanie zasadniczych wymagań innych niż określone w pkt 1, zasadnicze wymaganie, o którym mowa w załączniku I część I pkt 1, uznaje się za spełnione. Natomiast w przypadku gdy ocena ryzyka w cyberprzestrzeni wykaże dodatkowe ryzyko, które nie zostało w pełni uwzględnione w takich środkach, producenci są zobowiązani do wdrożenia odpowiednich środków w odniesieniu do produktu z elementami cyfrowymi w celu przeciwdziałania temu ryzyku, tak aby był on zgodny z zasadniczym wymaganiem, o którym mowa w załączniku I część I pkt 1. W praktyce oczekuje się, że w większości przypadków zgodność z pozostałymi zasadniczymi wymaganiami doprowadzi do zgodności z tym wymaganiem.

7.3. Ocena ryzyka i należyta staranność w odniesieniu do zależności zewnętrznych i włączonych komponentów

167. W akcie o cyberodporności ustanowiono dwa odrębne, ale uzupełniające się obowiązki producentów w odniesieniu do zarządzania ryzykiem w cyberprzestrzeni. Po pierwsze, w art. 13 ust. 2 zobowiązuje się producentów do przeprowadzenia oceny ryzyka w cyberprzestrzeni związanego z samym produktem z elementami cyfrowymi. Po drugie, w art. 13 ust. 5 nakłada się obowiązek zachowania należytej staranności w odniesieniu do włączonych komponentów. Łącznie te dwa obowiązki mają na celu zapewnienie, aby produkt z elementami cyfrowymi pozostawał bezpieczny, również w przypadku gdy wykorzystuje rozwiązania w zakresie zdalnego przetwarzania danych, usługi zdalne lub komponenty oprogramowania lub sprzętu stron trzecich.

168. Ocena ryzyka w cyberprzestrzeni dotyczy identyfikacji istotnych czynników ryzyka, które mogą mieć wpływ na produkt z elementami cyfrowymi, w tym czynników ryzyka pochodzących spoza samego produktu, takich jak sieci zewnętrzne, czynniki środowiskowe lub inne aspekty zewnętrzne, które mogą mieć wpływ na produkt z elementami cyfrowymi lub które produkt wykorzystuje, oraz dotyczy zarządzania tymi czynnikami ryzyka. W przypadku takiego ryzyka zewnętrznego akt o cyberodporności nie wymaga od producentów kontrolowania środowiska zewnętrznego ani zarządzania nim. Producenci są natomiast zobowiązani do zidentyfikowania takiego ryzyka i ograniczenia go poprzez zaprojektowanie i opracowanie samego produktu z elementami cyfrowymi. Będzie to obejmować wdrożenie odpowiednich zasadniczych wymagań określonych w załączniku I część I oraz, w razie potrzeby, dostarczanie użytkownikom informacji i instrukcji dotyczących ryzyka związanego z włączaniem komponentów lub wdrażaniem.

169. Na przykład producent może zidentyfikować ryzyko uzyskania przez osoby nieuprawnione dostępu do systemów zaplecza, które nie stanowią części samego produktu z elementami cyfrowymi, w czasie gdy produkt jest w trakcie działania, i próbować wysyłać złośliwe polecenia do produktu z elementami cyfrowymi. Takie systemy zaplecza, jeżeli nie zostały zaprojektowane i opracowane przez producenta lub na jego odpowiedzialność lub jeżeli nie obsługują jednej z funkcji produktu z elementami cyfrowymi, nie stanowią rozwiązań w zakresie zdalnego przetwarzania danych i w związku z tym nie wchodzą w zakres produktu z elementami cyfrowymi dla celów aktu o cyberodporności. Niemniej jednak w akcie o cyberodporności wymaga się od producenta przeciwdziałania ryzyku, jakie mogą stwarzać, za pomocą środków na poziomie produktu, takich jak wymóg kryptograficznego uwierzytelniania poleceń zdalnych, weryfikacja integralności zmian konfiguracji lub generowanie rejestrów lub alertów związanych z bezpieczeństwem w przypadku wykrycia nietypowego zachowania. Podobnie w przypadku gdy producent zidentyfikuje ryzyko wynikające z niedostępności takiej usługi zewnętrznej, na przykład z powodu przerw w dostawie prądu lub awarii infrastruktury, akt o cyberodporności może zawierać wymaganie zastosowania środków ograniczających ryzyko w cyberprzestrzeni na poziomie produktu, np. zapewnienia, aby przerwa w dostawie prądu nie spowodowała przejścia produktu z elementami cyfrowymi w stan niezabezpieczony. W takich przypadkach akt o cyberodporności reguluje sposób, w jaki produkt z elementami cyfrowymi reaguje na to ryzyko zewnętrzne; nie nakłada on obowiązków dotyczących sposobu organizacji, obsady personelem lub funkcjonowania infrastruktury zaplecza ani nie traktuje tej infrastruktury jako części produktu z elementami cyfrowymi.

170. Należyta staranność odnosi się do elementów, które stanowią część samego produktu z elementami cyfrowymi, w szczególności włączonych komponentów oprogramowania lub sprzętu dostarczonych przez stronę trzecią. Producenci są zobowiązani do wprowadzenia odpowiednich środków w celu zapewnienia, aby takie komponenty nie wpływały negatywnie na zgodność produktu z elementami cyfrowymi z zasadniczymi wymaganiami. Można to osiągnąć jedynie poprzez określenie, jakie są wymagania produktu z elementami cyfrowymi wobec jego komponentów, aby osiągnąć cele w zakresie cyberbezpieczeństwa, oraz poprzez zweryfikowanie, w oparciu o analizę ryzyka, czy komponenty te są zgodne z potrzebami produktu, jak wskazano również w motywie 34.

171. Zgodnie z przeprowadzoną oceną ryzyka w cyberprzestrzeni producent musi określić wymagania, jakie włączony komponent powinien spełniać. Na przykład jeżeli produkt z elementami cyfrowymi wykorzystuje funkcje kryptograficzne, mechanizmy aktualizacji lub bezpieczną komunikację zapewnianą przez komponent, producent musi, w ramach należytej staranności, zidentyfikować te potrzeby i sprawdzić, czy komponent je zaspokaja. Dowody to potwierdzające mogą obejmować dokumentację uzyskaną od producenta komponentu, taką jak specyfikacje techniczne, dokumentacja bezpieczeństwa lub odpowiednia dokumentacja zgodności lub usługi atestacyjnej. W stosownych przypadkach producent może również przeprowadzić badania w celu sprawdzenia, czy komponenty te prawidłowo realizują odpowiednie funkcje. Chociaż należyta staranność stanowi odrębny obowiązek prawny, wspiera ona i wzmacnia zdolność producenta do wykazania zgodności z zasadniczymi wymaganiami dotyczącymi produktu z elementami cyfrowymi jako całości.

172. Oceniając ryzyko dla produktu z elementami cyfrowymi jako całości, w ocenie ryzyka w cyberprzestrzeni należy uwzględnić elementy nienależące do produktu, takie jak elementy środowiskowe, infrastruktura zewnętrzna, inne systemy lub sieci, oraz, w stosownych przypadkach, uwzględnić je za pomocą środków na poziomie produktu w celu zapewnienia zgodności produktu z elementami cyfrowymi z zasadniczymi wymaganiami. W ocenie ryzyka należy również uwzględnić komponenty, które są fizycznie lub logicznie włączone do produktu z elementami cyfrowymi, ale pochodzą od strony trzeciej. Dla celów zapewnienia zgodności producent powinien jednak traktować te komponenty jako części dostarczane z zewnątrz, których właściwości są weryfikowane z zachowaniem należytej staranności w momencie włączenia komponentu, ponieważ producent mógł ich nie przeprojektować ani nie opracować na nowo.

173. Ta sama logika ma zastosowanie podczas opracowywania i włączania komponentów. W przypadku gdy producent samodzielnie opracowuje funkcjonalności, musi bezpośrednio wdrożyć zasadnicze wymagania. W przypadku gdy producent włącza komponenty opracowane przez innych, musi zapewnić, z zachowaniem należytej staranności, aby komponenty te mogły być wykorzystywane w sposób umożliwiający zgodność produktu z elementami cyfrowymi jako całości z przepisami. W obu przypadkach cel pozostaje taki sam: produkt z elementami cyfrowymi wprowadzany do obrotu osiąga odpowiedni poziom cyberbezpieczeństwa zgodnie z wymogami aktu o cyberodporności, z uwzględnieniem ryzyka zidentyfikowanego w ocenie ryzyka w cyberprzestrzeni.

7.4. **Ponowne wykorzystanie ocen ryzyka i dokumentacji zgodności w odniesieniu do rodzin produktów z elementami cyfrowymi**

174. Producenci mogą wprowadzać do obrotu produkty z elementami cyfrowymi, które są do siebie podobne, na przykład różne warianty, modele lub konfiguracje tej samej rodziny produktów. Jeżeli takie produkty z elementami cyfrowymi mają tę samą architekturę, projekt istotny z punktu widzenia bezpieczeństwa i przeznaczenie oraz są narażone na to samo ryzyko w cyberprzestrzeni, w akcie o cyberodporności nie wymaga się od producentów traktowania każdego wariantu jako całkowicie odrębnego produktu z elementami cyfrowymi do celów oceny ryzyka i oceny zgodności.

175. W takich przypadkach, pod warunkiem że wszystkie odnośne warianty są odpowiednio uwzględnione pod względem istotnego ryzyka i zasadniczych wymagań, producenci mogą oprzeć się na: (i) jednej ocenie ryzyka w cyberprzestrzeni przeprowadzonej zgodnie z art. 13 ust. 2 aktu o cyberodporności; (ii) pojedynczym zestawie dokumentacji technicznej; oraz (iii) jednej procedurze oceny zgodności. Umożliwia to również wydanie jednej deklaracji zgodności UE dla grupy produktów z elementami cyfrowymi, o ile wyraźnie określono w niej warianty produktu, do których ma ona zastosowanie.

176. Czynnikiem decydującym jest to, czy różnice między wariantami mają znaczenie dla cyberbezpieczeństwa. Różnice, które nie mają wpływu na właściwości produktu z elementami cyfrowymi w zakresie cyberbezpieczeństwa, takie jak różnice w kolorze, kształcie, wielkości pamięci lub innych cechach niezwiązanych z bezpieczeństwem, nie wymagają oddzielnych ocen ryzyka ani ocen zgodności. Z kolei w niektórych przypadkach warianty mogą różnić się w sposób wpływający na spełnienie zasadniczych wymagań, na przykład poprzez różne interfejsy komunikacyjne, stosy oprogramowania, mechanizmy aktualizacji lub łączność zdalną. W takich przypadkach różnice te muszą zostać odzwierciedlone w ocenie ryzyka oraz, w razie potrzeby, w ocenie zgodności i dokumentacji technicznej.

177. Producenci pozostają odpowiedzialni za zapewnienie, aby ocena ryzyka i powiązana dokumentacja dokładnie odzwierciedlały produkty z elementami cyfrowymi wprowadzone do obrotu. W przypadku gdy nowy wariant wprowadza nowe ryzyko w cyberprzestrzeni lub zmienia sposób wdrażania zasadniczych wymagań, należy odpowiednio zaktualizować istniejącą ocenę ryzyka i dokumentację zgodności. Poleganie na pojedynczej ocenie zgodności jest możliwe jedynie w zakresie, w jakim produkty z elementami cyfrowymi nie wykazują różnic pod względem swoich właściwości w zakresie cyberbezpieczeństwa.

8. **ZDALNE PRZETWARZANIE DANYCH**

178. W art. 3 pkt 1 aktu o cyberodporności produkt z elementami cyfrowymi zdefiniowano jako „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". W świetle powyższego producent musi traktować produkt z elementami cyfrowymi jako całość, w tym związane z nim rozwiązania w zakresie zdalnego przetwarzania danych (RDPS). Na przykład przy wykazywaniu, że produkt z elementami cyfrowymi spełnia zasadnicze wymagania określone w załączniku I, należy wziąć pod uwagę rozwiązania RDPS, począwszy od oceny ryzyka (art. 13 ust. 2). To samo dotyczy obowiązków związanych z cyklem życia produktu, takich jak zgłaszanie aktywnie wykorzystywanych podatności i poważnych incydentów (art. 14).

179. Celem niniejszych wytycznych jest zapewnienie producentom dodatkowego wsparcia w ustaleniu, czy ich produkt z elementami cyfrowymi posiada rozwiązanie w zakresie zdalnego przetwarzania danych zdefiniowane w akcie o cyberodporności oraz w jaki sposób wypełnić obowiązki dotyczące zgodności w tym zakresie. Po wstępnej analizie definicji i motywów określonych w akcie o cyberodporności w niniejszych wytycznych zostaną przedstawione pytania, które pomogą producentom w ustaleniu, czy ich produkt z elementami cyfrowymi zawiera rozwiązanie w zakresie zdalnego przetwarzania danych (zob. sekcja *8.1 Co uznaje się za rozwiązanie w zakresie zdalnego przetwarzania danych w odniesieniu do produktu z elementami cyfrowymi?*). Następnie omówione zostaną techniczne konsekwencje rozwiązania w zakresie zdalnego przetwarzania danych oraz sposób oceny zgodności z aktem o cyberodporności (zob. sekcja *8.2 Praktyczne i techniczne konsekwencje rozwiązań w zakresie zdalnego przetwarzania danych oraz korzystania z rozwiązań stron trzecich*).

180. Zgodnie z art. 3 pkt 2 pojęcie „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". Rozwiązanie w zakresie zdalnego przetwarzania danych (RDPS) definiuje się zatem jako elementy oprogramowania („części elektronicznego systemu informacyjnego, która składa się z kodu komputerowego", zgodnie z definicją zawartą w art. 3 pkt 4) służące do przetwarzania danych na odległość. Nie ma ono na celu włączenia, w ramach zakresu produktu z elementami cyfrowymi, sprzętu, na którym może opierać się zdalne przetwarzanie danych.

181. W motywach 11 i 12 zawarto dalsze wyjaśnienia dotyczące tego, jak należy interpretować to pojęcie. W motywie 11 wyjaśniono, że celem objęcia zakresem rozporządzenia rozwiązań w zakresie zdalnego przetwarzania danych jest zagwarantowanie, że „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". Stwierdza się tam również, że „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".

182. Z motywu 11 wynika zatem, że wymagania aktu o cyberodporności nie mają obejmować całej infrastruktury informatycznej organizacji, a jedynie komponenty oprogramowania, które umożliwiają realizację rozwiązania w zakresie przetwarzania danych. Za rozwiązania w zakresie zdalnego przetwarzania danych nie należy uznawać na przykład systemów wewnętrznych związanych z własnymi zasobami ludzkimi producenta, listami płac, zarządzaniem relacjami z klientami, ciągłą integracją/ciągłymi dostawami (CI/CD), czy dystrybucją aktualizacji zabezpieczeń do lokalizacji brzegowych. Podobnie systemy związane z działaniami w zakresie audytu i testowania, takie jak testy penetracyjne, aktywne poszukiwanie zagrożeń i *red teaming*, nie wchodzą w zakres produktu z elementami cyfrowymi objętego aktem o cyberodporności. Należy zauważyć, że chociaż przeprowadzanie skutecznych i regularnych testów i przeglądów bezpieczeństwa produktu z elementami cyfrowymi stanowi zasadniczy wymóg określony w załączniku I część II pkt 3 do aktu o cyberodporności, nie oznacza to, że takie działania należy uznać za rozwiązania w zakresie zdalnego przetwarzania danych w odniesieniu do produktu z elementami cyfrowymi.

183. W motywie 12 skoncentrowano się na usługach w chmurze i szczegółowo omówiono okoliczności, w których usługi w chmurze można uznać za rozwiązania w zakresie zdalnego przetwarzania danych. Motyw kończy się przypomnieniem, że usługi chmurowe oraz modele usług chmurowych wchodzą w zakres stosowania dyrektywy (UE) 2022/2555 (NIS 2) ([28]), w której ustanowiono wymagania w zakresie zarządzania ryzykiem w cyberprzestrzeni dla dostawców usług chmurowych. Wymagania te doprecyzowano w rozporządzeniu wykonawczym Komisji (UE) 2024/2690 ([29]).

8.1. **Co uznaje się za rozwiązanie w zakresie zdalnego przetwarzania danych w odniesieniu do produktu z elementami cyfrowymi?**

184. Definicja zdalnego przetwarzania danych określona w art. 3 pkt 2 opiera się zatem na trzech elementach: (i) czy przetwarzanie danych odbywa się „na odległość"; (ii) czy brak takiego przetwarzania danych spowodowałby, że produkt z elementami cyfrowymi nie mógłby wykonywać jednej ze swoich funkcji; oraz (iii) czy oprogramowanie zostało zaprojektowane i opracowane przez producenta lub na jego odpowiedzialność. W kolejnych trzech podsekcjach omówiono każdy z tych elementów bardziej szczegółowo.

([28]) 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, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27.

([29]) Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania, Dz.U. L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj.

8.1.1. *Pojęcie „na odległość”*

185. Pojęcie „na odległość”, o którym mowa w art. 3 pkt 2, ma znaczenie, ale nie jest wystarczające do ustalenia, czy produkt z elementami cyfrowymi obejmuje rozwiązanie w zakresie zdalnego przetwarzania danych. Ponadto, biorąc pod uwagę różnorodność rozwiązań, które mogą wchodzić w zakres tego pojęcia, nie jest możliwe przedstawienie wyczerpującej definicji terminu „na odległość”. Konieczna jest indywidualna ocena każdego przypadku przez producenta.

186. W motywie 11 aktu o cyberodporności wspomniano o danych przetwarzanych lub przechowywanych „zdalnie przez producenta” w przeciwieństwie do danych przetwarzanych lub przechowywanych „lokalnie na urządzeniu użytkownika”. Zdalne przetwarzanie danych zazwyczaj odbywa się poza środowiskiem użytkownika produktu z elementami cyfrowymi lub środowiskiem operacyjnym organizacji (w przypadku użytkownika profesjonalnego). Nie wyklucza to jednak, że przetwarzanie może również odbywać się w pobliżu urządzenia („na obrzeżach sieci”). Przesyłanie danych może odbywać się przewodowo (np. za pomocą kabla Ethernet) lub bezprzewodowo (np. Wi-Fi, Bluetooth). Przetwarzanie w chmurze, w tym przetwarzanie brzegowe, jest typowym przykładem przetwarzania danych „na odległość”. Na przykład w przypadku funkcji opartej na chmurze, do której użytkownik ma dostęp z aplikacji mobilnej, część przetwarzania danych odbywa się w chmurze, poza środowiskiem użytkownika.

187. Należy zauważyć, że rozwiązania w zakresie zdalnego przetwarzania danych niekoniecznie muszą być obsługiwane w ramach infrastruktury chmurowej stron trzecich. Zdalne przetwarzanie danych na lokalnych serwerach w siedzibie producenta może również stanowić rozwiązanie w zakresie zdalnego przetwarzania danych. Innymi słowy, rozwiązanie działające lokalnie oraz w chmurze prywatnej ma takie same szanse na zakwalifikowanie się jako rozwiązanie w zakresie zdalnego przetwarzania danych, jak rozwiązanie działające w chmurze publicznej poza siedzibą firmy.

188. Dwa decydujące i łączące się ze sobą pytania, od których zależy, czy przetwarzanie danych jest objęte aktem o cyberodporności jako rozwiązanie w zakresie zdalnego przetwarzania danych, przedstawiono poniżej w sekcjach *8.1.2* i *8.2*. Jeżeli na oba pytania zostanie udzielona odpowiedź twierdząca, zdalne przetwarzanie danych kwalifikuje się jako rozwiązanie w zakresie zdalnego przetwarzania danych.

8.1.2. *Czy brak takiego przetwarzania danych spowodowałby, że produkt z elementami cyfrowymi nie będzie mógł wykonywać jednej ze swoich funkcji?*

189. Jak określono w definicji „zdalnego przetwarzania danych” zawartej w art. 3 pkt 2, aby przetwarzanie danych na odległość kwalifikowało się jako rozwiązanie w zakresie zdalnego przetwarzania danych, jego brak spowodowałby, że produkt z elementami cyfrowymi nie mógłby wykonywać jednej ze swoich funkcji. Pojęcie „funkcji” zawarte w tej definicji nie ogranicza się do „podstawowej funkcjonalności” lub „przeznaczenia” produktu z elementami cyfrowymi, ponieważ w akcie o cyberodporności nie nałożono takiego ograniczenia. Funkcje objęte zakresem aktu o cyberodporności to zarówno funkcje, które bezpośrednio realizują przeznaczenie produktu z elementami cyfrowymi w sposób odczuwany przez użytkowników, jak i funkcje zwiększające ogólną efektywność produktu.

190. Przykłady funkcji, w ramach których może odbywać się przetwarzanie danych na odległość i które powodowałyby, że produkt z elementami cyfrowymi nie mógłby wykonywać jednej ze swoich funkcji, obejmują: (i) wysyłanie poleceń do urządzenia; (ii) synchronizację plików; (iii) rejestrację użytkownika; (iv) konfigurację (personalizację produktu z elementami cyfrowymi); (v) zautomatyzowaną dystrybucję aktualizacji, w tym aktualizacji funkcji i poprawek zabezpieczeń; (vi) zarządzanie tożsamością i dostępem;

191. W niektórych przypadkach użytkownik może korzystać z funkcji zarówno zdalnie, jak i ręcznie (np. przełączając żarówkę za pomocą aplikacji lub ręcznie). Istnienie tej możliwości nie wyklucza zakwalifikowania przetwarzania danych związanego ze zdalnym wykonywaniem tej funkcji jako rozwiązania w zakresie zdalnego przetwarzania danych. Wykonywanie tej funkcji zdalnie uznaje się również za część funkcji oferowanych przez produkt z elementami cyfrowymi.

192. Natomiast w przypadku gdy brak określonego przetwarzania danych nie powoduje, że produkt z elementami cyfrowymi nie może wykonywać jednej ze swoich funkcji, takiego przetwarzania nie uznaje się za rozwiązanie w zakresie zdalnego przetwarzania danych w rozumieniu aktu o cyberodporności. Obejmuje to na przykład zdalną analizę danych telemetrycznych gromadzonych wyłącznie do celów statystycznych lub przyszłego rozwoju produktu.

193. Niemniej jednak, nawet jeżeli przetwarzanie danych nie obsługuje jakiejś funkcji produktu z elementami cyfrowymi, producenci być może będą musieli rozważyć, czy te zdalne komponenty stwarzają ryzyko dla produktu z elementami cyfrowymi w ramach przeprowadzanej przez nich oceny ryzyka w cyberprzestrzeni (np. w świetle środowiska operacyjnego produktu), oraz odpowiednio ograniczyć takie ryzyko (np. poprzez środki ograniczające na poziomie produktu).

194. Strony internetowe stanowią szczególny przypadek, który wymaga dalszego doprecyzowania, jak wyjaśniono również w *sekcji 2.1 Wprowadzenie do obrotu*. Strony internetowe nie wchodzą w zakres rozwiązania w zakresie zdalnego przetwarzania danych, jeżeli nie obsługują funkcji produktu z elementami cyfrowymi, jak wyjaśniono w motywie 11 aktu o cyberodporności. Sam fakt, że strona internetowa zawiera informacje o produkcie z elementami cyfrowymi, nie wystarcza, aby uznać ją za objętą zakresem rozwiązania w zakresie zdalnego przetwarzania danych, nawet jeżeli produkt przekierowuje na taką stronę internetową. Na przykład przekierowywanie użytkowników na zewnętrzną stronę internetową zawierającą informacje i instrukcje dla użytkowników nie stanowi rozwiązania w zakresie zdalnego przetwarzania danych. Natomiast strona internetowa może stanowić rozwiązanie w zakresie zdalnego przetwarzania danych, jeżeli aktywuje lub obsługuje funkcję produktu z elementami cyfrowymi. Na przykład portal uwierzytelniania, który wydaje dane uwierzytelniające lub tokeny wymagane do działania produktu z elementami cyfrowymi, byłby uznawany za rozwiązanie w zakresie zdalnego przetwarzania danych (pod warunkiem że spełnione są również pozostałe kryteria zawarte w definicji).

8.1.3. *Czy oprogramowanie zostało zaprojektowane i opracowane przez producenta lub na jego odpowiedzialność?*

195. Definicja „zdalnego przetwarzania danych" zawarta w art. 3 pkt 2 aktu o cyberodporności stanowi ponadto, że oprogramowanie do takiego przetwarzania danych na odległość musi być zaprojektowane i opracowane przez producenta lub na jego odpowiedzialność. Zdalne przetwarzanie danych w całości opracowane i zaprojektowane przez producenta (wewnętrznie) w naturalny sposób kwalifikowałoby się jako rozwiązanie w zakresie zdalnego przetwarzania danych. Tak samo byłoby w przypadku, gdyby producenci polegali na zewnętrznym dostawcy usług przy opracowywaniu i projektowaniu rozwiązania (tj. „na jego odpowiedzialność"). Wyrażenie „na odpowiedzialność producenta" odnosi się do rozwiązań w zakresie zdalnego przetwarzania, które są dostosowane do potrzeb producenta. Są to przypadki, w których producent nie ogranicza się jedynie do udzielenia licencji na istniejący produkt z elementami cyfrowymi lub usługę cyfrową, które dostawca usług oferuje swoim klientom, ani na ich nieznacznie zmodyfikowane wersje. „[N]a odpowiedzialność producenta" oznacza, że oprogramowanie jest tworzone wyłącznie przez producenta lub na jego rzecz, w oparciu o dostarczone przez niego projekty i specyfikacje.

196. W rozumieniu rozwiązania w zakresie zdalnego przetwarzania danych kwestia tego, „kto obsługuje dane rozwiązanie", nie ma decydującego znaczenia, ponieważ definicja zawarta w akcie o cyberodporności odnosi się wyłącznie do projektowania i opracowywania rozwiązania w zakresie zdalnego przetwarzania danych. Jest to zgodne z podejściem przyjętym w akcie o cyberodporności, zgodnie z którym wymagania i obowiązki spoczywają na producentach produktu z elementami cyfrowymi, a nie na podmiotach zajmujących się eksploatacją. Jeżeli producenci projektują i opracowują rozwiązania, które są następnie eksploatowane przez osobę trzecią, pozostają odpowiedzialni za zgodność z zasadniczymi wymaganiami aktu o cyberodporności w odniesieniu do produktu z elementami cyfrowymi, który wprowadzają do obrotu.

197. Konieczne jest rozróżnienie między przypadkami, w których projektowaniem i opracowywaniem zajmują się producenci (lub odbywa się ono na ich odpowiedzialność), a przypadkami wykorzystywania rozwiązań stron trzecich, które nie zostały zaprojektowane ani opracowane przez producentów (lub na ich odpowiedzialność). Na przykład pomocne jest rozważenie najpowszechniejszych modeli usług w chmurze, które zapewniają użytkownikom różny stopień kontroli i które są również wymienione w motywie 12 aktu o cyberodporności, a mianowicie oprogramowania jako usługi (SaaS), platformy jako usługi (PaaS) i infrastruktury jako usługi (IaaS).

198. W przypadku rozwiązania IaaS oferowanego przez stronę trzecią producent nie zarządza bazowymi zasobami fizycznymi i wirtualnymi (takimi jak podstawowy sprzęt i hiperwizor dostawcy usług w chmurze) ani ich nie kontroluje, ale jest w stanie wdrożyć i obsługiwać dowolne oprogramowanie wykorzystujące takie zasoby, np. systemy operacyjne i aplikacje. Takie oprogramowanie jest projektowane i opracowywane przez producenta lub na jego odpowiedzialność i w związku z tym może kwalifikować się jako rozwiązanie w zakresie zdalnego przetwarzania danych (o ile spełnia pozostałe elementy definicji).

199. W przypadku rozwiązania PaaS oferowanego przez stronę trzecią producent wdraża własną (opracowaną lub nabytą) aplikację, wykorzystując języki programowania i środowiska wykonawcze zapewniane przez dostawcę usług w chmurze, oraz włącza aplikację do swojego produktu z elementami cyfrowymi. Producent ma kontrolę nad aplikacją i ewentualnie nad ustawieniami konfiguracji środowiska wykonawczego. Aplikacja jest zatem zaprojektowana i opracowana przez producenta lub na jego odpowiedzialność i w związku z tym może kwalifikować się jako rozwiązanie w zakresie zdalnego przetwarzania danych (o ile spełnia pozostałe elementy definicji).

200. W przypadku rozwiązania SaaS oferowanego przez stronę trzecią dostawca SaaS oferuje producentowi w pełni opracowaną aplikację, która ma być włączona do produktu z elementami cyfrowymi producenta. Producent ma ograniczoną zdolność do zarządzania ustawieniami konfiguracyjnymi aplikacji dostosowanymi do konkretnego użytkownika. Aplikacja nie jest zatem zaprojektowana i opracowana przez producenta ani na jego odpowiedzialność.

201. Jeżeli jednak niektóre elementy nie kwalifikują się jako rozwiązanie w zakresie zdalnego przetwarzania danych (np. hiperwizor w przypadku infrastruktury IaaS strony trzeciej, system operacyjny w przypadku rozwiązania PaaS strony trzeciej lub aplikacja SaaS strony trzeciej), ale są włączone do produktu z elementami cyfrowymi w sposób, który wpływa na jego bezpieczeństwo, takie rozwiązania należy uznać za podobne do komponentów będących własnością strony trzeciej. Producent jest zobowiązany do zidentyfikowania i oceny ryzyka związanego z włączaniem tych elementów oraz do zaradzenia temu ryzyku poprzez wdrożenie zasadniczych wymagań dotyczących samego produktu z elementami cyfrowymi. W stosownych przypadkach mogą temu towarzyszyć funkcje bezpieczeństwa udostępnione przez dostawcę usług w chmurze za pośrednictwem jego modelu współodpowiedzialności, w przypadku gdy producent wykorzystuje lub konfiguruje te funkcje w celu przeciwdziałania zidentyfikowanemu ryzyku. Ponadto oczekuje się, że producent będzie wypełniał obowiązek podobny do obowiązku dochowania należytej staranności, o którym mowa w art. 13 ust. 5, w odniesieniu do bezpieczeństwa tych komponentów, w sposób proporcjonalny do ryzyka, jakie rozwiązanie zdalne stwarza dla bezpieczeństwa produktu z elementami cyfrowymi.

202. W związku z tym można podsumować, że:

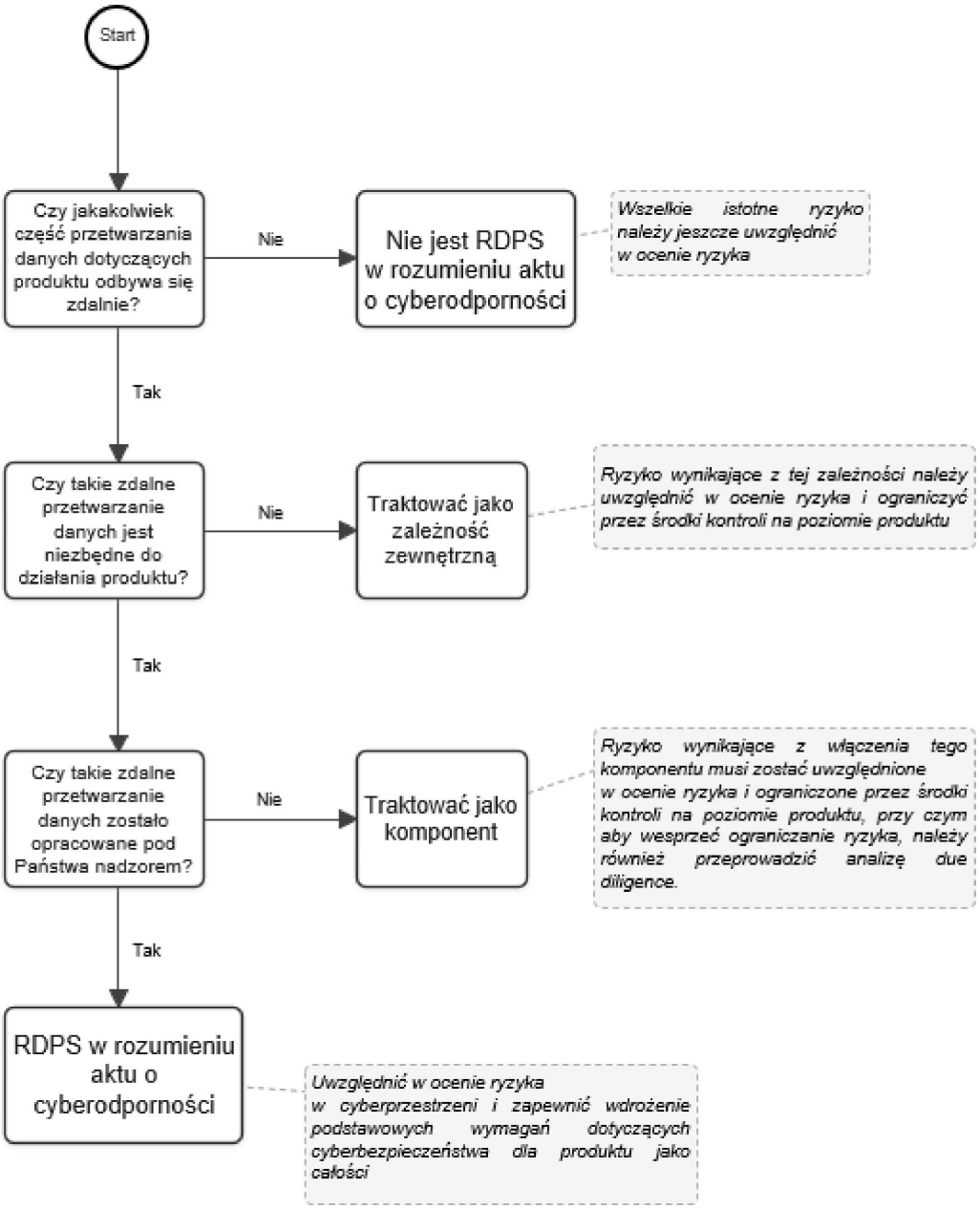
a) Aby przetwarzanie danych kwalifikowało się jako rozwiązanie w zakresie zdalnego przetwarzania danych, odpowiedź na oba pytania zadane w sekcjach *8.1.2 Czy brak takiego przetwarzania danych spowodowałby, że produkt z elementami cyfrowymi nie będzie mógł wykonywać jednej ze swoich funkcji?* i *8.1.3 Czy oprogramowanie zostało zaprojektowane i opracowane przez producenta lub na jego odpowiedzialność?* musi być twierdząca.

b) Jeżeli odpowiedź na pytanie zadane w sekcji *8.1.2 Czy brak takiego przetwarzania danych spowodowałby, że produkt z elementami cyfrowymi nie będzie mógł wykonywać jednej ze swoich funkcji?* jest przecząca, producenci powinni ocenić ryzyko wynikające z istnienia takiego przetwarzania danych w ramach przeprowadzanej przez siebie oceny ryzyka.

c) Jeżeli odpowiedź na pytanie postawione w sekcji *8.1.2 Czy brak takiego przetwarzania danych spowodowałby, że produkt z elementami cyfrowymi nie będzie mógł wykonywać jednej ze swoich funkcji?* jest twierdząca, ale odpowiedź na pytanie zadane w sekcji *8.1.3 Czy oprogramowanie zostało zaprojektowane i opracowane przez producenta lub na jego odpowiedzialność?* jest przecząca, producenci powinni traktować rozwiązanie przyjęte przez stronę trzecią jako komponent. W ramach oceny ryzyka producenci powinni ocenić ryzyko wynikające z włączenia takiego rozwiązania i odpowiednio je ograniczyć. Ponadto producenci powinni dochować należytej staranności.

Rys. 9:

Schemat przedstawiający ustalenie, czy produkt z elementami cyfrowymi zawiera rozwiązanie w zakresie zdalnego przetwarzania danych (RDPS)



8.2. Praktyczne i techniczne konsekwencje rozwiązań w zakresie zdalnego przetwarzania danych oraz korzystania z rozwiązań stron trzecich

203. W akcie o cyberodporności stosuje się podejście oparte na analizie ryzyka, które jest zapisane w art. 13 ust. 2 i 3, a także w pierwszym zasadniczym wymaganiu określonym w załączniku I część I, zgodnie z którym „produkty z elementami cyfrowymi należy projektować, opracowywać i produkować tak, by zapewniały odpowiedni poziom cyberbezpieczeństwa stosownie do ryzyka". W związku z tym przy stosowaniu wymagań aktu o cyberodporności do rozwiązań w zakresie zdalnego przetwarzania danych oraz do zmniejszania ryzyka wynikającego z usług stron trzecich włączonych do produktu z elementami cyfrowymi należy rozważyć podejście oparte na analizie ryzyka.

204. Po pierwsze, producenci powinni (i) wskazać w dokumentacji technicznej, że ich produkt z elementami cyfrowymi jest wyposażony w rozwiązanie w zakresie zdalnego przetwarzania danych lub wykorzystuje rozwiązania zdalne stron trzecich, oraz (ii) opisać takie rozwiązania. Jeżeli to samo rozwiązanie w zakresie zdalnego przetwarzania danych obsługuje kilka produktów z elementami cyfrowymi, należy je zadeklarować w dokumentacji technicznej każdego z tych produktów. Dokumentację dotyczącą rozwiązania w zakresie zdalnego przetwarzania danych obsługującego kilka produktów z elementami cyfrowymi można ponownie wykorzystać przy ocenie zgodności kolejnych produktów.

205. Jak wskazano w motywie 11, rozwiązania w zakresie zdalnego przetwarzania danych stanowiące część produktu z elementami cyfrowymi, a zatem podlegające ocenie zgodności tego produktu, powinny ograniczać się do tych modułów oprogramowania, które odpowiadają za funkcjonalność produktu z elementami cyfrowymi, oraz do interfejsów, z których moduły te korzystają w celu współpracy z usługami zewnętrznymi. Pozostałe systemy zaplecza, które realizują dalsze przetwarzanie i z którymi produkt z elementami cyfrowymi nie wchodzi w bezpośrednią interakcję, nie są uznawane za rozwiązania w zakresie zdalnego przetwarzania danych.

206. Te systemy zaplecza pozostają jednak zależnościami zewnętrznymi, które należy uwzględnić w ramach oceny ryzyka w cyberprzestrzeni i ograniczyć za pomocą środków na poziomie produktu. W rzeczywistości ocena ryzyka przeprowadzona przez producenta powinna uwzględniać: (i) ryzyko związane z rozwiązaniem w zakresie zdalnego przetwarzania danych; (ii) ryzyko związane z poleganiem na rozwiązaniach zdalnych stron trzecich (podobnie jak w przypadku komponentów stron trzecich); oraz (iii) ryzyko związane ze środowiskiem produktu (np. podstawowy sprzęt komputerowy). Producenci powinni wdrożyć środki kontroli w zakresie bezpieczeństwa samego produktu z elementami cyfrowymi, aby ograniczyć to ryzyko.

207. Ponadto w ramach oceny zgodności lub wypełniania obowiązków w zakresie należytej staranności związanych z usługami zdalnymi świadczonymi przez strony trzecie, na poparcie oceny producenta można ponownie wykorzystać następującą niewyczerpującą listę dokumentów potwierdzających:

a) dowód wypełnienia obowiązków wynikających z rozporządzenia wykonawczego Komisji (UE) 2024/2690;

b) dowód wypełnienia obowiązków wynikających z rozporządzenia (UE) 2022/2554 (akt w sprawie operacyjnej odporności cyfrowej);

c) oświadczenie o zgodności lub certyfikat uzyskany w ramach europejskiego programu certyfikacji cyberbezpieczeństwa (przyjętego na mocy rozporządzenia (UE) 2019/881 – aktu o cyberbezpieczeństwie);

d) dowód zgodności z normą ISO/IEC 27017:2015 lub ISO/IEC 27001:2022.

208. Ponadto w swoich kontaktach z dostawcami usług zdalnych będącymi osobami trzecimi producenci muszą wdrożyć najbardziej odpowiednie środki bezpieczeństwa w oparciu o przeprowadzoną przez siebie ocenę ryzyka (i, w stosownych przypadkach, przy wsparciu modelu wspólnej odpowiedzialności dostawcy). Te środki ograniczające ryzyko powinny obejmować środki kontroli bezpieczeństwa produktów z elementami cyfrowymi oraz weryfikację środków bezpieczeństwa zapewnianych przez samych dostawców zewnętrznych (należyta staranność). Narzędziem ograniczającym takie ryzyko może być włączenie gwarancji bezpieczeństwa do umów o gwarantowanym poziomie usług zawieranych z dostawcami zewnętrznymi, w tym gwarancji, że dostawcy odpowiednio radzą sobie z podatnościami. Istotna zmiana rozwiązań zapewnianych przez zewnętrznych dostawców usług zdalnych nie powinna kwalifikować się jako istotna modyfikacja produktu z elementami cyfrowymi, ponieważ elementy te nie wchodzą w zakres odpowiedzialności producenta. W ramach swoich obowiązków w zakresie należytej staranności oraz w celu prawidłowego ograniczenia ryzyka wynikającego z korzystania z usług dostawców będących osobami trzecimi producentów zachęca się jednak do zapewnienia, aby ich dostawcy usług w chmurze będący osobami trzecimi odpowiednio informowali ich o zmianach wprowadzanych w swoich rozwiązaniach. Na podstawie takich informacji producenci mogą być zmuszeni do zmiany swojej oceny ryzyka. W zaktualizowanej ocenie ryzyka należy uwzględnić, czy zewnętrzni dostawcy usług nadal zapewniają wystarczające gwarancje w zakresie cyberbezpieczeństwa oraz czy środki kontroli bezpieczeństwa na poziomie produktu są nadal odpowiednie. W niektórych przypadkach producenci mogą być zmuszeni do zmodyfikowania takich środków kontroli lub do zmiany dostawców usług będących osobami trzecimi.

8.3. **Przypadki użycia rozwiązań w zakresie zdalnego przetwarzania danych**

Aby zapewnić producentom dodatkowe praktyczne wytyczne, w niniejszej sekcji przedstawiono szereg fikcyjnych przypadków użycia opisujących typowe produkty z elementami cyfrowymi, które wykorzystują zdalne przetwarzanie danych, oraz ilustrujących, czy takie przetwarzanie kwalifikuje się jako rozwiązanie w zakresie zdalnego przetwarzania danych w rozumieniu aktu o cyberodporności.

8.3.1. *Aplikacja bankowości mobilnej*

Podmiot finansowy wprowadza do obrotu aplikację bankowości mobilnej. Systemy zaplecza aplikacji obsługują m.in. uwierzytelnianie, autoryzację, zarządzanie rachunkiem i płatności. Podmiot finansowy stosuje strategię hybrydową opartą zarówno na infrastrukturze własnej, jak i na zdalnych rozwiązaniach stron trzecich w celu obsługi funkcji aplikacji. Należą do nich:

Infrastruktura utrzymywana na własnych serwerach, opracowana przez podmiot finansowy:

— Klient otwiera aplikację bankowości mobilnej i jest uwierzytelniany za pośrednictwem interfejsu bankowego – niehostowanego rozwiązania opracowanego przez podmiot finansowy, które odbiera żądania aplikacji i zwraca odpowiednie odpowiedzi. Interfejs bankowy weryfikuje tożsamość klienta poprzez wysłanie zapytania do systemu zarządzania rachunkami i przyznaje dostęp do aplikacji.

— Klient inicjuje przelew za pośrednictwem aplikacji. Aplikacja przekazuje polecenie do interfejsu bankowego, który wysyła odpowiednie żądanie do systemu rejestru.

— System zarządzania rachunkami i system rejestru, oba utrzymywane na własnych serwerach, ale logicznie oddzielone od interfejsu bankowego, rejestrują transakcję.

— System rejestru zwraca status transakcji do interfejsu bankowego, który przedstawia wynik klientowi.

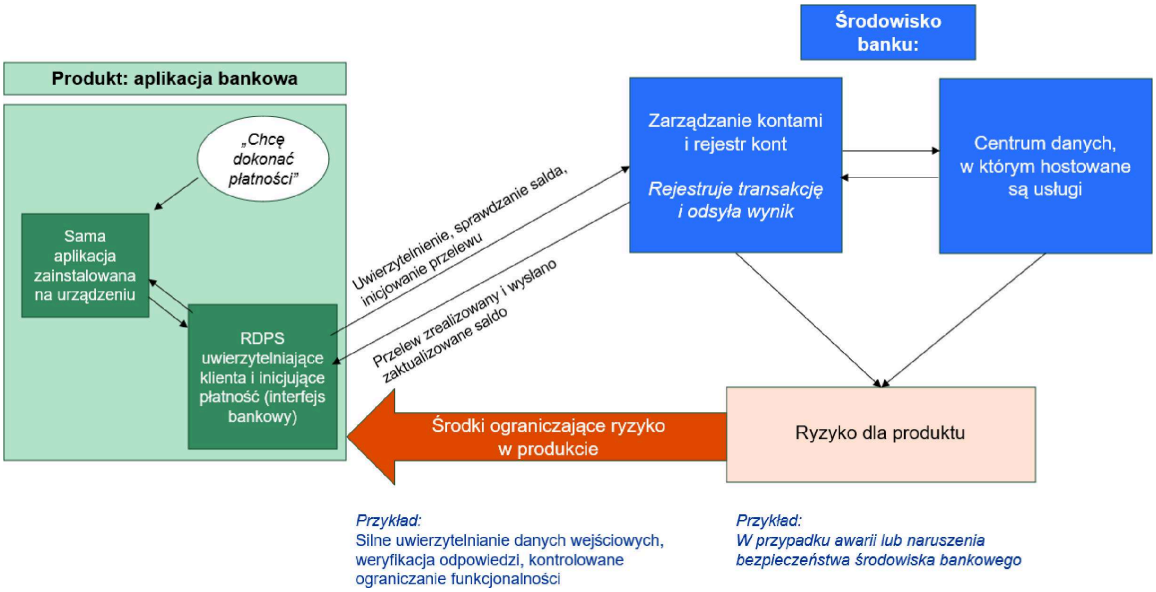
Konsekwencje dla rozwiązania w zakresie zdalnego przetwarzania danych:

— Interfejs bankowy jest niezbędny, aby aplikacja mogła wykonywać swoje funkcje, a mianowicie uwierzytelnianie klienta, przekazywanie poleceń klienta, w tym instrukcji płatniczych i poleceń przelewu, oraz zwracanie informacji o stanie rachunku po operacji. Interfejs bankowy został zaprojektowany i opracowany na odpowiedzialność producenta. Ponieważ odpowiedź na oba pytania przedstawione we wcześniejszych sekcjach jest twierdząca, interfejs bankowy należy uznać za rozwiązanie w zakresie zdalnego przetwarzania danych. Należy je zatem uwzględnić w ocenie ryzyka w cyberprzestrzeni oraz w procesie wdrażania zasadniczych wymagań dotyczących produktu z elementami cyfrowymi jako całości. Dalsze przetwarzanie przekazanego polecenia, w szczególności rejestrowanie transakcji w systemach zarządzania rachunkami i rejestru, ich rozrachunek i rozliczanie, odbywa się za pomocą systemów, z którymi aplikacja nie wchodzi w bezpośrednią interakcję i które w związku z tym nie stanowią rozwiązania w zakresie zdalnego przetwarzania danych.

— System zarządzania rachunkami i system rejestru nie kwalifikują się jako rozwiązanie w zakresie zdalnego przetwarzania danych w kontekście aplikacji bankowej. Aplikacja nie wchodzi z nimi w bezpośrednią interakcję (zamiast tego wchodzi w interakcję z interfejsem bankowym, który z kolei korzysta z tych systemów). Chociaż ich dostępność może być niezbędna do realizacji danej funkcji, akt o cyberodporności obejmuje tylko te części systemu, które wchodzą w bezpośrednią interakcję z produktem z elementami cyfrowymi. W związku z tym nie są one objęte rozwiązaniem w zakresie zdalnego przetwarzania danych dla celów aktu o cyberodporności. Systemy te pozostają jednak zależnościami zewnętrznymi, które mogą powodować znaczne ryzyko w cyberprzestrzeni w odniesieniu do produktu z elementami cyfrowymi. Na przykład naruszenie bezpieczeństwa systemu rejestru mogłoby umożliwić atakującemu wpływ na wyniki transakcji, które są następnie wyświetlane w aplikacji. Producent jest zatem zobowiązany do zidentyfikowania i oceny tego ryzyka w ramach oceny ryzyka w cyberprzestrzeni oraz do ograniczenia go za pomocą środków na poziomie produktu, takich jak silne uwierzytelnianie interfejsów zaplecza, ochrona integralności danych dotyczących transakcji, bezpieczne kanały komunikacji i weryfikacja odpowiedzi otrzymanych przez aplikację.

Rys. 10:

Schematyczne przedstawienie aplikacji bankowej wykorzystującej rozwiązanie w zakresie zdalnego przetwarzania danych (RDPS)



Usługa SaaS świadczona przez stronę trzecią w zakresie obsługi klienta:

— Podmiot finansowy włącza do swojej aplikacji rozwiązanie do obsługi klienta za pomocą czatu, opracowane i obsługiwane przez dostawcę będącego stroną trzecią; dostawca ten napisał kod serwera czatu, zbudował interfejs użytkownika i obsługuje infrastrukturę, na której czat jest wdrożony (tj. model SaaS).

— Gdy klient inicjuje wniosek o wsparcie, aplikacja łączy klienta z usługą strony trzeciej w celu nawiązania sesji czatu i obsługi przepływu komunikatów, nie udzielając stronie trzeciej dostępu do podstawowych systemów bankowych.

Konsekwencje dla rozwiązania w zakresie zdalnego przetwarzania danych:

— Rozwiązanie w postaci czatu do obsługi klienta jest niezbędne, aby produkt z elementami cyfrowymi mógł pełnić jedną ze swoich funkcji, ale nie zostało zaprojektowane i opracowane przez podmiot finansowy ani na jego odpowiedzialność; w związku z tym nie stanowi ono rozwiązania w zakresie zdalnego przetwarzania danych. Należy je jednak traktować jak komponent strony trzeciej. Korzystanie z tej usługi strony trzeciej może stwarzać ryzyko w cyberprzestrzeni dla aplikacji bankowej, na przykład gdyby atakujący korzystał z kanału czatu w celu podszycia się pod bank lub dostarczania użytkownikom złośliwych treści. Podmiot finansowy musi uwzględnić to ryzyko w swojej ocenie ryzyka w cyberprzestrzeni i ograniczyć je za pomocą środków na poziomie produktu, takich jak odizolowanie funkcji czatu od podstawowych funkcji bankowych, kontrola przepływu danych oraz weryfikacja treści. Należy również dochować należytej staranności w odniesieniu do usługi SaaS.

8.3.2. *Inteligentny termostat*

Inteligentny termostat umożliwia użytkownikom kontrolowanie temperatury w domu za pomocą aplikacji mobilnej. Aplikacja mobilna i inteligentny termostat wykorzystują zdalne przetwarzanie danych do wymiany danych (np. żądania podwyższenia temperatury) i przechowywania danych (np. preferencji użytkownika). Funkcje te zostały opracowane i zaprojektowane na odpowiedzialność producenta, ale działają w oparciu o podstawową infrastrukturę fizyczną i wirtualną zapewnianą przez stronę trzecią (usługa IaaS strony trzeciej).

Ponieważ inteligentny termostat nie byłby w stanie wykonywać swoich inteligentnych funkcji bez tego zdalnego przetwarzania danych, jego brak spowodowałby, że produkt z elementami cyfrowymi nie mógłby wykonywać jednej ze swoich funkcji. Ponadto oprogramowanie zostało opracowane i zaprojektowane na odpowiedzialność producenta inteligentnego termostatu. W związku z tym zdalne przetwarzanie danych kwalifikuje się jako rozwiązanie w zakresie zdalnego przetwarzania danych zgodnie z definicją zawartą w akcie o cyberodporności.

W celu zapewnienia zgodności z aktem o cyberodporności producent inteligentnego termostatu musi udokumentować rozwiązanie w zakresie zdalnego przetwarzania danych, a także fakt korzystania z usług IaaS świadczonych przez stronę trzecią w dokumentacji technicznej produktu z elementami cyfrowymi, w tym szczegóły dotyczące zawartej umowy o świadczenie usług. Producent musi uwzględnić te elementy w ocenie ryzyka, która obejmuje przeznaczenie i racjonalnie przewidywalne wykorzystanie produktu z elementami cyfrowymi. Producent wdraża zasadnicze wymagania aktu o cyberodporności stosownie do ryzyka związanego z rozwiązaniem w zakresie zdalnego przetwarzania danych. W przypadku usługi IaaS świadczonej przez stronę trzecią producent musi zapewnić, aby środki bezpieczeństwa zapewniane przez dostawcę będącego stroną trzecią były odpowiednie, lub podjąć odpowiednie środki w odniesieniu do infrastruktury. W pierwszym przypadku producent mógłby na przykład zwrócić się o przedstawienie dowodów potwierdzających spełnienie obowiązków wynikających z dyrektywy NIS 2.

8.3.3. *Czytnik książek elektronicznych*

Producent oprogramowania czytników książek elektronicznych korzysta z usługi przechowywania w modelu SaaS świadczonej przez stronę trzecią w celu przechowywania książek elektronicznych zakupionych przez klientów i umożliwienia im dostępu do ich książek. Brak tej usługi przechowywania spowodowałby, że produkt z elementami cyfrowymi nie mógłby wykonywać jednej ze swoich funkcji, ale usługa przechowywania w modelu SaaS świadczona przez stronę trzecią nie jest opracowywana przez producenta ani na jego odpowiedzialność; dostawca usługi SaaS udostępnia ją klientom w każdym przypadku użycia.

Usługa przechowywania w modelu SaaS nie odpowiada definicji rozwiązania w zakresie zdalnego przetwarzania danych. Producent czytnika książek elektronicznych korzysta jednak z tej usługi zewnętrznej, aby jego produkt z elementami cyfrowymi funkcjonował, i w związku z tym musi uwzględnić związane z tym ryzyko w swojej ocenie ryzyka w cyberprzestrzeni. Producent czytnika książek elektronicznych powinien traktować usługę SaaS jak komponent. Producent musi wdrożyć odpowiednie środki bezpieczeństwa na poziomie produktu, takie jak bezpieczne uwierzytelnianie, szyfrowanie i ochrona integralności komunikacji z usługą przechowywania. Należyta staranność przy wyborze i integracji dostawcy usługi SaaS również będzie wspierać wypełnianie obowiązków przez producenta, tak aby produkt z elementami cyfrowymi jako całość mógł spełniać zasadnicze wymagania.

8.3.4. *Robot przemysłowy*

Zadaniem robota przemysłowego jest podnoszenie części. Robot przesyła informacje zebrane za pomocą kamer do usługi zdalnej zaprojektowanej i opracowanej przez producenta. Usługa ta działa w oparciu o infrastrukturę fizyczną i wirtualną zapewnianą przez dostawcę usług będącego stroną trzecią (usługa IaaS strony trzeciej). Usługa w chmurze oblicza położenie części w oparciu o obrazy przesyłane przez kamery i wysyła polecenia z powrotem do robota, aby ten podniósł części.

Brak tego przetwarzania danych uniemożliwiłby robotowi przemysłowemu podnoszenie części, a tym samym wykonywanie jednej z jego funkcji. Ponadto oprogramowanie działające na infrastrukturze zostało zaprojektowane i opracowane przez producenta. Oprogramowanie zaprojektowane i opracowane przez producenta spełnia definicję rozwiązania w zakresie zdalnego przetwarzania danych.

Producent robota przemysłowego musi udokumentować rozwiązanie w zakresie zdalnego przetwarzania danych, a także fakt korzystania z usług IaaS świadczonych przez stronę trzecią w dokumentacji technicznej produktu z elementami cyfrowymi (w tym szczegóły dotyczące zawartej umowy o świadczenie usług). Producent musi również uwzględnić te elementy w ocenie ryzyka, która obejmuje przeznaczenie i racjonalnie przewidywalne wykorzystanie produktu z elementami cyfrowymi. Producent wdraża zasadnicze wymagania aktu o cyberodporności dotyczące produktu z elementami cyfrowymi, w tym swojego rozwiązania w zakresie zdalnego przetwarzania danych, stosownie do ryzyka. Należyta staranność przy wyborze dostawcy usługi IaaS również pomoże producentowi w wypełnieniu jego obowiązków. Producent mógłby na przykład zwrócić się o przedstawienie dowodów potwierdzających spełnienie obowiązków wynikających z dyrektywy NIS 2.

8.3.5. *Sieć komórkowa*

Smartfon korzysta z sieci 5G w celu zapewnienia użytkownikom połączenia internetowego, rozmów telefonicznych i wiadomości (łączność ruchoma). Sieć komórkowa jest rozwijana i projektowana przez operatorów telekomunikacyjnych. Sieć obejmuje małe komórki i wieże komórkowe oraz inne urządzenia sieciowe.

Produkt z elementami cyfrowymi powinien być w stanie prawidłowo połączyć się z siecią; jest to jedna z jego funkcji. To, czy sieć ta działa, czy też nie, nie ma jednak znaczenia dla ustalenia, czy produkt z elementami cyfrowymi działa prawidłowo. Sieć jest jedynie kanałem komunikacyjnym i nie jest konieczna do tego, aby produkt z elementami cyfrowymi mógł realizować swoją funkcję „prawidłowego łączenia się z siecią". Podobnie kabla ethernetowego, routera lub sygnału Wi-Fi nie uznaje się za przetwarzanie danych, którego brak spowodowałby, że produkt z elementami cyfrowymi nie mógłby wykonywać jednej ze swoich funkcji, lecz raczej za element umożliwiający komunikację/łączność.

W związku z tym sieć komórkowa nie spełnia definicji rozwiązania w zakresie zdalnego przetwarzania danych. Sieci nie należy uznawać za komponent strony trzeciej, ponieważ do produktu z elementami cyfrowymi nie włączono żadnego oprogramowania, a produkt jedynie korzysta z tej sieci. W związku z tym nie jest konieczne, aby producent wywiązywał się z obowiązków w zakresie należytej staranności wobec dostawcy sieci.

9. **ELEMENTY DODATKOWE**

9.1. **Obowiązki w zakresie zgłaszania**

209. Zgodnie z art. 14 ust. 1 i 3 aktu o cyberodporności producent jest zobowiązany do jednoczesnego zgłaszania CSIRT-owi wyznaczonemu na koordynatora oraz ENISA (i) jakichkolwiek aktywnie wykorzystywanych podatności zawartych w jego produkcie z elementami cyfrowymi, o których się dowiedział; oraz (ii) każdego poważnego incydentu mającego wpływ na bezpieczeństwo produktu z elementami cyfrowymi, o którym się dowie.

210. Zgodnie z art. 69 ust. 3 i art. 71 ust. 2 zdanie drugie obowiązek zapewnienia zgodności z art. 14 ma zastosowanie od dnia 11 września 2026 r. do wszystkich produktów z elementami cyfrowymi objętych zakresem aktu o cyberodporności, w tym produktów z elementami cyfrowymi wprowadzonych do obrotu przed dniem 11 grudnia 2027 r. Ponadto w przeciwieństwie do obowiązków w zakresie postępowania w przypadku wykrycia podatności, które obowiązują wyłącznie przez okres wsparcia produktu, obowiązki w zakresie sprawozdawczości nadal mają zastosowanie po zakończeniu wsparcia dla produktu z elementami cyfrowymi. W przypadku gdy produkt z elementami cyfrowymi został wprowadzony do obrotu przed dniem 11 grudnia 2027 r. lub gdy okres wsparcia dla niego dobiegł końca, producent nie jest zobowiązany do wypełniania obowiązków w zakresie postępowania w przypadku wykrycia podatności określonych w załączniku I część II.

211. Należy przypomnieć, że obowiązek zgłaszania takich zdarzeń ma zastosowanie od momentu, gdy producent dowie się, że podatność jest aktywnie wykorzystywana lub że wystąpił poważny incydent, który doprowadził do naruszenia bezpieczeństwa jego produktu z elementami cyfrowymi. W związku z tym wytyczne dotyczące tego, kiedy uznaje się, że producent dowiedział się o tym, powinny pomóc producentom w określeniu momentu, od którego zaczynają biec mające zastosowanie terminy zgłaszania.

212. Producenci mogą podlegać porównywalnym obowiązkom zgłaszania na mocy różnych aktów prawnych UE. Aby zapewnić spójną interpretację pojęcia „uzyskania wiedzy" oraz ułatwić producentom wypełnianie tych obowiązków, niniejsze wytyczne są dostosowane do motywu 31 rozporządzenia wykonawczego Komisji (UE) 2024/2690 i sekcji II lit. A) wytycznych 9/2022 dotyczących zgłaszania naruszeń ochrony danych osobowych na podstawie RODO.

213. W niektórych przypadkach podejrzane zdarzenie wykryje producent lub osoba trzecia, taka jak osoba fizyczna, klient, podmiot, organ, organizacja medialna lub inne źródło, zwróci jego uwagę na potencjalny incydent lub podatność. W takich przypadkach producent powinien niezwłocznie ocenić podejrzane zdarzenie w celu ustalenia, czy stanowi ono aktywnie wykorzystywaną podatność lub poważny incydent mający wpływ na bezpieczeństwo produktu z elementami cyfrowymi. Należy zatem uznać, że producent uzyskał wiedzę, gdy po dokonaniu takiej wstępnej oceny ma wystarczającą pewność, że: (i) podatność zawarta w jego produkcie z elementami cyfrowymi jest aktywnie wykorzystywana; lub (ii) wystąpił poważny incydent, który doprowadził do naruszenia bezpieczeństwa jego produktu z elementami cyfrowymi.

214. W związku z tym moment, w którym można uznać, że producent jest świadomy, będzie zależał od okoliczności konkretnej aktywnie wykorzystywanej podatności lub poważnego incydentu. W niektórych przypadkach od samego początku będzie stosunkowo jasne, że podatność jest aktywnie wykorzystywana lub że poważny incydent wpływa na bezpieczeństwo produktu z elementami cyfrowymi. W innych przypadkach ustalenie, czy na produkt z elementami cyfrowymi ma wpływ podatność i czy podatność ta jest wykorzystywana przez podmiot działający w złym zamiarze, lub czy incydent ma wpływ na bezpieczeństwo produktu z elementami cyfrowymi, może zająć trochę czasu. Należy jednak położyć nacisk na bezzwłoczne podjęcie działań w celu przeprowadzenia wstępnej oceny, aby ustalić, czy takie warunki są rzeczywiście spełnione, w szczególności w przypadku gdy podatność może stwarzać znaczne ryzyko, a jeżeli tak, należy podjąć działania naprawcze i dokonać zgłoszenia zgodnie z aktem o cyberodporności.

215. Ponadto struktura obowiązków w zakresie zgłaszania wymaga, aby producenci stopniowo aktualizowali swoje zgłoszenia w miarę postępów w dochodzeniach wewnętrznych, gdy ich wiedza na temat aktywnie wykorzystywanej podatności lub incydentu staje się bardziej szczegółowa. W szczególności producenci są zobowiązani do przedłożenia wczesnego ostrzeżenia zawierającego ograniczone informacje bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od uzyskania wiedzy. Dodatkowe informacje należy następnie przekazać w ramach zgłoszenia, którego należy dokonać bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od uzyskania wiedzy („72-godzinne zgłoszenie"). Pełne sprawozdanie należy przedłożyć w ciągu 14 dni po udostępnieniu środka naprawczego lub łagodzącego w odniesieniu do aktywnie wykorzystywanych podatności lub w ciągu jednego miesiąca od 72-godzinnego zgłoszenia o poważnych incydentach.

216. Jak przypomniano również w sekcji *3.3.1 Stałe wsparcie i zapewnienie opłacalności wolnego i otwartego oprogramowania*, opiekunowie otwartego oprogramowania są również zobowiązani do zgłaszania aktywnie wykorzystywanych podatności zgodnie z art. 24 ust. 3 ([30]). Obowiązek ten ma zastosowanie w momencie uzyskania wiedzy o aktywnie wykorzystywanej podatności, a nie tylko w przypadku, gdy podatność istnieje w bazie kodu wolnego i otwartego oprogramowania, w odniesieniu do którego podmiot ten jest opiekunem. W praktyce, ponieważ komponenty wolnego i otwartego oprogramowania są zazwyczaj łączone na dalszym etapie z innymi produktami z elementami cyfrowymi, opiekun prawdopodobnie dowie się o aktywnym wykorzystywaniu podatności za pośrednictwem zgłoszeń osób trzecich, które identyfikują takie wykorzystywanie w odniesieniu do komponentów wolnego i otwartego oprogramowania włączanych do innych produktów z elementami cyfrowymi. Może to mieć miejsce na przykład wtedy, gdy producent produktu z elementami cyfrowymi wykryje aktywne wykorzystywanie podatności w komponencie wolnego i otwartego oprogramowania włączonego do jego własnego produktu i zgłosi to opiekunowi tego komponentu; lub gdy użytkownik lub ekspert w obszarze bezpieczeństwa znajdzie dowody na wykorzystywanie podatności w komponencie wolnego i otwartego oprogramowania włączonego do produktu z elementami cyfrowymi i zgłosi to aktywne wykorzystywanie opiekunowi komponentu.

217. Należy również wyjaśnić, że ponieważ obowiązek zgłaszania aktywnie wykorzystywanych podatności ma zastosowanie, gdy producent dowie się o aktywnym wykorzystywaniu, nie jest on zobowiązany do zgłaszania podatności, o których aktywnym wykorzystywaniu dowiedział się już przed dniem 11 września 2026 r. (data rozpoczęcia stosowania obowiązku zgłaszania). W związku z tym akt o cyberodporności nie wymaga zgłaszania takich podatności z mocą wsteczną. Obowiązek ten ma natomiast zastosowanie w przypadku, gdy producent wiedział o podatności przed dniem 11 września 2026 r., ale nie wiedział w tym czasie o jej aktywnym wykorzystywaniu (ponieważ do tej pory nie doszło do jej wykorzystania albo producent nie dowiedział się o niej). Jeżeli następnie po dniu 11 września 2026 r. dojdzie do aktywnego wykorzystania lub producent dowie się o nim, podatność tę uznaje się za aktywnie wykorzystywaną podatność podlegającą obowiązkowi zgłaszania.

218. Podobnie producent ma obowiązek zgłaszania jedynie aktywnie wykorzystywanych podatności zawartych w jego produkcie z elementami cyfrowymi. W przypadku gdy produkt z elementami cyfrowymi zawiera aktywnie wykorzystywaną podatność pochodzącą z komponentu strony trzeciej, producent tego produktu z elementami cyfrowymi jest zobowiązany do zgłoszenia tej aktywnie wykorzystywanej podatności. Jeżeli jednak producent jest świadomy, że komponent strony trzeciej zawiera podatność, ale podatność ta (i) nie może zostać wykorzystana w jego produkcie z elementami cyfrowymi (np. ponieważ kod podatny na atak nie jest dostępny) albo (ii) nie została wykorzystana w jego produkcie z elementami cyfrowymi, podatność ta nie kwalifikuje się jako aktywnie wykorzystywana podatność zawarta w jego produkcie z elementami cyfrowymi, a zatem nie podlega obowiązkowi zgłoszenia przez tego producenta. Producent ten może nadal dobrowolnie zgłosić tę podatność, zgodnie z art. 15 aktu o cyberodporności. Jest on również zobowiązany do spełnienia wymagań dotyczących postępowania w przypadku wykrycia podatności określonych w załączniku I część II do aktu o cyberodporności, a także do zgłoszenia podatności osobie lub podmiotowi produkującemu lub utrzymującemu komponent, zgodnie z art. 13 ust. 6 i jak wyjaśniono bardziej szczegółowo w sekcji *9.2.1 Zgłaszanie na wyższym szczeblu łańcucha dostaw i udostępnianie poprawek zabezpieczeń*.

([30]) O ile opiekun jest zaangażowany w opracowywanie produktu z elementami cyfrowymi.

219. Po otrzymaniu informacji o wystąpieniu aktywnie wykorzystywanej podatności lub poważnego incydentu producenci są również zobowiązani, zgodnie z art. 14 ust. 8, do poinformowania użytkowników, na których incydent ma wpływ, oraz, w stosownych przypadkach, wszystkich użytkowników. Jeżeli nie uczynią tego w odpowiednim czasie, CSIRT-y, które otrzymały takie 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.

220. Zgodnie z podejściem opartym na analizie ryzyka przyjętym w akcie o cyberodporności obowiązek informowania użytkowników określony w art. 14 ust. 8 należy stosować w sposób oparty na analizie ryzyka i proporcjonalny. W szczególności przekazanie informacji o aktywnie wykorzystywanej podatności lub poważnym incydencie nie oznacza, że takie informacje muszą być podawane do wiadomości publicznej lub ujawniane bez rozróżnienia. W stosownych przypadkach oraz w świetle charakteru produktu z elementami cyfrowymi, użytkowników, których to dotyczy, oraz potencjalnego wpływu podatności lub incydentu, producenci mogą ograniczyć ujawnianie szczegółowych informacji odpowiednim użytkownikom lub klientom, których to dotyczy. Dotyczy to w szczególności produktów z elementami cyfrowymi wykorzystywanych w środowiskach wrażliwych lub o kluczowym znaczeniu, w przypadku których publiczne ujawnienie szczegółów technicznych mogłoby samo w sobie zwiększyć ryzyko w cyberprzestrzeni lub ułatwić dalsze wykorzystywanie.

221. Po odpowiednim usunięciu lub złagodzeniu podatności właściwe może być szersze ujawnienie. Dotyczyłoby to na przykład sytuacji, w której ujawnienie przyczynia się do zwiększenia ogólnej świadomości lub umożliwia użytkownikom zweryfikowanie, że ich produkty z elementami cyfrowymi nie są już narażone na tę podatność. W takich przypadkach poziom szczegółowości i termin szerszego ujawnienia powinny pozostać proporcjonalne i uwzględniać rezydualne ryzyko wykorzystania podatności, charakter produktu z elementami cyfrowymi oraz interesy użytkowników, których to dotyczy. Ponadto w załączniku I część II pkt 4 zobowiązano producentów do publicznego ujawniania informacji o naprawionych podatnościach po udostępnieniu aktualizacji zabezpieczeń.

9.2. **Postępowanie w przypadku wykrycia podatności**

9.2.1. *Zgłaszanie na wyższym szczeblu łańcucha dostaw i udostępnianie poprawek zabezpieczeń*

222. W art. 13 ust. 6 aktu o cyberodporności nakłada się na producentów obowiązek zgłaszania podatności w komponentach włączonych do ich produktów osobie lub podmiotowi produkującemu lub utrzymującemu ten komponent („zgłaszanie na wyższym szczeblu łańcucha dostaw”).

223. Producenci są zobowiązani do zgłaszania na wyższym szczeblu łańcucha dostaw wyłącznie w odniesieniu do wersji komponentu, który włączają do swojego produktu. W przypadku gdy osoba lub podmiot wytwarzające lub utrzymujące komponent ustanowiły politykę bezpieczeństwa, skoordynowane procesy ujawniania podatności lub wyznaczone kanały zgłaszania podatności, producenci powinni dokonywać zgłoszeń zgodnie z nimi, w szczególności w przypadku gdy przedwczesne ujawnienie nienaprawionych podatności mogłoby zwiększyć ryzyko w cyberprzestrzeni. Ponadto, aby zmniejszyć obciążenie podmiotów odpowiedzialnych za utrzymanie na wyższym szczeblu łańcucha dostaw, w szczególności w przypadku projektów opartych na otwartym oprogramowaniu, producenci nie są zobowiązani do dokonywania zgłoszeń na wyższym szczeblu łańcucha dostaw, jeżeli mogą potwierdzić, że osoba lub podmiot produkujący dany komponent lub go utrzymujący wie o istnieniu danej podatności. Producentów zachęca się do podejmowania uzasadnionych kroków w celu uniknięcia składania zduplikowanych zgłoszeń, na przykład poprzez sprawdzanie publicznie dostępnych baz danych dotyczących podatności, porad bezpieczeństwa dotyczących konkretnych projektów lub uznanych systemów śledzenia problemów przed dokonaniem zgłoszenia na wyższym szczeblu łańcucha dostaw.

224. Producenci są zobowiązani do zgłaszania na wyższym szczeblu łańcucha dostaw tylko tych podatności, które istnieją w samym włączonym komponencie, a nie podatności, które istnieją w wyniku łączenia komponentu z innym kodem opracowanym przez producenta lub w wyniku włączenia innych komponentów. Mogą jednak wystąpić sytuacje, w których włączenie komponentu do konkretnego produktu z elementami cyfrowymi prowadzi do zaobserwowania pewnych zachowań, interakcji lub istotnych z punktu widzenia bezpieczeństwa właściwości tego komponentu, które nie były widoczne lub nie były łatwe do zidentyfikowania w oderwaniu od siebie. W takich przypadkach producentów zachęca się do przekazywania tych informacji osobie lub podmiotowi produkującemu lub utrzymującemu dany komponent, aby wspierać dobre praktyki postępowania w przypadku wykrycia podatności mające na celu ułatwienie wdrożenia skutecznych środków zaradczych i poprawę ogólnego bezpieczeństwa ekosystemu komponentu.

225. Ponadto producenci nie są również zobowiązani do zgłaszania podatności na wyższym szczeblu łańcucha dostaw, jeżeli komponent nie posiada już podmiotu odpowiedzialnego za utrzymanie lub jeżeli producent nie polega już na pierwotnym podmiocie odpowiedzialnym za utrzymanie w odniesieniu do nowych wersji lub poprawek zabezpieczeń. W takich przypadkach zachęca się jednak producenta do informowania użytkowników tego komponentu za pomocą racjonalnych środków alternatywnych, np. za pośrednictwem istniejących mechanizmów społecznościowych (takich jak listy mailingowe lub zgłoszenia problemów) lub za pośrednictwem publicznych rejestrów podatności.

226. Ponadto zgodnie z art. 13 ust. 6 producenci, którzy opracowali modyfikację oprogramowania w celu wyeliminowania podatności we włączonym komponencie, są zobowiązani do udostępniania tej modyfikacji oprogramowania („poprawka zabezpieczeń") osobie lub podmiotowi produkującemu lub utrzymującemu komponent („udostępnianie na wyższym szczeblu łańcucha dostaw").

227. W przypadku gdy producenci są zobowiązani do udostępnienia poprawki zabezpieczeń zgodnie z art. 13 ust. 6, poprawka ta powinna, w stosownych przypadkach, być udostępniona w formacie nadającym się do odczytu maszynowego, w sposób umożliwiający jej łatwą weryfikację oraz, w stosownych przypadkach, integrację przez osobę lub podmiot produkujący lub utrzymujący dany komponent. W przypadku gdy komponent jest komponentem wolnym i opartym na otwartym oprogramowaniu, poprawka zabezpieczeń powinna być udostępniona w sposób zgodny z licencją tego komponentu, na przykład poprzez udostępnianie jej na podstawie tej samej licencji lub licencji, która umożliwia podmiotowi odpowiedzialnemu za utrzymanie dystrybucję poprawki na podstawie jego własnej licencji. W przypadku gdy podmiot odpowiedzialny za utrzymanie tego komponentu posiada wytyczne dotyczące sposobu udostępniania poprawek zabezpieczeń, producent powinien stosować się do tych wytycznych.

228. W akcie o cyberodporności nie wymaga się jednak od producentów zapewnienia, aby ich poprawki zabezpieczeń były koniecznie akceptowane przez osobę lub podmiot produkujący lub utrzymujący komponent. Nie są oni również zobowiązani do zapewnienia, aby poprawki te były koniecznie włączane do repozytorium kodu komponentu, na przykład w sytuacji gdy podmiot odpowiedzialny za utrzymanie może preferować inną opcję w celu naprawienia problemu. Podobnie producenci nie są zobowiązani do akceptowania proponowanej poprawki opracowanej przez osobę odpowiedzialną za utrzymanie komponentu i mogą preferować złagodzenie skutków problemu w inny odpowiedni sposób.

229. W niektórych przypadkach osoba lub podmiot produkujący lub utrzymujący komponent mógł już zapewnić poprawkę zabezpieczeń w celu wyeliminowania podatności, ale producent wdraża inną strategię ograniczania ryzyka (np. poprzez zmianę konfiguracji). W takich przypadkach w akcie o cyberodporności nie wymaga się od producenta udostępniania modyfikacji innej części systemu na wyższym szczeblu łańcucha dostaw. Zachęca się jednak producenta do takiego postępowania, jeżeli może to pomóc osobie lub podmiotowi utrzymującemu komponent.

9.2.2. *Znane podatności nadające się do wykorzystania*

230. Jedno z zasadniczych wymagań określonych w załączniku I część I do aktu o cyberodporności stanowi, że na podstawie oceny ryzyka w cyberprzestrzeni, o której mowa w art. 13 ust. 2, oraz, w stosownych przypadkach, produkty z elementami cyfrowymi muszą być udostępniane na rynku bez znanych nadających się do wykorzystania podatności.

231. W art. 3 pkt 41 zdefiniowano „nadającą się do wykorzystania podatność" jako „podatność, która może zostać skutecznie wykorzystana przez atakującego w praktycznych warunkach eksploatacji". Nie wszystkie podatności można wykorzystać w praktycznych warunkach eksploatacji, a niektóre podatności można wykorzystać wyłącznie w warunkach teoretycznych (np. w laboratorium lub w symulacji) lub nie w warunkach, jakie wystąpiłyby w środowisku operacyjnym produktu z elementami cyfrowymi.

232. Zgodnie z aktem o cyberodporności producenci mają obowiązek posiadać odpowiednią politykę i stosowne procedury postępowania z potencjalnymi podatnościami zgłoszonymi przez źródła wewnętrzne lub zewnętrzne oraz ich eliminowania (art. 13 ust. 8). Nie określono w nim jednak wyraźnie, kiedy nadającą się do wykorzystania podatność należy uznać za znaną producentowi, co powoduje powstanie obowiązku spełnienia tego zasadniczego wymagania w momencie wprowadzenia do obrotu.

233. Podatność należy uznać za znaną, gdy jest ona wymieniona w odpowiednich publicznie dostępnych bazach danych dotyczących podatności, takich jak europejska baza danych dotyczących podatności ustanowiona na podstawie art. 12 ust. 2 dyrektywy (UE) 2022/2555 lub inne renomowane bazy danych dotyczących podatności.

234. Ponadto podatność może być również znana, gdy producent został o niej powiadomiony za pośrednictwem informacji niepublicznych, na przykład poprzez skoordynowane ujawnienie przez eksperta w obszarze bezpieczeństwa lub poprzez własne wewnętrzne testy i analizy producenta, w tym na przykład podczas korzystania z usług opartych na sztucznej inteligencji. Podobnie podatność może być znana, jeżeli została publicznie i szeroko zrelacjonowana w wiarygodnych mediach, w tym w specjalistycznych publikacjach dotyczących cyberbezpieczeństwa lub w ogólnych środkach masowego przekazu.

235. Niemniej jednak sam fakt zgłoszenia lub wykrycia podatności nie oznacza jeszcze, że można ją wykorzystać w praktyce lub że ma ona zastosowanie do konkretnego produktu z elementami cyfrowymi. Producent będzie musiał zbadać tę kwestię i potwierdzić prawdziwość takich informacji oraz możliwość ich zastosowania do własnego produktu z elementami cyfrowymi. W związku z tym między pierwszym zgłoszeniem podatności a jej potwierdzeniem może upłynąć pewien czas. Jak wskazano w sekcji *9.1 Obowiązki w zakresie zgłaszania*, należy położyć nacisk na szybkie działania w celu zbadania sprawy i zareagowania.

236. Ponadto spoczywający na producentach obowiązek spełnienia zasadniczych wymagań określonych w załączniku I część I ma zastosowanie w momencie wprowadzenia do obrotu, zgodnie z art. 13 ust. 1. W praktyce może się zdarzyć, że nowe potencjalnie nadające się do wykorzystania podatności zostaną wykryte na końcowych etapach cyklu opracowywania produktu z elementami cyfrowymi, w tym na krótko przed jego wprowadzeniem do łańcucha dystrybucji (i w związku z tym wprowadzeniem do obrotu).

237. Ponieważ obowiązek wprowadzania do obrotu produktów z elementami cyfrowymi bez znanych możliwych do wykorzystania podatności jest obowiązkiem opartym na analizie ryzyka, do producenta należy ustalenie, na podstawie oceny ryzyka w cyberprzestrzeni, czy produkt z elementami cyfrowymi można bezpiecznie wprowadzić do obrotu, zgodnie z aktem o cyberodporności. Alternatywnie producent może określić, że nowa podatność, o której mógł się dowiedzieć, musi zostać usunięta, zanim produkt z elementami cyfrowymi będzie mógł zostać wprowadzony do obrotu. Dokonując tego ustalenia, producenci powinni wziąć pod uwagę krytyczność, możliwość wykorzystania i potencjalny wpływ podatności, a także ryzyko wynikające z użytkowania samego produktu z elementami cyfrowymi. Mogą oni również uwzględniać ryzyko związane z opóźnieniem wprowadzenia produktu na rynek do czasu usunięcia podatności, na przykład dlatego, że nowa wersja eliminuje również inne możliwe do wykorzystania podatności lub jest niezbędna do dalszego funkcjonowania systemów krytycznych. W każdym przypadku po wprowadzeniu produktu z elementami cyfrowymi do obrotu producent nadal podlega obowiązkowi skutecznego postępowania w przypadku wykrycia podatności zgodnie z wymaganiami postępowania w przypadku wykrycia podatności określonymi w załączniku I część II.

9.2.3. *Skuteczne i regularne testy i przeglądy*

238. W załączniku I część II pkt 3 zobowiązano producentów do przeprowadzania skutecznych i regularnych testów i przeglądów produktu z elementami cyfrowymi przez cały okres wsparcia. Przeprowadzanie regularnych testów nie wymaga mechanicznego powtarzania w stałych odstępach czasu niezmienionej serii testów. Oznacza to regularne sprawdzanie, czy nowe dane wejściowe, takie jak nowo zidentyfikowane zagrożenia lub nowo wykryte podatności, wymagają aktualizacji istniejących testów, oraz odpowiednie przeprowadzanie testów.

239. Częstotliwość, szczegółowość i treść przeglądu powinny być proporcjonalne do profilu ryzyka w cyberprzestrzeni produktu z elementami cyfrowymi, jego zmian w czasie oraz stanu krajobrazu zagrożeń. W przypadku gdy w ramach przeglądu zidentyfikowane zostaną istotne nowe dane wejściowe mające wpływ na zestaw testów, należy opracować i przeprowadzić nowe lub zmodyfikowane testy produktu, aby zapewnić, że żadne podatności nie pozostaną bez odpowiedniej reakcji. Może to obejmować ponowne przeprowadzenie dotychczasowych testów, w przypadku gdy modyfikacja produktu z elementami cyfrowymi sprawia, że tego typu testy są właściwe, np. testy regresyjne.

240. W przypadku gdy przegląd nie wykaże takich danych, nie ma potrzeby opracowywania dodatkowych testów. Równolegle nadal mają zastosowanie inne obowiązki w zakresie postępowania w przypadku wykrycia podatności, w tym obowiązki w zakresie eliminowania i niwelowania podatności w odniesieniu do stwarzanego ryzyka.

9.3. **Wzajemne powiązania z innymi przepisami**

9.3.1. *Rozporządzenie (UE) 2019/2144 i rozporządzenie (UE) nr 168/2013*

241. Art. 2 ust. 2 lit. c) aktu o cyberodporności stanowi, że rozporządzenia nie stosuje się do produktów z elementami cyfrowymi, do których ma zastosowanie rozporządzenie (UE) 2019/2144. Rozporządzenie (UE) 2019/2144 stosuje się do „pojazdów kategorii M, N i O zdefiniowanych w art. 4 rozporządzenia (UE) 2018/858 oraz do układów, komponentów i oddzielnych zespołów technicznych zaprojektowanych i zbudowanych do tych pojazdów".

242. Podobnie produkty z elementami cyfrowymi objęte zakresem rozporządzenia (UE) nr 168/2013 zostały wyłączone z zakresu aktu o cyberodporności rozporządzeniem delegowanym Komisji (UE) 2025/1535. Rozporządzenie (UE) nr 168/2013 ma zastosowanie do pojazdów kategorii L oraz „do układów, komponentów i oddzielnych zespołów technicznych, a także części i wyposażenia, zaprojektowanych i skonstruowanych dla takich pojazdów" (art. 2 ust. 1).

243. Pojazdy, do których stosuje się te rozporządzenia, nie podlegają przepisom aktu o cyberodporności. Ponadto konieczne są dodatkowe wyjaśnienia dotyczące zakresu wyłączenia układów, komponentów, oddzielnych zespołów technicznych, części i wyposażenia (do celów niniejszej sekcji „komponenty") zaprojektowanych i skonstruowanych dla takich pojazdów, które uznaje się za produkty z elementami cyfrowymi w rozumieniu aktu o cyberodporności.

244. Uznaje się, że takie komponenty nie podlegają przepisom aktu o cyberodporności, pod warunkiem że są one zaprojektowane i skonstruowane wyłącznie w celu wbudowania w pojazdy objęte rozporządzeniami (UE) 2019/2144 i nr 168/2013. Jest tak niezależnie od tego, czy producent danego komponentu sprzedaje go bezpośrednio producentowi pojazdów, czy też innemu podmiotowi gospodarczemu w łańcuchu dostaw w przemyśle motoryzacyjnym, o ile ten komponent jest wyraźnie przeznaczony i nadaje się wyłącznie do ostatecznego wbudowania w te pojazdy.

245. Natomiast producent, który sprzedaje komponenty ogólnego przeznaczenia, które są produktami z elementami cyfrowymi i można je wbudować w różne rodzaje produktów, a nie wyłącznie w pojazdy objęte tymi rozporządzeniami, podlega aktowi o cyberodporności.

246. Ocena, czy dany komponent jest wprowadzany do obrotu w rozumieniu aktu o cyberodporności, musi opierać się na obiektywnych warunkach, na jakich jest on udostępniany. W przypadku gdy producent oferuje komponent, który nie jest przeznaczony wyłącznie do ostatecznego wbudowania w te pojazdy, za pośrednictwem kanałów dystrybucji otwartych dla klientów spoza łańcucha dostaw w przemyśle motoryzacyjnym, takich jak ogólne punkty sprzedaży detalicznej lub internetowe kanały sprzedaży przyjmujące zamówienia od ogółu społeczeństwa, komponent ten jest objęty zakresem stosowania aktu o cyberodporności, niezależnie od jakichkolwiek oświadczeń dotyczących jego zamierzonego zastosowania. W takich okolicznościach nie można uznać, że komponent został zaprojektowany i skonstruowany wyłącznie w celu wbudowania w pojazdy objęte rozporządzeniami (UE) 2019/2144 i nr 168/2013, a producent jest zobowiązany do przestrzegania aktu o cyberodporności. Natomiast korzystanie z ograniczonych kanałów dystrybucji między przedsiębiorstwami, ograniczonych do łańcucha dostaw w przemyśle motoryzacyjnym, może wskazywać, że został on zaprojektowany i skonstruowany wyłącznie w celu takiego wbudowania.

9.3.2. *Ważność certyfikatów badania typu UE (art. 69 ust. 1)*

247. Art. 69 ust. 1 aktu o cyberodporności stanowi, że „[c]ertyfikaty 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".

248. Należy rozumieć, że dalsza ważność takich certyfikatów i decyzji o zatwierdzeniu ogranicza się do ryzyka w cyberprzestrzeni i odpowiadających mu wymagań, które są objęte odpowiednim unijnym prawodawstwem harmonizacyjnym, na podstawie którego zostały wydane. W odniesieniu do tego ryzyka producenci nie są zobowiązani do ponownej oceny lub ponownego wykazania zgodności wyłącznie do celów aktu o cyberodporności w okresie ważności, o którym mowa w art. 69 ust. 1, w odniesieniu do produktów z elementami cyfrowymi, które zamierzają wprowadzić do obrotu w dniu 11 grudnia 2027 r. lub po tej dacie, do dnia 11 czerwca 2028 r. ([31]) Dotyczy to certyfikatów i decyzji o zatwierdzeniu wydanych w przypadku, gdy mające zastosowanie unijne prawodawstwo harmonizacyjne wymaga od producenta przeprowadzenia procedury oceny zgodności za pośrednictwem jednostki notyfikowanej, a także w przypadku, gdy producent dobrowolnie się na to zdecydował.

249. W związku z tym istnienie ważnego certyfikatu lub decyzji o zatwierdzeniu wydanych na podstawie innego unijnego prawodawstwa harmonizacyjnego nie zwalnia producentów z przeprowadzania kompleksowej oceny ryzyka w cyberprzestrzeni na podstawie aktu o cyberodporności (ani z innych obowiązków wynikających z tego aktu). Umożliwia im natomiast wykorzystanie istniejących certyfikatów jako dowodu zgodności w ramach ich procedury oceny zgodności, o ile obejmują one już odpowiednie ryzyko w cyberprzestrzeni. W przypadku gdy certyfikat lub decyzja o zatwierdzeniu są ważne na mocy innego unijnego prawodawstwa harmonizacyjnego wykraczającego poza dzień 11 czerwca 2028 r., producent może jednak powoływać się na taki certyfikat lub decyzję do celów aktu o cyberodporności wyłącznie do dnia 11 czerwca 2028 r.

250. W przypadku gdy ocena ryzyka w cyberprzestrzeni przeprowadzona zgodnie z art. 13 ust. 2 wykaże dodatkowe ryzyko nieobjęte wymaganiami w zakresie cyberbezpieczeństwa leżącymi u podstaw istniejącego certyfikatu lub decyzji o zatwierdzeniu, producenci pozostają odpowiedzialni za przeciwdziałanie temu ryzyku zgodnie z aktem o cyberodporności. W takich przypadkach zgodność wymaga oceny i ograniczenia zidentyfikowanych luk, niezależnie od tego, czy istniejący certyfikat lub decyzja o zatwierdzeniu zachowują ważność.

251. Można to zilustrować na przykładzie sytuacji, w której produkt z elementami cyfrowymi podlega wymaganiom w zakresie cyberbezpieczeństwa określonym w rozporządzeniu delegowanym Komisji (UE) 2022/30 uzupełniającym dyrektywę 2014/53/UE (akt delegowany dotyczący dyrektywy w sprawie urządzeń radiowych (RED)) oraz w którym na podstawie tych wymagań wydano certyfikat badania typu UE lub decyzję o zatwierdzeniu. W takim przypadku certyfikat lub decyzja pozostają ważne, zgodnie z art. 69 ust. 1, w odniesieniu do ryzyka w cyberprzestrzeni objętego tym certyfikatem i związanego z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w dyrektywie 2014/53/UE (dyrektywa w sprawie urządzeń radiowych).

252. W takich przypadkach producenci nie są zobowiązani, do celów aktu o cyberodporności, do ponownej oceny lub ponownego wykazania zgodności w odniesieniu do ryzyka już uwzględnionego w tych certyfikatach, dopóki odpowiedni certyfikat lub decyzja o zatwierdzeniu pozostają ważne, a w każdym razie nie dłużej niż do dnia 11 czerwca 2028 r. Obejmuje to na przykład ryzyko w cyberprzestrzeni związane z ochroną sieci, ochroną danych osobowych i prywatności lub zapobieganiem oszustwom (w zakresie, w jakim ryzyko to jest objęte tym certyfikatem) związane z wymaganiami w zakresie cyberbezpieczeństwa określonymi w dyrektywie w sprawie urządzeń radiowych i odzwierciedlone w ocenie zgodności.

253. Jeżeli jednak ocena ryzyka w cyberprzestrzeni przeprowadzona zgodnie z art. 13 ust. 2 aktu o cyberodporności wykaże dodatkowe ryzyko w cyberprzestrzeni nieobjęte tymi certyfikatami, producenci pozostają odpowiedzialni za przeciwdziałanie temu ryzyku zgodnie z aktem o cyberodporności. Może to obejmować na przykład ryzyko związane z procesami postępowania w przypadku wykrycia podatności, minimalizacją danych i zmniejszeniem powierzchni ataku lub innymi aspektami cyberbezpieczeństwa specyficznymi dla danego produktu, których nie uwzględniono w tych certyfikatach lub które w każdym razie nie są objęte zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w dyrektywie w sprawie urządzeń radiowych.

254. W związku z tym istnienie ważnego certyfikatu badania typu UE lub decyzji o zatwierdzeniu wydanej na podstawie dyrektywy w sprawie urządzeń radiowych w odniesieniu do jej zasadniczych wymagań dotyczących cyberbezpieczeństwa nie świadczy samo w sobie o pełnej zgodności z aktem o cyberodporności. Umożliwia to natomiast producentom powołanie się na ten certyfikat lub decyzję jako dowód zgodności w odniesieniu do odpowiedniego ryzyka, przy jednoczesnym zapewnieniu, aby wszelkie pozostałe lub nowo zidentyfikowane ryzyko zostało ocenione i ograniczone zgodnie z aktem o cyberodporności.

([31]) Produkty z elementami cyfrowymi wprowadzone do obrotu przed dniem 11 grudnia 2027 r. podlegają przepisom Unii mającym zastosowanie w momencie ich wprowadzenia do obrotu, a jeżeli były zgodne z tymi przepisami, mogą być sprzedawane i wprowadzane do użytku, chyba że w dniu 11 grudnia 2027 r. lub po tej dacie zostaną poddane istotnym modyfikacjom. Pojęcia „wprowadzania do obrotu" i „udostępniania na rynku" znajdują się również w sekcji *2.1 Wprowadzenie do obrotu* niniejszego dokumentu oraz w rozdziale 2 Niebieskiego przewodnika.

255. Podobnie w przypadku gdy produkt z elementami cyfrowymi podlega zasadniczym wymaganiom w zakresie zdrowia i bezpieczeństwa związanym z cyberbezpieczeństwem określonym w rozporządzeniu (UE) 2023/1230 (rozporządzenie w sprawie maszyn), mającym w pełni zastosowanie od dnia 20 stycznia 2027 r., oraz w przypadku gdy certyfikat badania typu UE lub decyzja o zatwierdzeniu zostały wydane na podstawie tych wymagań, ten certyfikat lub ta decyzja o zatwierdzeniu pozostają ważne, zgodnie z art. 69 ust. 1 aktu o cyberodporności, w odniesieniu do ryzyka w cyberprzestrzeni objętego rozporządzeniem w sprawie maszyn.

256. Dotyczy to w szczególności aspektów cyberbezpieczeństwa związanych z zabezpieczeniem przed uszkodzeniem oraz bezpieczeństwem i niezawodnością układów sterowania, określonymi w sekcjach 1.1.9 i 1.2.1 załącznika III do rozporządzenia w sprawie maszyn. W odniesieniu do tego ryzyka producenci nie są zobowiązani, do celów aktu o cyberodporności, do ponownej oceny lub ponownego wykazania zgodności, dopóki odpowiedni certyfikat lub decyzja o zatwierdzeniu pozostają ważne, a w każdym razie nie dłużej niż do dnia 11 czerwca 2028 r. Ma to zastosowanie, o ile ryzyko to zostało uwzględnione w ramach oceny zgodności przeprowadzonej na podstawie rozporządzenia w sprawie maszyn.

257. Podobnie jak w przypadku wspomnianych powyżej zasadniczych wymagań w zakresie cyberbezpieczeństwa określonych w dyrektywie w sprawie urządzeń radiowych, w przypadku gdy ocena ryzyka w cyberprzestrzeni przeprowadzona na podstawie art. 13 ust. 2 aktu o cyberodporności wykaże dodatkowe ryzyko w cyberprzestrzeni, które nie jest objęte odpowiednim certyfikatem wydanym na podstawie rozporządzenia w sprawie maszyn i które jest związane z wymaganiami w zakresie cyberbezpieczeństwa określonymi w tym rozporządzeniu, producenci pozostają odpowiedzialni za przeciwdziałanie temu ryzyku zgodnie z aktem o cyberodporności.