WYMOGI

Z wdrożeniem DORA nie należy czekać

Do 17 stycznia 2025 r. m.in. towarzystwa funduszy inwestycyjnych i domy maklerskie zobowiązane są do wdrożenia zharmonizowanych zasad operacyjnej odporności cyfrowej.

NIKOLA JADWISZCZAK-NIEDBAŁKA
BARTOSZ POSŁUSZNY

Intensywny rozwój usług elektronicznych oraz powszechność stosowania technologii cyfrowych stanowi istotny czynnik stymulujący rozwój gospodarek światowych, w tym rynków państw członkowskich UE. Niemniej, oprócz istotnych korzyści, stosowanie rozwiązań cyfrowych generuje znaczące wyzwania w zakresie cyberbezpieczeństwa. Odpowiedź na rosnące cyberzagrożenia stanowić ma Rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Celem jest zwiększenie cyfrowej odporności operacyjnej sektora finansowego UE poprzez wzmocnienie technologii informacyjno-komunikacyjnych (ICT). Nowe wymogi regulacyjne dotyczyć będą szerokiego grona podmiotów finansowych, chociaż zakres ich zastosowania będzie różnił się w zależności od skali i rodzaju prowadzonej działalności. Instytucje podlegające pod zakres DORA mają czas na ich wdrożenie do 17 stycznia 2025 r.

Domy maklerskie oraz TFI objęte DORA

Działania mające na celu odpowiednie dostosowanie swojej działalności do wymogów DORA powinny jak najszybciej podjąć m.in. towarzystwa funduszy inwestycyjnych (TFI) oraz domy maklerskie (DM), które jako jedne z licznych podmiotów sektora finansowego zostały objęte regulacjami w zakresie operacyjnej odporności cyfrowej z poziomu UE.

Zgodnie z art. 2 ust. 1 lit. e i k DORA co do zasady DORA ma zastosowanie do firm inwestycyjnych (DM) oraz zarządzających alternatywnymi funduszami inwestycyjnymi, tj. do tzw. ZAFI (na gruncie polskiego porządku prawnego są nimi TFI oraz zarządzający alternatywnymi spółkami inwestycyjnymi, tzw. ZASI). W odniesieniu jednak do TFI, jak i ZASI (łącznie jako ZAFI) ustawodawca unijny zdecydował się na wyłączenie stosowania DORA w zakresie, w jakim łączna wartość zarządzanych przez takiego ZAFI aktywów – w tym nabytych za pomocą dźwigni finansowej – ogółem nie przekracza progu 100 mln EUR. Limit ten wynosi 500 mln EUR, gdy ZAFI zarządza funduszami, które nie stosują dźwigni finansowej i jednocześnie, w których prawa do umorzenia nie mogą być wykonywane przez okres pięciu lat od daty początkowej inwestycji (minimum 5-letni lock up).

Na polskim rynku będą zatem takie TFI (jak i ZASI), które nie będą zobowiązane do stosowania wymogów regulacyjnych DORA, bo też pod zakres podmiotowy tego rozporządzenia w ogóle nie będą podpadać. W związku z tym, że ustawodawca przyjął kryterium warunkujące podleganie bądź nie pod wymogi DORA na podstawie wartości zarządzanych przez TFI aktywów (odpowiednio 100 mln EUR i 500 mln EUR) i jednocześnie nie przewidział przepisów przejściowych, które wprowadzałyby dla takich TFI odpowiedni okres na dostosowanie, te z nich, które obecnie znajdują się nieznacznie pod progiem, mogą być zmuszone do przyjęcia odpowiednich rozwiązań wdrażających DORA na wypadek przekroczenia wskazanych wyżej progów. Pytanie jednak, jaka wartość zarządzanych aktywów powinna zmusić TFI do podjęcia działań wdrażających jeszcze przed przekroczeniem progów, o których mowa w DORA? Z pewnością przyjęcie odpowiedniego rozwiązania w tym zakresie stanowi jedną z większych trudności na gruncie DORA.

W odniesieniu do DM wskazać należy, że ustawodawca przyjął rozwiązanie polegające na ograniczeniu zakresu obowiązków nakładanych DORA w odniesieniu do małych, niepowiązanych wzajemnie firm inwestycyjnych, którymi na gruncie ustawy o obrocie instrumentami finansowymi są tzw. małe domy maklerskie. W ocenie ustawodawcy unijnego uzasadnione jest przyjęcie, że niektóre podmioty finansowe – ze względu na ich wielkość lub świadczone usługi – są objęte łagodniejszymi wymogami lub zwolnieniami.

Nowe (stare) ramy zarządzania ryzykiem

Bez wątpienia przyjęcie z poziomu UE rozporządzenia regulującego zharmonizowane zasady operacyjnej odporności cyfrowej są rewolucją dla podmiotów, które dotychczas w ogóle nie były objęte podobnymi regulacjami. Jak jest w przypadku TFI i DM?

Dotychczas w działalności TFI i DM istotne znaczenie miały regulacje wynikające z ustaw sektorowych – odpowiednio ustawy o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi oraz ustawy o obrocie instrumentami finansowymi oraz rozporządzenia wykonawcze do tych aktów. Oprócz jednak zasad dotyczących outsourcingu oraz generalnych zasad, wedle których powinien działać system zarządzania ryzykiem w tych podmiotach, próżno szukać w wymienionych aktach prawnych regulacji odnoszących się stricte do operacyjnej odporności cyfrowej oraz ochrony zasobów ICT przed zagrożeniami.

Co prawda takie działanie TFI, jak i DM powinny podejmować oraz regulować chociażby z poziomu odpowiedniego zarządzania ryzykiem operacyjnym i ryzykiem związanym z bezpieczeństwem informacji, to jednak na podstawie obecnie obowiązujących przepisów ustaw sektorowych brak szczególnych wytycznych w zakresie zarządzania ryzykiem ICT. Wskazówki w tym zakresie można jednak było dotychczas odnaleźć w stanowiskach i wytycznych nadzorczych, w szczególności wytycznych UKNF dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego – odrębnie dla TFI i DM, czy komunikacie chmurowym, wytycznych EBA w sprawie outsourcingu czy też wytycznych w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT. Ponadto system zarządzania ryzykiem ICT powinien być zgodny z dotychczas obowiązującymi normami międzynarodowymi, w szczególności normami ISO.

W zakresie zarządzania ryzykiem jako takim podejście oparte na zasadzie risk based approach jest znane TFI i DM z dotychczas stosowanych rozwiązań na gruncie przepisów RODO czy AML. Niemniej, dotychczasowe regulacje sektorowe jedynie częściowo uwzględniały rozwiązania odnoszące się do ryzyka związanego z ICT. Brak zharmonizowania przepisów w tym obszarze skutkował z kolei poważnymi lukami oraz niespójnościami wynikającymi z wprowadzanych rozbieżnych rozwiązań w różnych krajach UE. DORA ma stanowić remedium na przedmiotowe bolączki.

Jak się przygotować

Przepisy DORA w dużej mierze bazują na dotychczasowych rozwiązaniach, rozproszonych po wymienionych wcześniej aktach prawnych, wytycznych oraz normach międzynarodowych, i gromadzą je w pięciu zasadniczych obszarach:

- zarządzanie ryzykiem związanym z ICT,
- zarządzanie incydentami związanymi z ICT,
- testowanie cyfrowej odporności operacyjnej,
- zarządzanie ryzykiem współpracy z zewnętrznymi dostawcami, oraz
- wymiana informacji dotyczącej zagrożeń cybernetycznych.

Kluczem do wdrożenia rozwiązań mających na celu zwiększenie cyberbezpieczeństwa jest uwzględnienie środowiska wewnętrznego i zewnętrznego organizacji, jej strategii biznesowej i ogólnego profilu ryzyka, w celu podjęcia działań proporcjonalnych do charakteru prowadzonej działalności.

W procesie wdrożenia lub dostosowania regulacji wewnętrznych do przepisów DORA, TFI i DM powinny w pierwszej kolejności dokonać przeglądu zasobów ICT i dotychczas obowiązujących regulacji wewnętrznych, dokonać analizy luk (zidentyfikować braki) i dotychczasowego umiejscowienia obszaru ICT w strukturze organizacyjnej oraz zbadać, czy osoby dotychczas zajmujące się tym obszarem w organizacji rzeczywiście posiadają odpowiednią wiedzę i kompetencje w tym zakresie. Kolejne działania dostosowawcze powinny oscylować wokół opracowania i przyjęcia procedur wewnętrznych. Ostatni krok to wdrożenie regulacji przyjętych na gruncie procedur – przyjęcie odpowiednich rozwiązań technologicznych i operacyjnych, które pozwolą na skuteczne wykonywanie obowiązków wynikających z procedur wewnętrznych (stanowiących odzwierciedlenie, z uwzględnieniem jednak zasady proporcjonalności, wymogów DORA). /®

ZDANIEM AUTORÓW

Nikola Jadwiszczak-Niedbałka

radca prawny w Krzysztof Rożko i Wspólnicy Kancelaria Prawna

MATPRAS.

Bartosz Posłuszny

radca prawny w Krzysztof Rożko i Wspólnicy Kancelaria Prawna

MATPRAS.

Mimo że przepisy DORA są bezpośrednio stosowane, obecnie trwają prace nad projektem ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego, a KNF już teraz sygnalizuje rozpoczęcie kontroli w zakresie zgodności z wymogami przewidzianymi w DORA począwszy od 18 stycznia 2025 r. TFI i DM pozostało zatem niewiele czasu na podjęcie działań dostosowawczych. Co istotne, oprócz zapewnienia zasobów ludzkich do przeprowadzenia działań wdrożeniowych, TFI i DM powinny w budżetach na 2024 r. przewidzieć koszty związane z wdrożeniem, które z uwagi na specyfikę i szeroki zakres mogą okazać się znaczne. Rzetelne podejście do kwestii wdrożenia wymogów DORA zmityguje jednak nie tylko ryzyka w zakresie cyberzagrożeń, ale również ryzyka nadzorcze – a te zmaterializują się automatycznie, jeśli w styczniu 2025 r. TFI i DM nie będą jeszcze w pełni dostosowane.