NOWE TECHNOLOGIE

Zakres uproszczonych ram zarządzania ryzykiem w DORA

Objęcie uproszczonymi ramami zarządzania ryzykiem małych domów maklerskich będzie miało niebagatelne znaczenie dla wdrożenia wymogów DORA w tych instytucjach.

KRZYSZTOF ROŻKO

radca prawny, wspólnik zarządzający w Krzysztof Rożko i Wspólnicy Kancelaria Prawna

BARTOSZ POSŁUSZNY

radca prawny w Krzysztof Rożko i Wspólnicy Kancelaria Prawna

Ramy zarządzania ryzykiem w rozporządzeniu DORA, czyli Digital Operational Resilience Act, mają zastosowanie głównie do dostawców usług cyfrowych oraz instytucji finansowych. Ich zakres obejmuje identyfikację, ocenę i zarządzanie ryzykiem związanym z operacjami cyfrowymi, w tym zagrożeniami dla bezpieczeństwa, ciągłości działania i integralności danych.

W związku ze wzrostem znaczenia rozwiązań cyfrowych, a tym samym zagrożeń w obszarze cyberbezpieczeństwa, podejmowane są kolejne działania w ramach realizacji strategii odporności cyfrowej Unii Europejskiej ogłoszonej w 2020 r. Elementem tych działań jest przyjęcie rozporządzenia DORA, które zacznie być stosowane, począwszy od 17 stycznia 2025 r.

Przepisy DORA będą miały istotne znaczenie dla szeregu podmiotów finansowych oraz dostawców usług technologii informacyjno-komunikacyjnych (ICT). Jednakże nie wszystkie wymogi przewidziane w DORA będą dotyczyć podmiotów finansowych w tym samym stopniu. Część z nich zostanie całkowicie zwolniona z realizacji nowych obowiązków, inne zaś zobowiązane będą wdrożyć ich uproszczone wersje. Do tej drugiej grupy należą zwłaszcza małe podmioty finansowe, takie jak małe domy maklerskie. Na jakie ułatwienia mogą zatem liczyć mniejsi uczestnicy rynku kapitałowego?

Znaczenie skali działalności

Chociaż przepisy DORA obejmują szeroką grupę podmiotów finansowych, to w myśl zasady proporcjonalności ustawodawca unijny zdecydował o zróżnicowaniu rodzajów wymogów oraz ich intensywności w zależności od skali i rodzaju działalności prowadzonej przez dany podmiot. Ze względu na rozmiar prowadzonej działalności wybrane podmioty objęto wyłączeniem z zakresu regulacji DORA, dotyczy to m.in.:

- zarządzających alternatywnymi funduszami inwestycyjnymi (ZAFI), tj. funduszami inwestycyjnymi zamkniętymi, specjalistycznymi funduszami inwestycyjnymi otwartymi lub alternatywnymi spółkami inwestycyjnymi, w przypadku gdy łączna wartość zarządzanych przez ZAFI aktywów, w tym nabytych za pomocą dźwigni finansowej, ogółem nie przekracza progu 100 mln EUR lub progu 500 mln EUR, gdy ZAFI zarządza funduszami, które nie stosują dźwigni finansowej oraz w których prawa do umorzenia nie mogą być wykonywane przez okres pięciu lat od daty początkowej inwestycji;
- małych zakładów ubezpieczeń i zakładów reasekuracji oraz
- instytucji pracowniczych programów emerytalnych (liczących do 15 członków).

Dodatkowo wybrane małe podmioty finansowe, które nie zostały objęte wyłączeniem, będą zobowiązane spełnić łagodniejsze wymogi względem podstawowych ram zarządzania ryzykiem. W przypadku tych podmiotów znajdą bowiem zastosowanie uproszczone ramy zarządzania ryzykiem związanym z ICT. Dla porządku należy dodać, że przepisy DORA przewidują wyłączenia oraz modyfikacje w zakresie wybranych wymagań w przypadku mikroprzedsiębiorców, którzy jednak nie mają możliwości zastosowania ram uproszczonych.

Podmioty korzystające z ram uproszczonych

Możliwość stosowania uproszczonych ram zarządzania ryzykiem została ograniczona do wybranych podmiotów wskazanych w przepisach DORA.

Należą do nich:

- małe i niepowiązane wzajemnie firmy inwestycyjne,
- zwolnione instytucje płatnicze, zwolnione instytucje pieniądza elektronicznego oraz inne wybrane instytucje wskazane w odrębnych przepisach prawa unijnego oraz
- małe instytucje pracowniczych programów emerytalnych (obsługujące programy emerytalne liczące łącznie mniej niż 100 uczestników).

W powyższej grupie należy zwrócić szczególną uwagę na kategorię małych i niepowiązanych wzajemnie firm inwestycyjnych, rozumianych jako podmioty spełniające kryteria finansowe wskazane w rozporządzeniu IFR (rozporządzenie w sprawie wymogów ostrożnościowych dla firm inwestycyjnych), dotyczące m.in. wartości aktywów, którymi zarządza firma inwestycyjna, oraz wartości obsługiwanych zleceń. Na gruncie polskich przepisów wskazana grupa obejmuje małe domy maklerskie, których działalność uregulowano przepisami ustawy o obrocie instrumentami finansowymi stanowiącymi transpozycję do polskiego porządku prawnego unijnego pakietu regulacyjnego w obszarze nadzoru ostrożnościowego nad firmami inwestycyjnymi.

Wdrożenie odpowiednich rozwiązań wewnętrznych w zakresie cyberodporności może stanowić wyzwanie organizacyjne dla podmiotów finansowych

Podmioty wdrażające uproszczone ramy zarządzania ryzykiem związanym z ICT będą mogły skorzystać z ułatwień dotyczących m.in. węższego zakresu i mniejszej częstotliwości audytów wewnętrznych

Objęcie uproszczonymi ramami zarządzania ryzykiem małych domów maklerskich będzie miało niebagatelne znaczenie dla wdrożenia wymogów DORA w tych instytucjach. Pierwszym etapem procesu wdrożeniowego powinno być bowiem dokonanie autoidentyfikacji, w tym określenie profilu ryzyka podmiotu z uwzględnieniem skali i rodzaju prowadzonej działalności, rozpoznanie ram regulacyjnych obejmujących dany podmiot finansowy, a w konsekwencji obowiązków prawnych, które należy spełnić.

Uproszczone ramy

Chociaż wskazane wyżej podmioty finansowe skorzystają z ułatwień wynikających ze stosowania uproszczonych ram zarządzania ryzykiem, to nie zostały one objęte wyłączeniem odnośnie do pozostałych obowiązków przewidzianych w rozporządzeniu. W szczególności dotyczy to zarządzania incydentami ICT, testowania operacyjnej odporności cyfrowej czy wreszcie zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT. Niemniej również w tym zakresie w przepisach DORA przewidziano wyjątki względem podmiotów stosujących uproszczone ramy zarządzania ryzykiem.

Ogólne wymogi względem podmiotów stosujących uproszczone ramy zarządzania ryzykiem ICT obejmują przede wszystkim:

- wprowadzenie i utrzymanie udokumentowanych (uproszczonych) ram zarządzania ryzykiem związanym z ICT,
- stałe monitorowanie systemów ICT,
- reagowanie na incydenty ICT,
- identyfikację zależności od zewnętrznych dostawców usług ICT,
- zapewnienie ciągłości działania,
- regularne testowanie ram zarządzania ryzykiem oraz rozwiązań zapewniających ciągłość działania oraz
- stały rozwój w zakresie odporności cyfrowej, w tym przeprowadzanie szkoleń.

W stosunku do podstawowych ram zarządzania ryzykiem wersja uproszczona została uregulowana w treści DORA jedynie w podstawowym zakresie, a szczegółowe wymogi zostaną dookreślone w aktach wykonawczych do rozporządzenia (regulacyjnych standardach technicznych – RTS). Opublikowane projekty RTS precyzują elementy uproszczonych ram zarządzania ryzykiem, jak również rodzaje i składowe wymaganych polityk i procedur wewnętrznych, m.in. dotyczących polityki bezpieczeństwa informacji, ciągłości działania, kontroli dostępów oraz zarządzania projektami ICT.

Porównanie uproszczonych ram zarządzania ryzykiem do podstawowych wymogów przewidzianych przepisami DORA prowadzi do wniosku, że różnice pomiędzy nimi sprowadzają się przede wszystkim do stopnia złożoności rozwiązań mających na celu zapewnienie odporności cyfrowej podmiotu finansowego. Wynika to z przyjęcia założenia, że mniejsza skala działalności związana jest z odpowiednio niższym stopniem ryzyka w obszarze ICT, dlatego też stosowanie środków bezpieczeństwa powinno być realizowane w proporcjonalnie węższym zakresie.

Podmioty wdrażające uproszczone ramy zarządzania ryzykiem związanym z ICT będą mogły skorzystać z ułatwień dotyczących m.in. węższego zakresu i mniejszej częstotliwości audytów wewnętrznych, wyłączenia obowiązku utrzymywania nadmiarowych zdolności w zakresie ICT oraz posiadania systemów redundantnych (zastępczych). Dodatkowo podmioty te zwolnione będą z obowiązku raportowania w przypadku powtarzających się incydentów związanych z ICT, przeprowadzania zaawansowanych testów penetracyjnych ukierunkowanych przez analizę zagrożeń oraz obowiązku przyjmowania strategii dotyczącej ryzyka ze strony zewnętrznych dostawców usług ICT.

Wdrożenie wymaga przygotowania

Przepisy dotyczące uproszczonych ram zarządzania ryzykiem związanym z ICT przewidują mniej złożone wymagania względem ram podstawowych oraz wydają się dawać większą swobodę w zakresie ustalenia rodzaju środków bezpieczeństwa i zasad ich stosowania. Ma to na celu umożliwienie małym podmiotom finansowym wdrożenia minimalnych rozwiązań pozwalających na osiągnięcie cyberodporności przy jednoczesnym ograniczeniu obciążenia nałożonego na te podmioty. Należy jednak zwrócić uwagę, że pomimo wskazanych różnic oba rodzaje ram zarządzania pozostają bardzo zbliżone. Dlatego też ostateczny kształt wdrożonych rozwiązań (a tym samym stopień ich złożoności) będzie zależał od specyfiki działalności danego podmiotu finansowego i zidentyfikowanego przez niego poziomu ryzyka operacyjnego.

Niezależnie od ułatwień przewidzianych w przepisach DORA wdrożenie odpowiednich rozwiązań wewnętrznych może stanowić wyzwanie organizacyjne i finansowe, w szczególności w przypadku podmiotów, w tym małych domów maklerskich, które do tej pory nie posiadały szczegółowych rozwiązań w zakresie cyberbezpieczeństwa. Wobec tego ważne jest możliwie szybkie rozpoczęcie działań wdrożeniowych w celu zarówno ograniczenia ryzyka regulacyjnego, jak i zwiększenia odporności organizacji w zakresie cyberbezpieczeństwa. Nowe przepisy to nie tylko dodatkowe wymogi regulacyjne, ale również szansa dla podmiotów finansowych na poprawę bezpieczeństwa systemów informatycznych i ograniczenie negatywnych konsekwencji, w tym kosztów, związanych z występowaniem incydentów ICT. /