SECURE
Cyber Resilience for SMEs

CRA101: Zrozumienie obowiązków wynikających z CRA

31/03/2026

Funded by the European Union

Oświadczenie o finansowaniu UE: Projekt finansowany przez Unię Europejską w ramach umowy nr 101190325. Wyrażone poglądy i opinie są wyłącznie poglądami autora (autorów) i nie muszą odzwierciedlać poglądów Unii Europejskiej lub Europejskiego Centrum Kompetencji w zakresie Przemysłu, Technologii i Badań nad Cyberbezpieczeństwem. Ani Unia Europejska, ani organ przyznający dotację nie ponoszą za nie odpowiedzialności.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Zastrzeżenie ECCC: Projekt jest wspierany przez Europejskie Centrum Kompetencji w zakresie Cyberbezpieczeństwa i jego członków.

ZASTRZEŻENIE

Niniejszy dokument stanowi część rezultatu D4.1 „Wytyczne i materiały dotyczące zgodności MŚP z CRA" projektu SECURE. Został on po raz pierwszy opublikowany w październiku 2025 r. i zaktualizowany w marcu 2026 r.

Pierwszy autor: *Centre for Cybersecurity Belgium (CCB)*

Drugi autor: *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Spis treści

Spis tabel i rysunków

Skróty

CE – (z fr. Conformité Européenne) zgodność europejska

CRA – (z ang. Cyber Resilience Act) Rozporządzenie (UE) 2024/2847 (akt o cyberodporności)

CSIRT – (z ang. Computer Security Incident Response Team) Zespół Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym

CVD – (z ang. Coordinated Vulnerability Disclosure) skoordynowane ujawnianie luk w zabezpieczeniach

ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

EU DoC – (z ang. European Union Declaration of Conformity) Deklaracja zgodności Unii Europejskiej

MŚP – małe i średnie przedsiębiorstwa

NB – (z ang. Notified Body) jednostka notyfikowana

PDE – (z ang. Product with Digital Elements) produkt zawierający elementy cyfrowe

SBOM – (z ang. Software Bill of Materials) lista komponentów oprogramowania

SPOC – (z ang. Single Point of Contact) pojedynczy punkt kontaktowy

UE – Unia Europejska

Wprowadzenie

Unia Europejska (UE) przyjęła rozporządzenie **o cyberodporności** (CRA), rozporządzenie (UE) 2024/2847, w celu zwiększenia gotowości i odporności rynku cyfrowego UE w obliczu rosnących wyzwań związanych z cyberbezpieczeństwem. Poprzez wprowadzenie zharmonizowanych zasad i jasnych minimalnych wymagań w zakresie cyberbezpieczeństwa, CRA ma na celu zmniejszenie luk w zabezpieczeniach oraz ochronę zarówno konsumentów, jak i przedsiębiorstw. To przełomowe rozporządzenie weszło w życie w grudniu 2024 roku i przewiduje wdrażanie etapowe, umożliwiając okres przejściowy i adaptacyjny od 2024 do 2027 roku. CRA wymienia obowiązki producentów, importerów i dystrybutorów produktów zawierających elementy cyfrowe (PDE). **W art. 13 i załączniku I** do CRA wymieniono podstawowe wymogi w zakresie cyberbezpieczeństwa, których producenci muszą przestrzegać zarówno przy wprowadzaniu swoich PDE na rynek UE, jak i przez cały cykl życia PDE. Część I wymogów załącznika I koncentruje się na właściwościach PDE, a część II na postępowaniu w przypadku luk w zabezpieczeniach. Poza załącznikiem I do rozporządzenia CRA i art. 13 nakładane są także inne wymogi – na przykład dotyczące informacji i instrukcji dla użytkowników (załącznik II), obowiązków raportowania (art. 14–17) oraz zgodności (art. 27–32). W ramach wstępnych działań mających na celu przełożenie kluczowych obowiązków prawnych na konkretne wskazówki, **niniejsze wytyczne zawierają uproszczony przegląd[1] tych obowiązków**, podzielony na **pięć sekcji**, które należy uwzględnić **jako minimum**. Celem jest zwiększenie dostępności rozporządzenia oraz poprawa świadomości i zrozumienia na podstawowym poziomie, w szczególności wśród małych i średnich przedsiębiorstw (MŚP), zgodnie z celami **projektu SECURE**[2] . W celu uzyskania wskazówek technicznych i narzędzi dotyczących praktycznego wdrażania tych wymogów, na bieżąco udostępniane są dalsze materiały w **otwartym repozytorium SECURE**.

Harmonogram CRA:

- Wejście w życie: 10 grudnia 2024 r.
- Obowiązywanie wymogu raportowania: 11 września 2026 r.
- Pełne zastosowanie wymogów CRA: 11 grudnia 2027 r.

[1] Jest to niewyczerpująca lista, której celem jest uproszczenie obowiązków wynikających z rozporządzenia CRA, i która nie obejmuje wyjątków przewidzianych w tym rozporządzeniu. W celu przedstawienia ogólnego zarysu uwzględniono jedynie podstawowe obowiązki. Zostały one wybrane na podstawie dokładnej analizy tekstu rozporządzenia CRA.

[2] Projekt „Wzmocnienie cyberodporności MŚP w UE" (SECURE) oferuje wsparcie finansowe i wytyczne dla MŚP w zakresie zgodności z CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Zrozumienie obowiązków wynikających z CRA – CRA 101

1. Ocena ryzyka cyberbezpieczeństwa

W celu spełnienia obowiązku zapewnienia, że urządzenie PDE „zostało zaprojektowane, opracowane i wyprodukowane zgodnie z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa określonymi w części I załącznika I"[3] – tj. gwarantując „odpowiedni poziom cyberbezpieczeństwa w oparciu o ryzyko"[4] – *należy* przeprowadzić ocenę ryzyka w zakresie cyberbezpieczeństwa. Ocena ta musi zostać **udokumentowana**[5] i **regularnie aktualizowana** przez tzw. cały „okres wsparcia"[6] .

W praktyce ocena ryzyka powinna obejmować co najmniej[7]:

1) **Analizę ryzyka związanego z cyberbezpieczeństwem**, uwzględniającą:
   - Przeznaczenie i przewidywalne wykorzystanie PDE;
   - Warunki użytkowania (np. środowisko operacyjne, zasoby, które mają być chronione).

2) **Doprecyzowanie, wyjaśnienie i/lub uzasadnienie**
   - Zastosowania cyberbezpieczeństwa w fazie projektowania[8] – tj. w jaki sposób jest ono stosowane?
   - Zastosowania (lub braku zastosowania) wymagań zawartych w załączniku I, część I, do PDE – tj. czy i w jaki sposób mają zastosowanie wymagania bezpieczeństwa?
   - Zastosowania i wdrażanie wymogów dotyczących postępowania z lukami w zabezpieczeniach[9] – tj. w jaki sposób stosowane są wymogi dotyczące postępowania z lukami w zabezpieczeniach?

W przypadku gdy PDE zawiera komponenty pochodzące od stron trzecich, CRA oczekuje dołożenia **należytej staranności** w celu zapewnienia cyberbezpieczeństwa produktu końcowego. Może to oznaczać na przykład zgłoszenie zidentyfikowanej luki w zabezpieczeniach producentowi tego komponentu oraz podjęcie dalszych działań naprawczych. W tym celu należy prowadzić wykaz

[3] Art. 13 ust. 1 CRA.
[4] Załącznik I, część I pkt 1, CRA.
[5] Dokumentacja techniczna: wyjaśniono w pkt 5.
[6] Okres wsparcia: wyjaśniono w pkt 2.
[7] Art. 13 ust. 3 CRA.
[8] Załącznik I, część I pkt 1, CRA.
[9] Załącznik I, część II, CRA.

komponentów oprogramowania (SBOM)[10] oraz politykę skoordynowanego ujawniania luk w zabezpieczeniach (CVD) dla dostawców i udostępniać je organom nadzoru rynku na ich żądanie.

2. Postępowanie w przypadku luk w zabezpieczeniach i aktualizacje zabezpieczeń

Zgodnie z art. 13 ust. 8 producenci muszą zapewnić, aby luki w zabezpieczeniach PDE i jego komponentów były – „skutecznie obsługiwanie zgodnie z zasadniczymi wymaganiami określonymi w części II załącznika I"[11] przez cały okres wsparcia.

Oznacza to między innymi[12] :

1) **Identyfikowanie i dokumentowanie luk w zabezpieczeniach** – tj. sporządzanie wykazu komponentów oprogramowania (SBOM) (przynajmniej dla zależności najwyższego poziomu) i udostępnianie go organom nadzoru rynku na ich wniosek[13] ;
2) Niezwłoczne reagowanie na luki w zabezpieczeniach i ich usuwanie – tj. **dostarczanie aktualizacji zabezpieczeń** bez zbędnej zwłoki i bezpłatnie (wraz z komunikatami informacyjnymi dla użytkowników):
    - Każda aktualizacja zabezpieczeń wydana w okresie wsparcia musi pozostawać dostępna przez co najmniej 10 lat od daty wydania lub przez pozostałą część okresu wsparcia, w zależności od tego, który z tych okresów jest dłuższy[14] .
3) Regularne **przeglądy i testy** bezpieczeństwa produktu;
4) **Udostępnianie informacji** o naprawionych (i potencjalnych) lukach w zabezpieczeniach, ich skutkach i stopniu zagrożenia, instrukcji dla użytkowników dotyczących usuwania luk, adresów kontaktowych do zgłaszania luk, a także ustanowienie i egzekwowanie polityki CVD.

Wspomniany powyżej „**okres wsparcia**" „odzwierciedla czas, przez który produkt ma być używany"[15] i powinien proporcjonalnie uwzględniać oczekiwania użytkowników, charakter (cel) PDE oraz odpowiednie prawo unijne.

[10] Formalny zapis szczegółów i powiązań w łańcuchu dostaw komponentów zawartych w elementach oprogramowania PDE (art. 3 ust. 39 CRA).
[11] Art. 13 ust. 8, CRA.
[12] Załącznik I, część II, CRA.
[13] Udostępnienie go użytkownikom jest opcjonalne.
[14] Art. 13 ust. 9, CRA.
[15] Art. 13 ust. 8, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

W praktyce, przy określaniu okresu wsparcia powinien on wynosić:

- Co najmniej pięć lat (chyba, że okres użytkowania produktu jest krótszy niż pięć lat, wtedy okres wsparcia jest równy okresowi użytkowania produktu);
- wyraźnie określony (data zakończenia: miesiąc i rok) w momencie zakupu / na opakowaniu / w formie cyfrowej (po upływie tego okresu użytkownicy powinni zostać o tym poinformowani)[16].

Określenie i definicja okresu wsparcia powinny być zawarte w dokumentacji technicznej[17].

3. Informacje dla użytkowników, instrukcje i pojedynczy punkt kontaktowy

Zgodnie z art. 13 ust. 14–18 oraz załącznikiem II producenci *muszą* co najmniej **jasno poinformować użytkowników**, zamieszczając w formie papierowej/cyfrowej:

- dane producenta (nazwa, zarejestrowana nazwa handlowa lub znak towarowy, adres pocztowy, adres e-mail lub kontakt cyfrowy, strona internetowa);
- Dane dotyczące PDE (nazwa, typ, przeznaczenie, środowisko bezpieczeństwa i właściwości bezpieczeństwa, podstawowe funkcje, możliwe zagrożenia dla cyberbezpieczeństwa, zapewniane wsparcie techniczne w zakresie bezpieczeństwa, data zakończenia okresu wsparcia);
- Szczegółowe instrukcje lub link do nich (dotyczące środków zapewniających bezpieczne użytkowanie, możliwych skutków dla bezpieczeństwa danych wynikających ze zmian w produkcie, instalowania aktualizacji zabezpieczeń, bezpiecznego wycofania z eksploatacji i usuwania danych użytkownika, domyślnych ustawień instalacji aktualizacji zabezpieczeń);
- Należy wyznaczyć jeden punkt kontaktowy (SPOC), aby umożliwić użytkownikom:
    - Nawiązanie bezpośredniego i szybkiego kontaktu z producentem za pomocą preferowanych przez niego środków komunikacji (nie tylko za pomocą narzędzi automatycznych);
    - Zgłaszanie luk w zabezpieczeniach;
    - Znalezienie polityki CVD.
- Linki (jeśli dotyczy) do polityki CVD, unijnej deklaracji zgodności (EU DoC)[18] oraz SBOM (jeśli jest udostępniony użytkownikom).

[16] Art. 13 ust. 19, CRA.

[17] Dokumentacja techniczna: wyjaśniono w pkt 5.

[18] EU DoC: wyjaśnione w pkt 5.

Instrukcje dla użytkownika powinny być napisane prostym językiem i dostępne w formie elektronicznej lub papierowej, przez co najmniej dziesięć lat lub przez okres wsparcia (w zależności od tego, który z tych okresów jest dłuższy).

4. Obowiązki w zakresie zgłaszania incydentów i luk w zabezpieczeniach

Poniższa tabela zawiera przegląd obowiązków użytkownika w odniesieniu do zgłaszania[19]. Poniżej znajdują się dalsze wyjaśnienia.

Tabela 1:
Zgłaszanie incydentów i luk w zabezpieczeniach

Zgłaszanie	Luki w zabezpieczeniach	Incydenty
CO zgłaszać	*Konieczne:* „aktywnie wykorzystywane luki w zabezpieczeniach" *Możliwe:* luki w zabezpieczeniach (nieeksploatowane aktywnie); cyberzagrożenia	*Konieczne*: „poważne incydenty" *Możliwe*: incydenty (inne niż poważne); sytuacje potencjalnie niebezpieczne
DO KOGO zgłaszać	CSIRT[20] Jednolita platforma zgłaszania (ENISA) Użytkownicy, których to dotyczy	
W JAKI SPOSÓB zgłaszać	1) Powiadomienie wczesnego ostrzegania (24 godz.) 2) Powiadomienie o luce w zabezpieczeniach (72 godz.) 3) Raport końcowy (14 dni)	1) Powiadomienie wczesnego ostrzegania (24 godz.) 2) Powiadomienie o incydencie (72 godz.) 3) Raport końcowy (1 miesiąc)

[19] Art. 14–17, CRA.

[20] Art. 3 ust. 51 CRA: „CSIRT wyznaczony jako koordynator" oznacza CSIRT wyznaczony jako koordynator zgodnie z art. 12 ust. 1 dyrektywy (UE) 2022/2555.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4.1. Co zgłaszać

Zgodnie z definicjami określonymi w art. 3 CRA,

- „aktywnie wykorzystywana luka" wymaga wiarygodnych dowodów na to, że została wykorzystana przez złośliwy podmiot w systemie bez zgody właściciela[21] ;
- Incydent uznaje się za „poważny", gdy[22]:
    - ma negatywny wpływ lub może mieć wpływ na zdolność PDE do ochrony dostępności, autentyczności, integralności lub poufności danych lub funkcji; lub
    - doprowadził lub może doprowadzić do wprowadzenia/wykonania złośliwego kodu w produkcie lub w sieciach i systemach informatycznych użytkownika.

4.2. Do kogo zgłaszać

Zgłoszenie należy kierować do Zespołu Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym (CSIRT) państwa członkowskiego, w którym producent[23] :

- ma swoją główną siedzibę; lub, jeśli nie można tego ustalić,
- posiada zakład zatrudniający największą liczbę pracowników.

W przypadku podmiotów spoza UE można zastosować łańcuch zastępczy, który uwzględnia siedzibę upoważnionego przedstawiciela producenta → importera → dystrybutora → miejsce, w którym znajduje się największa liczba urządzeń końcowych lub użytkowników.

Pomijając kilka wyjątków, wszystkie zgłoszenia będą przechodziły przez jednolitą platformę zgłoszeniową, która ma zostać utworzona i utrzymywana przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), a następnie będą przekazywane do innych zespołów CSIRT oraz organów nadzoru rynku za pośrednictwem elektronicznego punktu końcowego do zgłoszeń.

Użytkownicy, których to dotyczy (a w stosownych przypadkach wszyscy użytkownicy), muszą również zostać powiadomieni o lukach w zabezpieczeniach / incydentach oraz działaniach

[21] Art. 3 ust. 42, CRA.

[22] Art. 3 ust. 44 CRA; art. 14 ust. 5 CRA.

[23] CSIRT to zazwyczaj krajowy CERT: Zespół Reagowania na Incydenty Komputerowe.

użytkowników, najlepiej w formacie nadającym się do odczytu maszynowego. CSIRT mogą poinformować użytkowników, jeśli producent tego nie zrobi[24].

4.3. W jaki sposób zgłaszać

Istnieje kilka różnic w zgłaszaniu incydentów i luk w zabezpieczeniach.

Luki w zabezpieczeniach

1) **Powiadomienie wczesnego ostrzegania**: powinno zostać przesłane najpóźniej w ciągu 24 godzin od stwierdzenia luki i powinno wskazywać, w stosownych przypadkach, państwa członkowskie, w których dostępny jest PDE.
2) **Powiadomienie o luce w zabezpieczeniach**: powinno zostać przesłane najpóźniej w ciągu 72 godzin od wykrycia i powinno zawierać:
    - Ogólne informacje o PDE;
    - Ogólny charakter luki w zabezpieczeniach;
    - Środki naprawcze lub ograniczające ryzyko, które zostały podjęte lub mogą zostać podjęte przez użytkowników;
    - Wrażliwość zgłoszonych informacji.
3) **Raport końcowy**: należy go przedłożyć nie później niż **14 dni** po podjęciu środków naprawczych/ograniczających i powinien on zawierać:
    - Opis – stopień zagrożenia i skutki;
    - Informacje na temat złośliwego podmiotu, jeśli dotyczy;
    - Szczegóły dotyczące aktualizacji zabezpieczeń lub innych dostępnych środków naprawczych.

Incydenty

1) **Powiadomienie wczesnego ostrzegania**: powinno zostać złożone najpóźniej w ciągu 24 godzin od uzyskania wiedzy o zdarzeniu i powinno wskazywać:
    - W stosownych przypadkach, państwa członkowskie, w których dostępny jest PDE;
    - Czy istnieje podejrzenie, że incydent został spowodowany działaniami niezgodnymi z prawem lub złośliwymi.

[24] Art. 14 ust. 8 CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2) **Powiadomienie o incydencie**: powinno zostać złożone najpóźniej w ciągu 72 godzin od stwierdzenia incydentu i powinno zawierać:
    - Ogólne informacje o charakterze zdarzenia;
    - Wstępną ocenę incydentu;
    - Środki naprawcze lub łagodzące, które zostały podjęte lub mogą zostać podjęte przez użytkowników;
    - Wrażliwość zgłoszonych informacji.
3) **Raport końcowy**: należy złożyć w ciągu miesiąca od zgłoszenia incydentu i powinien zawierać:
    - Opis – stopień zagrożenia i skutki;
    - Rodzaj zagrożenia lub przyczynę źródłową, która prawdopodobnie spowodowała incydent;
    - Zastosowane i trwające środki łagodzące.

5. Ocena zgodności

Przed wprowadzeniem PDE do obrotu producent musi wykazać, że spełnia on zasadnicze wymogi w zakresie cyberbezpieczeństwa określone w załączniku I do CRA. Odbywa się to w ramach **procedury oceny zgodności** mającej zastosowanie do danej kategorii produktów.

5.1. Procedury oceny zgodności

CRA przewiduje między innymi:

- Kontrolę wewnętrzną (moduł A);
- Badanie typu UE, a następnie zgodność z typem (moduły B + C);
- Pełne zapewnienie jakości (moduł H);
- Ocenę w ramach Europejskiego Systemu Certyfikacji Cyberbezpieczeństwa, w stosownych przypadkach.

Zharmonizowane normy i wspólne specyfikacje nie są procedurami zgodności. Mogą one jednak stanowić wsparcie przy wykazywaniu zgodności.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5.2. Domniemanie zgodności

Produkt zgodny z

- normami zharmonizowanymi, których odniesienia zostały opublikowane w Dzienniku Urzędowym, lub
- wspólnymi specyfikacjami przyjętymi przez Komisję Europejską

uznaje się **za zgodny**[25] z zasadniczymi wymaganiami objętymi tymi normami lub specyfikacjami.

W przypadku gdy takie normy lub specyfikacje nie są (w pełni) stosowane, producent musi bezpośrednio wykazać zgodność z wymaganiami załącznika I poprzez odpowiednią procedurę oceny zgodności. W stosownych przypadkach do wykazania zgodności można również wykorzystać europejski certyfikat cyberbezpieczeństwa, w granicach przewidzianych przez CRA.

5.3. Kategorie produktów

Procedura oceny zgodności, którą należy zastosować, zależy od klasyfikacji PDE zgodnie z rozporządzeniem CRA, określonej w załącznikach III i IV do rozporządzenia CRA[26] . Rozporządzenie CRA rozróżnia produkty domyślne, ważne (klasy I i II) oraz krytyczne.

W zależności od kategorii:

- kontrola wewnętrzna może być wystarczająca;
- może być wymagane zaangażowanie jednostki notyfikowanej (NB); lub
- ocena w ramach europejskiego systemu certyfikacji może być obowiązkowa lub dozwolona.

Prawidłowa klasyfikacja ma zatem decydujące znaczenie dla określenia procedury, która ma zastosowanie.

Przegląd procedur, które mogą być stosowane w poszczególnych klasach produktów, znajduje się w tabeli 2 poniżej.

[25] Art. 27, CRA.

[26] Art. 32, CRA; załącznik VIII, CRA.

Tabela 2:
Procedury oceny zgodności

	Kontrola wewnętrzna (moduł A)	Badanie **typu UE, a następnie ocena zgodności z typem (moduły B + C)**	Pełne zapewnienie jakości (moduł H)	Europejski system certyfikacji cyberbezpieczeń--stwa	Normy zharmonizowane/ Wspólne specyfikacje[27]
Produkty domyślne	**X**	**X**	**X**	**X**	**X** Może zapewnić zgodność z wymaganiami, które obejmuje
Produkty ważne klasy I	**X**[28]	**X**	**X**	**X** poziom: znaczny[29]	**X** Może zapewnić zgodność z wymaganiami, które obejmuje
Ważne produkty klasy II		**X**	**X**	**X** poziom: znaczny[30]	**X** Może zapewnić zgodność z wymaganiami, które obejmuje
Produkty krytyczne				**X** poziom: znaczny	**X** Może zapewnić wsparcie w zakresie zgodności z wymaganiami, które obejmuje

[27] Normy zharmonizowane i wspólne specyfikacje nie są procedurami, ale mogą stanowić wsparcie przy wykazywaniu zgodności.

[28] Kontrola wewnętrzna (moduł A) może być stosowana wyłącznie w przypadku stosowania norm zharmonizowanych, wspólnych specyfikacji lub, w stosownych przypadkach, odpowiedniego systemu certyfikacji. W przeciwnym razie obowiązują następujące ścieżki: badanie typu UE, a następnie zgodność z typem (moduły B + C) lub pełne zapewnienie jakości (moduł H).

[29] Jeżeli na mocy art. 8 ust. 1 rozporządzenia w sprawie oceny zgodności zostanie przyjęty akt delegowany, można zastosować unijny system certyfikacji cyberbezpieczeństwa. W przeciwnym razie należy zastosować przepisy dotyczące produktów ważnych klasy II.

[30] Zastosowanie ma przypis 29.

5.4. Deklaracja zgodności UE (EU DoC)

Po pomyślnym przeprowadzeniu oceny zgodności producent sporządza **unijną deklarację zgodności** (EU DoC)[31] .

Owa deklaracja potwierdza, że PDE spełnia obowiązujące zasadnicze wymagania i zawiera wymagane elementy przewidziane w CRA. Wzór struktury znajduje się w załączniku V do CRA. Uproszczoną deklarację zgodności UE (EU DoC) można znaleźć w załączniku VI. Musi ona być udostępniona w językach wymaganych przez państwo członkowskie, w którym PDE jest wprowadzane do obrotu, i musi pozostawać dostępna przez okres przewidziany przepisami prawa.

5.5. Oznakowanie CE

Aby umożliwić konsumentom rozpoznanie urządzeń PDE spełniających wymogi rozporządzenia CRA oraz podejmowanie świadomych decyzji przy zakupie i użytkowaniu takich urządzeń, **oznakowanie CE**[32] musi być „umieszczone w widocznym, czytelnym i trwałym miejscu"[33] przed wprowadzeniem urządzenia PDE do obrotu. Należy to zrobić bezpośrednio na samym produkcie. W przypadku, gdy nie jest to możliwe ze względu na charakter produktu, znak ten należy umieścić na opakowaniu oraz dołączyć do towarzyszącej mu unijnej deklaracji zgodności[34] [35]. Oznaczenie CE wskazuje, że produkt jest zgodny ze wszystkimi obowiązującymi przepisami unijnymi wymagającymi oznaczenia CE, w tym z aktem o cyberodporności (CRA).

5.6. Wykazanie zgodności za pomocą dokumentacji technicznej

Kluczowym elementem oceny zgodności jest **dokumentacja techniczna.** Zgodnie z art. 31 CRA i załącznikiem VII dokumentacja techniczna ma znaczenie dla wszystkich omówionych wcześniej punktów, ponieważ musi zostać sporządzona przed wprowadzeniem PDE do obrotu i stale aktualizowana przez cały okres wsparcia[36]. Dokumentacja techniczna, obejmująca większość obowiązków wynikających z CRA, powinna zatem zawierać[37]:

- Ogólny opis PDE (przeznaczenie, wersje oprogramowania mające wpływ na zgodność, dowody dotyczące cech zewnętrznych, oznakowanie i układ wewnętrzny produktów sprzętowych, informacje dla użytkownika i instrukcje);

[31] Art. 28 CRA; załączniki V–VI do CRA.

[32] Oznaczenie Conformité Européenne (zgodność europejska).

[33] Art. 30 ust. 1, CRA.

[34] Art. 29–30 ustawy o ocenie zgodności (CRA).

[35] W przypadku udziału jednostki notyfikowanej w ocenie zgodności mają zastosowanie dodatkowe przepisy.

[36] Art. 31 ust. 2, CRA.

[37] Załącznik VII do CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Opis projektowania, rozwoju i produkcji PDE oraz procesów postępowania z lukami w zabezpieczeniach (np. opis architektury systemu, SBOM, polityka CVD, procesy monitorowania itp.);
- Ocenę ryzyka cyberbezpieczeństwa;
- Określenie i definicję okresu wsparcia;
- Zastosowane normy zharmonizowane (lub ich części);
- Raporty z badań zgodności i raporty dotyczące postępowania w przypadku luk w zabezpieczeniach;
- Kopię unijnego dokumentu zgodności (EU DoC).

Komisja Europejska opracuje **uproszczony** formularz **dokumentacji technicznej** dla mikroprzedsiębiorstw i małych przedsiębiorstw[38]. Ponadto art. 33 stanowi, że zarówno państwa członkowskie, jak i Komisja Europejska mają zapewnić **wsparcie dla MŚP** – między innymi w formie wytycznych[39] oraz możliwości wsparcia finansowego.

Projekt SECURE oferuje wsparcie finansowe dla MŚP zobowiązanych do przestrzegania CRA oraz na bieżąco udostępnia wytyczne i materiały mające na celu pomoc MŚP we wdrażaniu CRA, takie jak niniejsze wytyczne CRA101.

[38] Art. 33 ust. 5, CRA.

[39] Art. 26, CRA.

Wnioski

Aby zapewnić **przystępny przegląd kluczowych obowiązków określonych w CRA**, niniejsze wytyczne skupiają się na **pięciu elementach** CRA, które należy uwzględnić jako minimum: (1) ocena ryzyka cyberbezpieczeństwa; (2) postępowanie w przypadku luk w zabezpieczeniach i aktualizacje zabezpieczeń; (3) informacje dla użytkowników, instrukcje i pojedynczy punkt kontaktowy; (4) obowiązek zgłaszania incydentów i luk w zabezpieczeniach; (5) ocena zgodności. Wyjaśnia takie elementy, jak okres wsparcia, unijna deklaracja zgodności i oznakowanie CE oraz dokumentacja techniczna. Mając na celu **wsparcie MŚP w poruszaniu się po złożonych ramach prawnych**, niniejszy przewodnik zawiera podsumowanie kluczowych obowiązków prawnych, które należy zrozumieć przed ich wdrożeniem. W celu uzyskania praktycznych wskazówek dotyczących dalszego podejścia do tych przepisów prawnych i ich wdrażania, a także dotyczące poszczególnych elementów CRA (np. SBOM, zarządzanie lukami w zabezpieczeniach itp.), w miarę postępów we wdrażaniu CRA w **centralnym repozytorium SECURE** będą na bieżąco udostępniane dodatkowe wytyczne techniczne i narzędzia. Jako kolejne kroki dla MŚP zaleca się zapoznanie się z innymi wytycznymi w repozytorium SECURE, takimi jak **„Essential Cybersecurity Requirements: Annex I, Part I"** , zawierającymi praktyczne sugestie i zalecenia dotyczące każdego z przepisów załącznika I, a także **„CRA Methodological Compliance Assessment Framework"**, zawierającym zestaw narzędzi i listę kontrolną krok po kroku dotyczącą zgodności z CRA wykraczającą poza załącznik I.