Akt o cyberodporności – cele i ogólny zakres regulacji

Cyberpolicy NASK

Autor: Piotr Słowiński

NASK-PIB
ul. Kolska 12
01–045 Warszawa
NIP: 521 04 17 157
Regon: 010464542
KRS: 0000012938
nask@nask.pl
+48 22 380 82 00
+48 22 380 82 01
nask.pl

NASK

Spis treści

1. Wstęp

Rozporządzenie Parlamentu Europejskiego i Rady 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, w skrócie zwane także aktem o cyberodporności (Cyber Resilience Act, CRA) zostało opublikowane 24 października 2024 r.[1] i weszło w życie 10 grudnia 2024 r. Główne obowiązki wprowadzone regulacją będą miały zastosowanie od 11 grudnia 2027 r.

2. Cele i zakres regulacji

CRA ma na celu zapewnienie prawidłowego funkcjonowania rynku wewnętrznego poprzez **tworzenie warunków do rozwoju bezpiecznych produktów z elementami cyfrowymi** oraz umożliwienie użytkownikom **uwzględnianie cyberbezpieczeństwa przy wyborze i użytkowaniu takich produktów**. Wzmacnia tym samym **znaczenie norm cyberbezpieczeństwa** w przypadku wspomnianych kategorii rzeczy.

Dotychczasowe uregulowania unijne, w tym akt o cyberbezpieczeństwie[2] i dyrektywa NIS 2[3], nie obejmowało bezpośrednio obowiązkowych wymagań dotyczących bezpieczeństwa produktów z elementami cyfrowymi. CRA ma za zadanie wypełnić tę lukę, ustanawiając zharmonizowane wymogi, co pozwoli na usunięcie przeszkód w swobodnym przepływie tego rodzaju produktów i zwiększenie cyberbezpieczeństwa zarówno dla konsumentów, jak i przedsiębiorstw.

2.1. Zakres podmiotowy

Akt o cyberodporności obejmuje szereg podmiotów gospodarczych w łańcuchu dostaw produktów z elementami cyfrowymi, przypisując im konkretne obowiązki. Obowiązki producentów, importerów i dystrybutorów obejmują zapewnienie, że produkty z elementami cyfrowymi spełniają wymagania cyberbezpieczeństwa, są odpowiednio instalowane, utrzymywane i używane zgodnie z przeznaczeniem.

---

[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), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:L_202402847

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)

[3] 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)

Tabela 1. Wybrane podmioty objęte aktem o cyberodporności

RODZAJ PODMIOTU GOSPODARCZEGO	DEFINICJA PODMIOTU
Producent	Osoba fizyczna lub prawna, która opracowuje lub wytwarza produkty z elementami cyfrowymi, lub zleca ich projektowanie, opracowanie lub wytworzenie, i wprowadza je do obrotu pod własną nazwą lub znakiem towarowym, odpłatnie lub bezpłatnie.
Zarządca wolnego i otwartego oprogramowania (Open-source software steward)	Osoba prawna, inna niż producent, której celem jest systematyczne zapewnienie stałego wsparcia dla rozwoju konkretnych produktów wolnego i otwartego oprogramowania przeznaczonych do działalności komercyjnej orazktóra zapewnia żywotność tych produktów.
Upoważniony przedstawiciel	Osoba fizyczna lub prawna z siedzibą w Unii, która otrzymała pisemne pełnomocnictwo od producenta do działania w jego imieniu w określonych zadaniach.
Importer	Osoba fizyczna lub prawna z siedzibą w Unii, która wprowadza do obrotu produkt z elementami cyfrowymi noszący nazwę lub znak towarowy osoby mającej siedzibę poza Unią.
Dystrybutor	Osoba fizyczna lub prawna w łańcuchu dostaw, inna niż producent lub importer, która udostępnia produkt z elementami cyfrowymi na rynku unijnym, nie wpływając na jego właściwości.
Inne osoby fizyczne lub prawne	Podlegające obowiązkom związanym z wytwarzaniem lub udostępnianiem produktów z elementami cyfrowymi na rynku zgodnie z niniejszym rozporządzeniem

Zgodnie z aktem muszą zostać także spełnione wymagania dotyczące procesów obsługi podatności, które muszą być obowiązkowo wdrożone przez producentów, aby zapewnić cyberbezpieczeństwo produktów przez cały cykl ich życia. Zgodnie z tekstem przyjętym przez PE **okres wsparcia produktów** z elementami cyfrowymi **w zakresie obsługi podatności nie może być krótszy niż 5 lat**. Wyjątkiem od tej zasady jest sytuacja, gdy cykl życia danego produktu jest krótszy niż ten czas – wtedy wsparcie musi być dawane przez cały ten czas.

2.2. Zakres przedmiotowy

Zakresem przedmiotowym regulacji są objęte wszystkie **produkty z elementami cyfrowymi**, które mają **bezpośrednie** lub **pośrednie połączenie z urządzeniem lub siecią**. Produktami z elementami cyfrowymi będą zarówno oprogramowanie, sprzęt, jak i rozwiązania w zakresie zdalnego przetwarzania danych (choćby powiązane usługi w chmurze lub infrastruktura zaplecza, które są integralne dla funkcjonowania produktu), w tym elementy oprogramowania lub sprzętu wprowadzane niezależnie do obrotu[4].

Warto podkreślić, że CRA wykracza poza producenta produktu końcowego i obejmuje także dostawców poszczególnych komponentów. Jest to bezpośrednia odpowiedź na rosnącą kompleksowość łańcuchów dostaw i świadomość, że podatności często powstają już na poziomie komponentów.

Istnieją jednak wyłączenia co do zakresu przedmiotowego CRA. Regulacja nie będzie obejmowała produktów z elementami cyfrowymi certyfikowanych zgodnie z:

- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz
- Dyrektywą Parlamentu Europejskiego i Rady 2014/90/UE z dnia 23 lipca 2014 r. w sprawie wyposażenia morskiego.

Rozporządzenie nie ma zastosowania do następujących kategorii produktów z elementami cyfrowymi:

- Produkty objęte rozporządzeniami (UE) 2017/745 (wyroby medyczne) i (UE) 2017/746 (wyroby medyczne do diagnostyki in vitro);
- Produkty objęte rozporządzeniem (UE) 2019/2144 (wymogi homologacji typu dla pojazdów silnikowych);
- Produkty certyfikowane zgodnie z rozporządzeniem (UE) 2018/1139 (bezpieczeństwo lotnictwa cywilnego);
- Urządzenia objęte zakresem dyrektywy 2014/90/UE (wyposażenie morskie);
- Części zamienne wprowadzane do obrotu w celu zastąpienia identycznych komponentów w produktach z elementami cyfrowymi, wyprodukowane zgodnie z tymi samymi specyfikacjami;
- Produkty opracowane lub zmodyfikowane wyłącznie do celów bezpieczeństwa narodowego lub obrony;
- Produkty specjalnie zaprojektowane do przetwarzania informacji niejawnych;

[4] Art. 3 pkt (1) CRA

- Obowiązki wynikające z rozporządzenia nie pociągają za sobą obowiązku dostarczania informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obrony państw członkowskich.

2.2.1. Wymagania w zakresie cyberbezpieczeństwa produktów

CRA wprowadza **horyzontalne wymagania w zakresie cyberbezpieczeństwa** dotyczące **projektowania, rozwoju i produkcji produktów z elementami cyfrowymi** oraz **obowiązki podmiotów gospodarczych** w tym zakresie, to znaczy: producentów, upoważnionych przedstawicieli, importerów, dystrybutorów lub każdą inną osobę fizyczną lub prawną. Obejmuje to branie pod uwagę kwestii cyberbezpieczeństwa w całym cyklu życia produktów lub procesy obsługi podatności uwzględniając przy tym tak istotne elementy jak łańcuch dostaw. Ponadto warunkiem jest także to, że produkty są prawidłowo zainstalowane oraz utrzymywane, a także wykorzystywane zgodnie z ich przeznaczeniem lub w warunkach które daje się racjonalnie przewidzieć. W stosownych przypadkach konieczne jest także, aby były aktualizowane.

Produkt z elementami cyfrowymi musi zapewniać **odpowiedni poziom cyberbezpieczeństwa** wobec **zidentyfikowanych przez producenta ryzyk**. Obowiązkowa ocena ryzyka produktów z elementami cyfrowymi w zakresie cyberbezpieczeństwa musi zostać wykonana przez producenta. Oznacza to, że produkty z elementami cyfrowymi są dostępne na rynku, jeżeli spełniają wymogi określone w CRA, a producent wdrożył procedury zgodne z przepisami rozporządzenia. Oznacz to, że muszą:

- być wolne od znanych, możliwych do wykorzystania podatności;
- co do zasady posiadać bezpieczną konfigurację domyślną, w tym opcję przywrócenia do stanu początkowego, chyba że uzgodniono inaczej dla produktów dostosowanych do potrzeb określonego użytkownika biznesowego;
- umożliwiać eliminowanie podatności poprzez aktualizacje bezpieczeństwa: w tym automatyczne aktualizacje bezpieczeństwa instalowane w odpowiednim czasie jako ustawienie domyślne; użytkownicy muszą dysponować jasnym i łatwym w użyciu mechanizmem rezygnacji, a także otrzymywać powiadomienia o dostępnych aktualizacjach i mieć możliwość ich tymczasowego odroczenia;
- zapewniać ochronę przed nieautoryzowanym dostępem, w tym poprzez odpowiednie mechanizmy kontroli, takie jak systemy uwierzytelniania, tożsamości lub zarządzania dostępem, oraz możliwość zgłaszania możliwego nieautoryzowanego dostępu;
- chronić poufność danych przechowywanych, przesyłanych lub w inny sposób przetwarzanych (osobowych lub innych), na przykład poprzez szyfrowanie odpowiednich danych odłożonych lub przesyłanych przy użyciu najnowocześniejszych mechanizmów i innych środków technicznych;
- chronić integralność danych przechowywanych, przesyłanych lub w inny sposób przetwarzanych (osobowych lub innych), a także poleceń, programów i konfiguracji przed nieautoryzowaną manipulacją lub modyfikacją przez użytkownika, a także powiadamiać o ich uszkodzeniach;

- przetwarzać tylko niezbędne dane (minimalizacja danych) czyli takie, które są adekwatne, istotne i ograniczone do tego, co jest niezbędne do ich zamierzonego celu;
- chronić dostępność podstawowych funkcji nawet po incydencie;
- minimalizować negatywny wpływ produktów lub urządzeń podłączonych do internetu na usługi świadczone przez inne urządzenia lub sieci;
- ograniczać powierzchnie ataku poprzez odpowiednie projektowanie, opracowywanie i produkcję produktów;
- zmniejszać wpływ incydentów;
- dostarczać informacji związanych z bezpieczeństwem dzięki rejestrowaniu i monitorowaniu odpowiedniej aktywności wewnętrznej, takiej jak dostęp do danych, usług lub funkcji lub ich modyfikacja, z mechanizmem opt-out dla użytkownika;
- umożliwiać bezpieczne i łatwe usuwanie danych i ustawień, a jeśli mogą one być przekazywane do innych produktów lub systemów, musi to odbywać się w sposób bezpieczny.

2.2.2. Ocena zgodności

Na mocy przepisów CRA domyślnie obowiązuje domniemanie, że **produkty spełniające normy zharmonizowane (lub ich części)** opublikowane w Dzienniku Urzędowym Unii Europejskiej **spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa**. Podobnie domniemywa się w przypadku produktów, dla których wydano unijną deklarację zgodności lub certyfikat w ramach europejskiego programu certyfikacji cyberbezpieczeństwa.

Zgodnie z przepisami CRA producent dokonuje oceny zgodności produktu z elementami cyfrowymi z procedurami wprowadzanymi przez niego. Celem jest ustalenie czy zostały spełnione zasadnicze wymagania w zakresie cyberbezpieczeństwa. Wybór konkretnej procedury oceny zgodności należy do producenta, natomiast ich katalog został wskazany w rozporządzeniu:

- kontrola wewnętrzna (zgodnie z modułem A),
- badanie typu UE (zgodnie z modułem B),
- ocena zgodności oparta na pełnym zapewnieniu jakości (zgodnie z modułem H),
- europejski program certyfikacji cyberbezpieczeństwa - o ile jest dostępny i ma zastosowanie.

Przy wyborze odpowiedniej procedury oceny zgodności producent bierze także pod uwagę klasę lub rodzaj produktu - klasa I, klasa II, produkty krytyczne, wolne i otwarte oprogramowanie. W zależności od tego dostępny katalog procedur może być węższy – dla wybranych klas lub rodzajów można zastosować tylko niektóre procedury określone w CRA.

2.2.3. Dokumentacja techniczna

Jednym z istotnych elementów oceny zgodności produktu jest także **obowiązek sporządzenia dokumentacji technicznej**, która zawiera wszelkie istotne dane dotyczące środków zastosowanych przez producenta. Ma ona

na celu zapewnienie, że produkt i procedury spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa. Dokumentacja ta powinna być stale aktualizowana, ale jej pierwsza wersja musi zostać sporządzona przed wprowadzeniem do obrotu produktu z elementami cyfrowym.

Dokumentacja techniczna jest kluczowym elementem procesu oceny zgodności. Musi ona zawierać wszystkie istotne dane lub szczegóły dotyczące środków zastosowanych przez producenta w celu zapewnienia zgodności produktu z elementami cyfrowymi i procesów wdrożonych przez producenta z podstawowymi wymaganiami cyberbezpieczeństwa, takie jak:

- Ogólny opis produktu, jego przeznaczenie, wersje oprogramowania, zdjęcia/ilustracje (dla sprzętu);
- Informacje o projektowaniu, rozwoju, produkcji i obsłudze podatności (w tym zestawienie podstawowych materiałów do produkcji oprogramowania, politykę CVD, adres kontaktowy do zgłaszania podatności, rozwiązania techniczne dla bezpiecznej dystrybucji aktualizacji);
- Ocenę ryzyka cyberbezpieczeństwa i sposób zastosowania wymagań z Załącznika I;
- Informacje dotyczące określenia okresu wsparcia;
- Wykaz zastosowanych norm zharmonizowanych, wspólnych specyfikacji lub europejskich schematów certyfikacji cyberbezpieczeństwa (w przypadku częściowego zastosowania lub braku zastosowania – opis alternatywnych rozwiązań);
- Sprawozdania z testów;
- Kopia deklaracji zgodności UE;
- W stosownych przypadkach zestawienie podstawowych materiałów do produkcji oprogramowania, jeśli zażąda tego organ nadzoru rynku i jest to konieczne do sprawdzenia zgodności z Załącznikiem I.

2.2.4. Deklaracja zgodności i oznakowanie CE

Zgodnie z CRA producenci mają obowiązek dołączyć do produktu **deklarację zgodności UE** albo uproszczoną deklarację zgodności UE, ale w tym przypadku musi ona także zawierać adres witryny internetowej, gdzie będzie dostępna pełna jej wersja. Deklaracja zgodności jest formalnym oświadczeniem producenta, że produkt spełnia podstawowe wymagania cyberbezpieczeństwa określone w Załączniku I do CRA. Musi być także sporządzona według przyjętego wzoru. Tym samym poprzez sporządzenie deklaracji producent przyjmuje na siebie odpowiedzialność za zgodność produktu z wymogami określonymi w akcie o cyberodporności.

W tym kontekście należy wspomnieć również o **oznakowaniu CE**, za pomocą którego producent deklaruje, że produkt z elementami cyfrowymi oraz wdrożone przez niego procedury spełniają zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w CRA lub innym odpowiednim unijnym ustawodawstwie harmonizacyjnym. Oznakowanie CE umieszcza się na produkcie w sposób widoczny, czytelny i trwały przed jego wprowadzeniem do obrotu. W przypadku oprogramowania oznacza to umieszczenie go na deklaracji zgodności lub na stronie internetowej, łatwo i bezpośrednio dostępnej dla konsumentów.

2.3. Wsparcie dla małych i średnich przedsiębiorstw

W ramach wsparcie małych i średnich przedsiębiorstw (MŚP) oraz start-upów państwa członkowskie mogą organizować działania w zakresie zwiększające świadomość, prowadzić szkolenia oraz ustanawiać piaskownice regulacyjne w zakresie cyberodporności. Ponadto KE zapewnia MŚP wytyczne i wsparcie finansowe oraz może określić **uproszczony formularz dokumentacji technicznej** dla mikroprzedsiębiorstw i małych przedsiębiorstw.

Dodatkowo CRA zawiera uregulowanie możliwości zawierania przez UE **umów o wzajemnym uznawaniu** z państwami trzecimi w celu wspierania i ułatwiania handlu międzynarodowego. Przy ewentualnym rozpatrywaniu możliwości nawiązania tego rodzaju relacji gospodarczych na poziomie unijnym należy wziąć pod uwagę poziom rozwoju technicznego i podejście do oceny zgodności przez potencjalnego partnera handlowego.

3. Nadzór i egzekwowanie przepisów

Każde państwo członkowskie jest zobowiązane do wyznaczenia **jednego lub więcej organów nadzoru rynku odpowiedzialnych za skuteczne wdrożenie CRA**. Mogą to być zarówno istniejące, jak i nowo utworzone organy. Organy te są zobowiązane do regularnej współpracy i wymiany informacji z różnymi odpowiednimi podmiotami, w tym z krajowymi organami certyfikacji cyberbezpieczeństwa, zespołami reagowania na incydenty komputerowe (CSIRT) i ENISA (szczególnie w zakresie nadzoru nad obowiązkami zgłaszania aktywnie wykorzystywanych podatności i poważnych incydentów), innymi organami nadzoru rynku wyznaczonymi na mocy innych unijnych przepisów harmonizacyjnych oraz organami nadzorującymi unijne prawo o ochronie danych.

Państwa członkowskie muszą zapewnić, że wyznaczone organy nadzoru rynku dysponują odpowiednimi zasobami finansowymi i technicznymi, w tym narzędziami automatyzacji procesów i zasobami ludzkimi z niezbędnymi umiejętnościami w zakresie cyberbezpieczeństwa. Każde państwo członkowskie ma również wyznaczyć jedno biuro łącznikowe odpowiedzialne za reprezentowanie skoordynowanego stanowiska organów nadzoru rynku i pomoc we współpracy między organami w różnych państwach członkowskich.

Ponadto w celu jednolitego stosowania CRA ustanowiono dedykowaną **grupę współpracy administracyjnej (ADCO)**, która składa się z przedstawicieli wyznaczonych organów nadzoru rynku i, w stosownych przypadkach, przedstawicieli biur łącznikowych. ADCO zajmuje się również kwestiami związanymi z działaniami nadzoru rynku dotyczącymi obowiązków nałożonych na zarządców wolnego i otwartego oprogramowania.

W ramach zapobiegania występowaniu ryzyka lub neutralizowania ich negatywnego wpływu organy nadzoru rynku mogą uzgadniać wspólne działania z innymi odpowiednimi organami w celu zapewnienia cyberbezpieczeństwa i ochrony konsumentów. Dodatkowo Komisja lub ENISA mogą proponować wspólne działania organom nadzoru rynku na podstawie wskazań potencjalnej niezgodności w wielu państwach członkowskich.

3.1. Działania kontrolne

Organy nadzoru rynku mają przeprowadzać jednoczesne skoordynowane akcje kontrolne dotyczące określonych produktów z elementami cyfrowymi lub ich kategorii w celu sprawdzenia zgodności z CRA lub wykrycia jego naruszeń. Mogą one także obejmować kontrole produktów z elementami cyfrowymi nabytych pod ukrytą tożsamością. Kontrole są koordynowane przez KE, chyba że uczestniczące w nich organy nadzoru rynku uzgodnią inaczej. W stosownych przypadkach koordynator akcji kontrolnej podaje jej zagregowane wyniki do publicznej wiadomości.

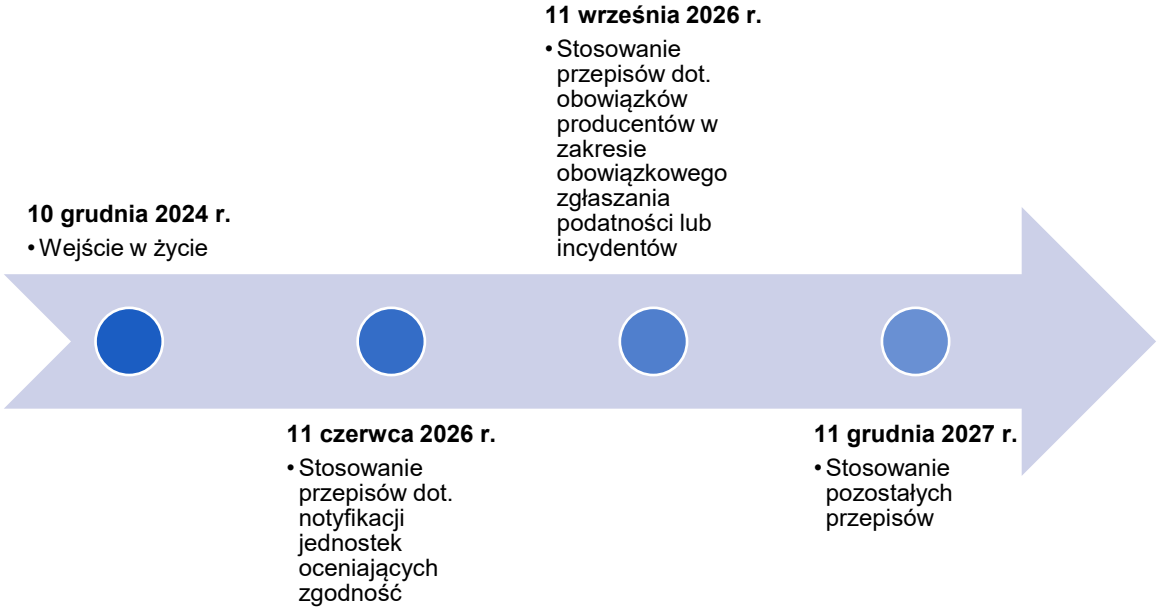
Organy nadzoru rynku uczestniczące w akcjach kontrolnych mogą korzystać z uprawnień w zakresie postępowania kontrolnego określone w CRA w zakresie nadzoru rynku oraz egzekwowania prawa, a także wszelkich innych uprawnień nadanych im na mocy przepisów prawa krajowego.

4. Dalsze kroki

Przewidziany w aktualnym projekcie **CRA czas na wdrożenie nowych wymagań** to **36 miesięcy od dnia wejścia w życie** przepisów aktu – co oznacza, że **przepisy CRA będą stosowane od 11 grudnia 2027 r.** Jedynymi wyjątkami od tej zasady są:

- artykuł 14 (obowiązki wytwórców w zakresie podatności) oraz
- rozdział IV (art. 35 – 51, Notyfikacja jednostek oceniających zgodność przez państwa członkowskie).

Ten pierwszy ma być stosowany **21 miesięcy** od dnia wejścia w życie (11 września 2026 r.), a drugi – **18 miesięcy** (11 czerwca 2026 r.). Oznacza to, że w tych dwóch przypadkach konieczne jest zapewnienie zgodności wcześniej niż to jest w przypadku pozostałych przepisów.



5. Podsumowanie i wnioski

- Akt o cyberodporności wprowadza kompleksowe wymagania dotyczące cyberbezpieczeństwa dla produktów z elementami cyfrowymi, mające na celu zwiększenie poziomu cyberbezpieczeństwa, a tym samym także zaufania użytkowników oraz atrakcyjności tego typu produktów na rynku. Uzupełnia jednocześnie istniejące akty prawne w obszarze cyberbezpieczeństwa (np. NIS 2, akt o cyberbezpieczeństwie), koncentrując się na produktach z elementami cyfrowymi.
- CRA wprowadza obowiązek uwzględniania cyberbezpieczeństwa w całym cyklu życia produktów z elementami cyfrowymi, w tym poprzez wdrożenie procesów obsługi podatności oraz zapewnienie wsparcia w zakresie aktualizacji bezpieczeństwa przez co najmniej 5 lat (lub przez cały cykl życia produktu, jeśli jest krótszy).
- Regulacja obejmuje szeroki katalog podmiotów w łańcuchu dostaw – od producentów po dystrybutorów – przypisując im konkretne obowiązki w zakresie zapewnienia zgodności produktów z wymaganiami cyberbezpieczeństwa. CRA ustanawia horyzontalne wymagania dotyczące projektowania, rozwoju i produkcji produktów z elementami cyfrowymi, w tym obowiązek przeprowadzenia oceny ryzyka oraz zapewnienia mechanizmów ochrony poufności, integralności i dostępności danych.
- Współpraca i wymiana informacji organów odpowiedzialnych za wdrożenie CRA z organami ustanowionymi na gruncie aktu o cyberbezpieczeństwie, dyrektywy NIS 2 czy innych regulacji zapewnia, że informacje zebrane w ramach nadzoru rynku (np. dotyczące konkretnych podatności produktów lub trendów niezgodności) mogą być bezpośrednio wykorzystywane do tworzenia krajowych i unijnych danych wywiadowczych o zagrożeniach, umożliwiając szybsze i skuteczniejsze reagowanie na incydenty cyberbezpieczeństwa.
- Wprowadzenie procedur oceny zgodności, dokumentacji technicznej oraz obowiązku oznakowania CE ma na celu ujednolicenie standardów i zwiększenie przejrzystości na rynku wewnętrznym UE.
- Obszerna lista wyłączeń dla sektorów takich jak wyroby medyczne, motoryzacja, lotnictwo i sprzęt morski jest istotna, ponieważ posiadają one własne ramy regulacyjne, które obejmują bezpieczeństwo, a w coraz większym stopniu również cyberbezpieczeństwo. Oznacza to, że CRA jest zaprojektowany jako horyzontalna regulacja uzupełniająca, która ma wypełniać luki regulacyjne tam, gdzie nie istnieją specyficzne wymagania cyberbezpieczeństwa lub są one niewystarczające. Sugeruje to warstwowe podejście do regulacji UE, w którym przepisy sektorowe mają pierwszeństwo, jeśli oferują równoważny lub wyższy poziom ochrony.
- Regulacja przewiduje wsparcie dla MŚP i start-upów poprzez uproszczone procedury, wytyczne oraz możliwość korzystania z piaskownic regulacyjnych, co ma na celu ograniczyć bariery wejścia i koszty wdrożenia obowiązków.

- Harmonogram wdrożenia przewiduje 36-miesięczny okres przejściowy, z wcześniejszym wejściem w życie wybranych obowiązków (np. w zakresie obsługi podatności), co wymaga od podmiotów odpowiedniego planowania, a także działań w określonej perspektywie czasowej, w tym poprzez dostosowania procesów i wdrożenie adekwatnych do regulacji procedur.