Cyber Resilience Act

Miesiąc Prawa EY Law

The better the question.
The better the answer.
The better the world works.

EY
Shape the future with confidence

CRA w skrócie

CRA to unijne rozporządzenie, które określa wymagania bezpieczeństwa dla produktów z elementami cyfrowymi oferowanych na rynku UE. Jego celem jest ograniczenie luk bezpieczeństwa oraz zapewnienie, aby producenci dbali o bezpieczeństwo produktu od projektowania aż do zakończenia wsparcia.

CRA dotyczy podmiotów, które wprowadzają lub udostępniają na rynku UE produkty z elementami cyfrowymi – przede wszystkim ich producentów, importerów i dystrybutorów. Przewiduje także szczególne zasady dla organizacji stale i systematycznie wspierających rozwój komercyjnego otwartego oprogramowania.

Zakres obowiązków zależy od roli organizacji wobec danego produktu, a importer lub dystrybutor może zostać uznany za producenta, jeżeli oferuje produkt pod własną nazwą lub marką albo dokonuje w nim istotnej zmiany.

1 Jakie produkty obejmuje CRA?

W uproszczeniu CRA obejmuje sprzęt i oprogramowanie, które łączą się bezpośrednio lub pośrednio z urządzeniem albo siecią. Może obejmować także niezbędne do działania produktu funkcje zdalne, np. funkcję chmurową przygotowaną przez producenta. Przykłady to systemy operacyjne, aplikacje, routery, inteligentne zamki i inne urządzenia podłączone do sieci.

1

Bezpieczeństwo od początku

Cyberbezpieczeństwo ma być uwzględniane już przy projektowaniu produktu i przez cały czas jego używania.

2

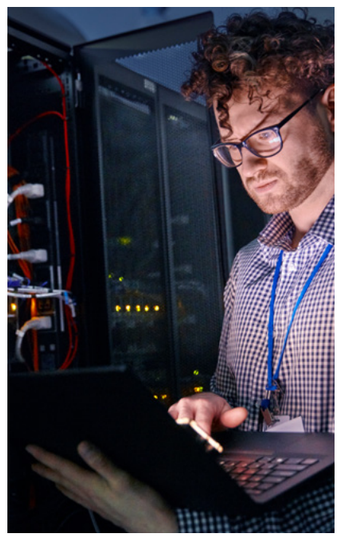
Aktualizacje bezpieczeństwa

Producent ma usuwać wykryte luki i udostępniać poprawki przez okres wsparcia produktu.

3

Obowiązki w całym łańcuchu dostaw

Wymagania dotyczą producentów, importerów i dystrybutorów. CRA przewiduje też szczególne zasady dla organizacji stale wspierających rozwój komercyjnego otwartego oprogramowania.



2 Najważniejsze daty

11 grudnia 2027 r.

Zaczyna być stosowana większość przepisów CRA

11 września 2026 r.

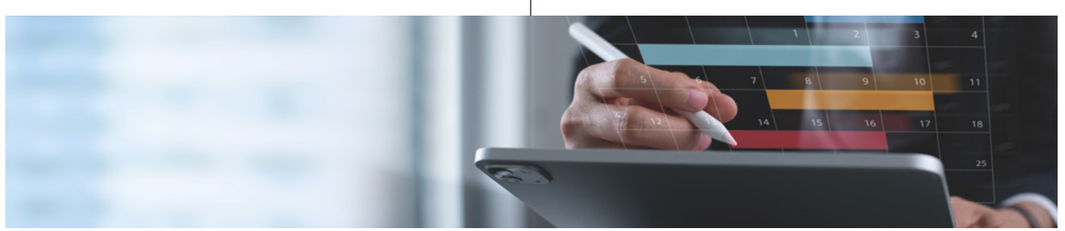
Producenci zaczynają zgłaszać luki bezpieczeństwa faktycznie wykorzystywane przez atakujących oraz poważne incydenty

11 czerwca 2026 r.

Zaczynają obowiązywać przepisy dotyczące wyznaczania podmiotów uprawnionych do niezależnej oceny zgodności (na dzień dzisiejszy brak takich notyfikacji)

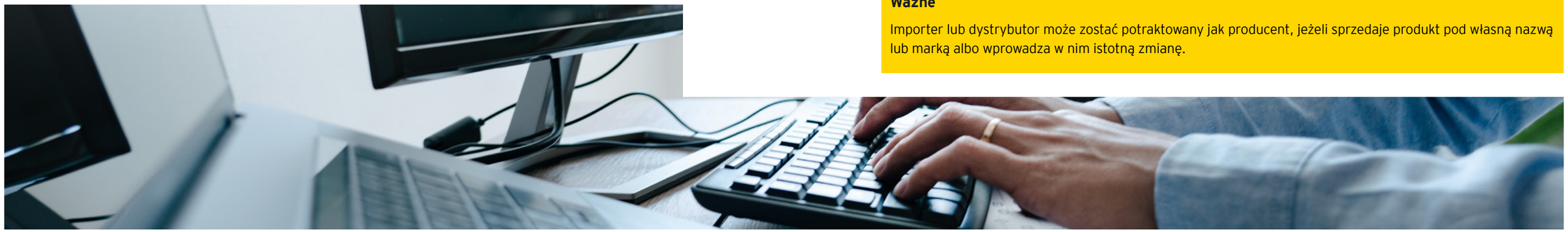
10 grudnia 2024 r.

CRA wszedł w życie



3 CRA: najważniejsze pytania

Czy każdy produkt podlega takim samym zasadom?	Nie. Sposób sprawdzenia zgodności zależy od kategorii produktu. Produkty z kategorii ważne/krytyczne o większym znaczeniu dla cyberbezpieczeństwa podlegają bardziej rygorystycznym wymogom niż standardowe produkty cyfrowe.
Jak długo producent ma usuwać luki bezpieczeństwa?	Co do zasady przez co najmniej pięć lat. Jeżeli produkt ma być używany krócej, okres ten powinien być odpowiednio krótszy. Jeżeli można oczekiwać dłuższego używania produktu, wsparcie powinno trwać odpowiednio dłużej.
Co z produktami wprowadzonymi na rynek przed 11 grudnia 2027 r.?	Pełne wymagania CRA obejmą taki produkt, jeżeli po tej dacie zostanie zmieniony w sposób wpływający na jego bezpieczeństwo albo przeznaczenie. Obowiązki zgłaszania luk faktycznie wykorzystywanych przez atakujących i poważnych incydentów obejmą jednak także produkty wprowadzone wcześniej.
Czy wszystkie produkty podlegają CRA?	Nie. Wyłączenia dotyczą m.in. określonych wyrobów medycznych, niektórych produktów motoryzacyjnych i lotniczych, wyposażenia morskiego oraz produktów przeznaczonych wyłącznie do bezpieczeństwa narodowego lub obronności.



4 Twoje najważniejsze obowiązki

Jeśli jesteś producentem	**Jeśli jesteś importerem**	**Jeśli jesteś dystrybutorem**
Uwzględniaj bezpieczeństwo już przy projektowaniu produktu.	Wprowadzaj na rynek produkty zgodne z CRA.	Przed udostępnieniem produktu sprawdź, czy spełniono podstawowe wymagania CRA.
Sprawdź zagrożenia, przygotuj wymagane dokumenty i potwierdź zgodność produktu z CRA.	Sprawdź, czy producent potwierdził zgodność produktu i przygotował wymagane dokumenty.	Sprawdź oznakowanie CE oraz wymagane dokumenty i informacje.
Usuwaj wykryte luki i bezpłatnie dostarczaj aktualizacje bezpieczeństwa w okresie wsparcia.	Zweryfikuj oznakowanie CE, deklarację zgodności oraz informacje dla użytkownika.	Nie udostępniaj produktu, jeśli nie jest zgodny z CRA.
Zgłaszaj luki faktycznie wykorzystywane przez atakujących oraz poważne incydenty.	Nie wprowadzaj produktu, jeśli nie jest zgodny lub stwarza istotne ryzyko.	Po otrzymaniu informacji o luce niezwłocznie poinformuj producenta.
Przygotuj deklarację zgodności UE i oznakowanie CE.	Informuj producenta o wykrytych lukach i współpracuj z organami nadzoru.	Współpracuj z organami nadzoru i wspieraj działania naprawcze.

Ważne

Importer lub dystrybutor może zostać potraktowany jak producent, jeżeli sprzedaje produkt pod własną nazwą lub marką albo wprowadza w nim istotną zmianę.

5 Jak przygotować organizację do CRA?

Co warto zrobić już teraz?

Sprawdź, które produkty w Twojej ofercie podlegają CRA, ustal rolę organizacji i zaplanuj dostosowanie projektowania, dokumentacji, usuwania luk, aktualizacji oraz potwierdzania zgodności.

Zakres

Czy oferowany produkt jest sprzętem, oprogramowaniem albo korzysta z niezbędnej funkcji zdalnej?

Kategoria

Do jakiej kategorii należy produkt i czy wymaga niezależnej oceny zgodności?

Cykl życia

Czy procesy obejmują bezpieczne projektowanie, testy, aktualizacje oraz usuwanie luk bezpieczeństwa?

Terminy

Czy organizacja jest gotowa na obowiązki od 11 czerwca 2026 r., 11 września 2026 r. i 11 grudnia 2027 r.?

Źródła
Rozporządzenie (UE) 2024/2847, Akt o cyberodporności
PARP, „Akt o Cyberodporności – cele i zakres regulacji"

Zapraszamy do kontaktu!

Joanna Ostrowska

Partner | Leader of Digital, Cyber & Data Team, EY Law

joanna.ostrowska@pl.ey.com

Gabriela Sacha

Manager | Digital, Cyber & Data Team, EY Law

gabriela.sacha@pl.ey.com

Agata Wilska

Project Manager | Digital, Cyber & Data Team, EY Law

agata.wilska@pl.ey.com

EY | Building a better working world

Celem działalności EY jest budowanie lepiej funkcjonującego świata poprzez wspieranie klientów, pracowników, społeczeństwa i planety w tworzeniu trwałych wartości oraz budowanie zaufania na rynkach kapitałowych.

Korzystając z danych, sztucznej inteligencji oraz zaawansowanych technologii, zespoły EY pomagają klientom odważnie kształtować przyszłość i znajdować odpowiedzi na obecne i przyszłe wyzwania.

EY świadczy kompleksowe usługi w zakresie audytu, doradztwa, podatków, strategii i transakcji. Dzięki wiedzy sektorowej, globalnie połączonym, multidyscyplinarnym zespołom i różnorodnym partnerstwom EY może świadczyć usługi w ponad 150 krajach.

EY w Polsce to prawie 4000 specjalistów pracujących w 8 miastach: Warszawie, Gdańsku, Katowicach, Krakowie, Łodzi, Poznaniu, Wrocławiu i Rzeszowie. Działając na polskim rynku, co roku EY doradza tysiącom firm, zarówno małym i średnim przedsiębiorstwom, jak i największym korporacjom. Tworzy unikatowe analizy, dzieli się wiedzą, integruje środowisko przedsiębiorców oraz angażuje się społecznie.

Wszystko po to, aby z odwagą kształtować przyszłość.

ey.com/pl

Designed by EY Creative Services Warsaw, Poland.