

DORA

Miesiąc Prawa EY Law



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

The EY logo, consisting of the letters 'EY' in a bold, white, sans-serif font, with a yellow diagonal line above the 'Y'.

Shape the future
with confidence



DORA w skrócie

DORA to unijne rozporządzenie, które pomaga instytucjom finansowym wzmocnić operacyjną odporność cyfrową.

Wymaga, aby skutecznie zarządzały ryzykiem ICT, utrzymywały ciągłość usług w razie cyberataku, awarii lub innego zakłócenia technologicznego oraz właściwie zarządzały ryzykiem związanym z dostawcami usług ICT.

Odpowiedzialność za zgodność z DORA pozostaje przy tym po stronie instytucji finansowej. Rozporządzenie stosuje się od 17 stycznia 2025 r.

1

Najważniejsze daty związane z DORA



Co oznacza „operacyjna odporność cyfrowa”?

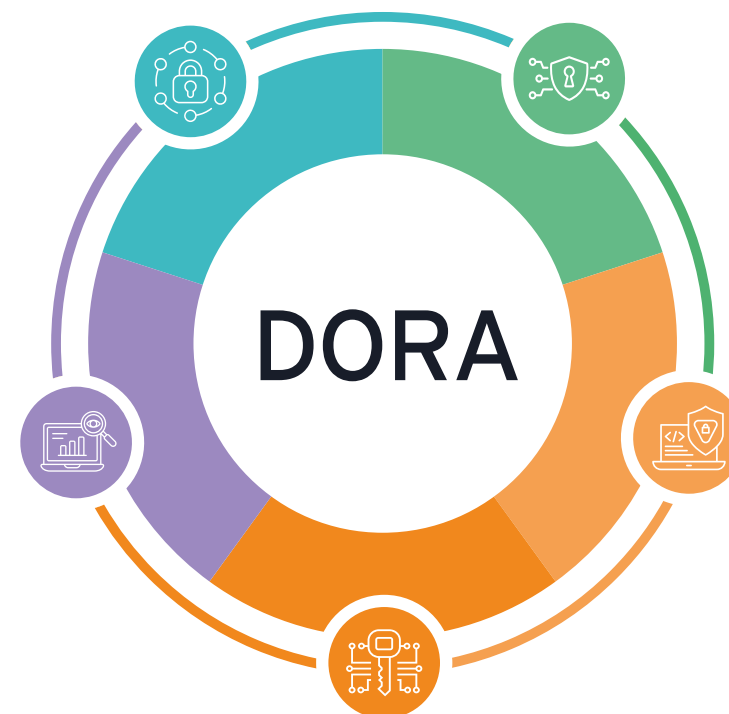
To zdolność organizacji do utrzymania bezpiecznego i niezawodnego działania systemów oraz ciągłości usług finansowych, także podczas zakłóceń. Obejmuje zapobieganie, wykrywanie problemów, reagowanie oraz utrzymywanie i przywracanie ciągłości działania.

Kogo obejmuje DORA?

DORA obejmuje szeroką grupę podmiotów finansowych, m.in. banki, instytucje płatnicze, firmy inwestycyjne, zakłady ubezpieczeń. Wpływa również na współpracę tych podmiotów z zewnętrznymi dostawcami ICT, np. dostawcami usług chmurowych, oprogramowania i przetwarzania danych.

2

Pięć najważniejszych obszarów DORA



Zarządzanie ryzykiem ICT

Organizacja ma wiedzieć, od jakich systemów zależy, jakie zagrożenia mogą wystąpić i jak ograniczać ich skutki.

Incydenty ICT

Poważne zdarzenia technologiczne trzeba odpowiednio klasyfikować, obsługiwać i zgłaszać właściwym organom.

Testowanie odporności

Systemy, procedury i plany awaryjne należy regularnie sprawdzać, aby wykrywać słabości przed wystąpieniem kryzysu.

Dostawcy usług ICT

Korzystanie z zewnętrznej technologii nie przenosi odpowiedzialności z podmiotu finansowego; potrzebne są odpowiednie umowy, ocena ryzyka i monitorowanie dostawców.

Wymiana informacji

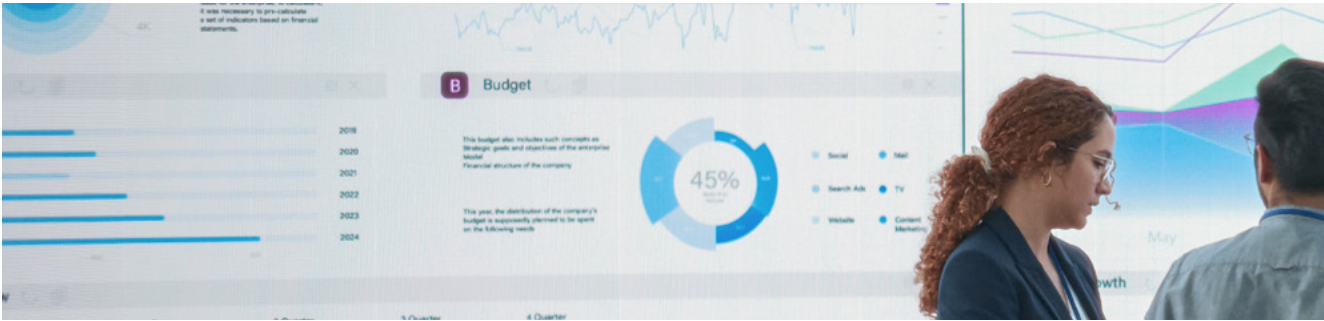
Podmioty finansowe mogą wymieniać informacje o cyberzagrożeniach w zaufanych grupach, z poszanowaniem poufności, ochrony danych i prawa konkurencji.



3

Najważniejsze pytania

Czy DORA dotyczy wyłącznie działów IT?	Nie. Odpowiedzialność obejmuje całą organizację, a organ zarządzający zatwierdza i nadzoruje zasady zarządzania ryzykiem ICT. DORA łączy technologię, ciągłość działania, zarządzanie incydentami, umowy z dostawcami oraz szkolenia pracowników.
Czy każdy podmiot finansowy ma identyczne obowiązki?	Nie. DORA opiera się na zasadzie proporcjonalności. Zakres działań uwzględnia wielkość i profil ryzyka organizacji oraz charakter, skalę i złożoność jej usług. Dla części mniejszych podmiotów przewidziano uproszczone ramy zarządzania ryzykiem ICT.
Czy skorzystanie z dostawcy chmurowego przenosi odpowiedzialność na dostawcę?	Nie. Podmiot finansowy pozostaje odpowiedzialny za zgodność z DORA także wtedy, gdy korzysta z zewnętrznych usług ICT. Musi oceniać ryzyko, prowadzić rejestr umów, monitorować dostawców i mieć plan bezpiecznego zakończenia współpracy.
Czy każdy incydent trzeba zgłaszać organowi?	Nie. Wszystkie incydenty ICT trzeba rejestrować i obsługiwać, natomiast obowiązkowemu zgłoszeniu podlegają poważne incydenty spełniające właściwe kryteria.
Czy wszystkie podmioty muszą wykonywać zaawansowane testy TLPT?	Nie. Zaawansowane testy imitujące działania realnych atakujących dotyczą podmiotów wskazanych przez właściwe organy na podstawie kryteriów określonych w DORA. Pozostałe podmioty testują odporność proporcjonalnie do swojego ryzyka.



4

Najważniejsze obowiązki i wymagania praktyczne

Jeśli jesteś podmiotem finansowym	Jeśli świadczysz usługi ICT dla podmiotów finansowych
Ustal odpowiedzialność za ryzyko ICT i zaangażuj organ zarządzający.	Ustal, które wymagania wynikają bezpośrednio z DORA, a które z umów z klientami finansowymi.
Zidentyfikuj najważniejsze systemy, procesy, dane i zależności od dostawców.	Zapewnij klientowi informacje i współpracę potrzebne do oceny bezpieczeństwa oraz ciągłości usługi.
Chroń systemy, wykrywaj nieprawidłowości oraz przygotuj plany reagowania, kopii zapasowych i przywracania działania.	Wspieraj obsługę incydentów dotyczących świadczonych usług i realizuj uzgodnione obowiązki informacyjne.
Rejestruj incydenty, klasyfikuj je i zgłaszaj poważne zdarzenia właściwemu organowi.	Bądź gotowy do udziału w audytach, kontrolach i testach, jeżeli przewiduje to DORA lub umowa.
Regularnie testuj systemy, procedury i plany awaryjne oraz usuwaj wykryte słabości.	Zapewnij uzgodnione poziomy usług, ochronę danych, plany awaryjne i możliwość bezpiecznego odzyskania lub przeniesienia danych.
Prowadź rejestr umów z dostawcami ICT, oceniaj ryzyko i zapewnij wymagane postanowienia umowne oraz strategie wyjścia.	Pamiętaj, że bezpośrednie unijne ramy nadzoru dotyczą dostawców wyznaczonych jako kluczowi; pozostali dostawcy są przede wszystkim objęci wymaganiami umownymi i monitorowaniem przez klientów finansowych.

Ważne

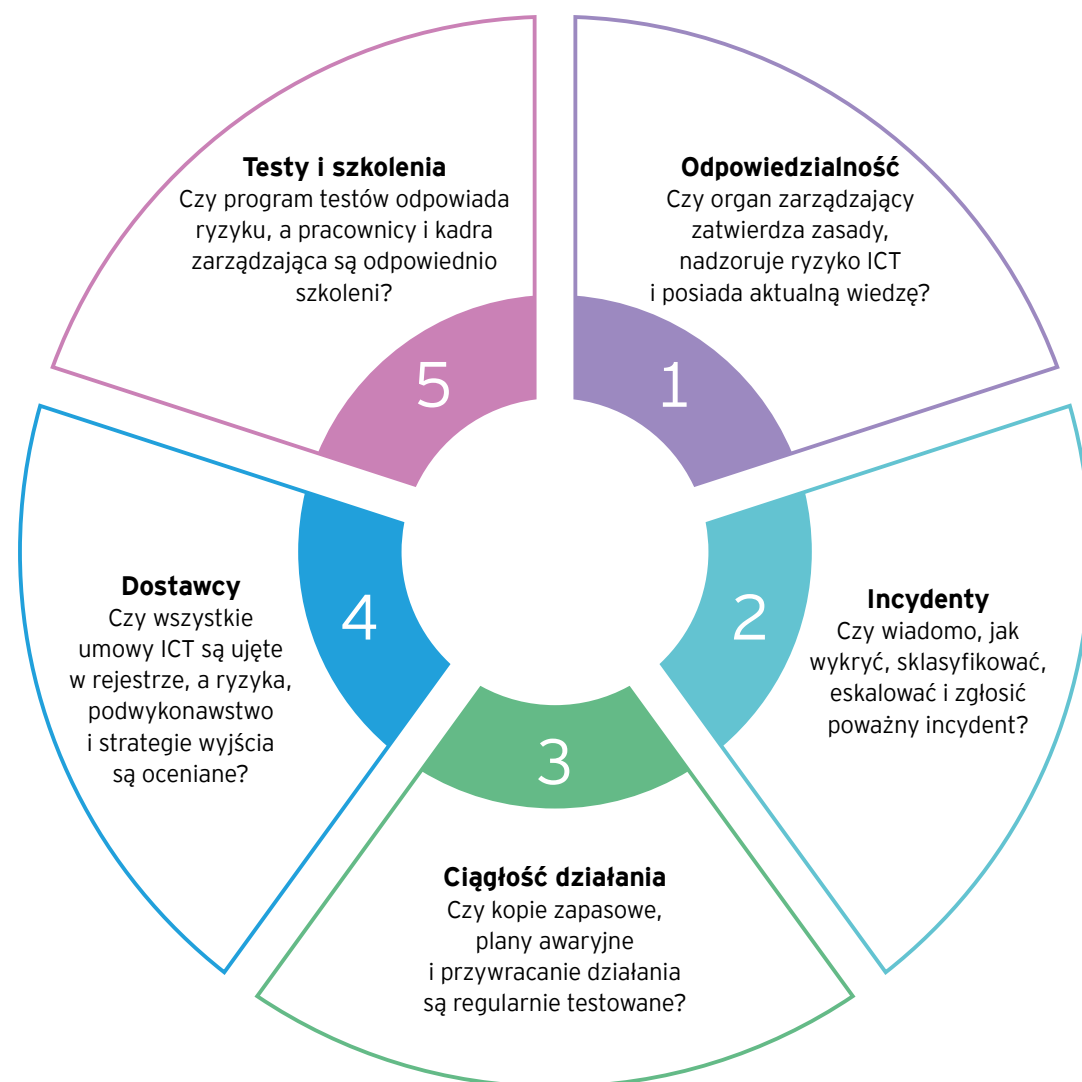
Podmiot finansowy nie może przenieść swojej odpowiedzialności na dostawcę ICT. Umowa i outsourcing pomagają zarządzać usługą, ale odpowiedzialność za spełnienie obowiązków DORA pozostaje po stronie podmiotu finansowego.

5

Jak przygotować organizację do DORA?

Co warto sprawdzić?

Czy organizacja zna swoje kluczowe systemy i dostawców, ma aktualne procedury reagowania na incydenty, regularnie testuje odporność oraz posiada umowy i plany wyjścia spełniające wymagania DORA?



Źródła

[Rozporządzenie Parlamentu Europejskiego i Rady \(UE\) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego](#)
[European Banking Authority - Preparations for reporting of DORA registers of information](#)

Zapraszamy do kontaktu!



Joanna Ostrowska

Partner | Leader of Digital,
Cyber & Data Team, EY Law
joanna.ostrowska@pl.ey.com



Agata Wilska

Project Manager | Digital,
Cyber & Data Team, EY Law
agata.wilska@pl.ey.com



Gabriela Sacha

Manager | Digital,
Cyber & Data Team, EY Law
gabriela.sacha@pl.ey.com

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.

Nazwa EY odnosi się do firm członkowskich Ernst & Young Global Limited, z których każda stanowi osobny podmiot prawny. Ernst & Young Global Limited, brytyjska spółka z odpowiedzialnością ograniczoną do wysokości sumy gwarancyjnej (company limited by guarantee), nie świadczy usług na rzecz klientów. Informacje na temat sposobu gromadzenia przez EY i przetwarzania danych osobowych oraz praw przysługujących osobom fizycznym w świetle przepisów o ochronie danych osobowych są dostępne na stronie ey.com/pl/pl/home/privacy. Firmy członkowskie EY nie prowadzą praktyki prawniczej, jeśli jest to zabronione przez prawo lokalne. Aby uzyskać więcej informacji, wejdź na www.ey.com/pl.

© 2026 EYGM Limited.
All Rights Reserved.
SCORE: 01002-162

Niniejsza publikacja została sporządzona z należytą starannością, jednak z konieczności pewne informacje zostały podane w skróconej formie. W związku z tym publikacja ma charakter wyłącznie orientacyjny, a zawarte w niej dane nie powinny zastąpić szczegółowej analizy problemu ani profesjonalnego osądu. EY nie ponosi odpowiedzialności za jakiegokolwiek straty powstałe w wyniku czynności podjętych ani zaniechanych na podstawie niniejszej publikacji. Zalecamy, by wszelkie przedmiotowe kwestie były konsultowane z właściwym doradcą.

ey.com/pl