Jak zmieni się nasze otoczenie prawne?

Rozporządzenia DORA | implementacja w polskim sektorze bankowym

Paweł Rudolf | Counsel

Konwentu na rzecz Współpracy i Rozwoju Polskiej Bankowości Spółdzielczej

Józefów, 18 stycznia 2024 r.

DORA skierowana jest głównie do instytucji rynku finansowego, w tym przede wszystkim do:

banków (instytucji kredytowych)	firm inwestycyjnych	instytucji płatniczych	zakładów ubezpieczeń i reasekuracji	instytucji pieniądza elektronicznego
dostawców usług z zakresu kryptoaktywów	zarządzających alternatywnymi funduszami inwestycyjnymi	dostawców usług finansowania społecznościowego (crowdfunding)	repozytoriów sekurytyzacji	administratorów kluczowych wskaźników referencyjnych
	kontrahentow centralnych	zewnętrzni dostawcy usług ICT	przewiduje szereg wyłączeń w zakresie jej stosowania, w tym „opcje nardowe”	

DZP

DORA | Główne obszary regulacji

Zarządzanie ryzykiem związanym z ICT

- wewnętrzne ramy zarządzania i kontroli, które zapewniają skuteczne i ostrożne zarządzanie wszystkimi rodzajami ryzyka związanego z ICT*

Zarządzanie incydentami związanymi z ICT, ich klasyfikacja i zgłaszanie

- identyfikowanie, śledzenie, rejestrowanie, kategoryzowanie i klasyfikowania oraz zgłaszanie incydentów związanych z ICT według ich priorytetu i dotkliwości oraz krytyczności usług, na które incydenty te mają wpływ

Testowanie operacyjnej odporności cyfrowej

- ustanowienie i utrzymywanie adekwatnego i kompleksowego programu testowania operacyjnej odporności cyfrowej stanowiącego integralną część ram zarządzania ryzykiem związanym z ICT

Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT

- zarządzanie ze strony zewnętrznych dostawców usług ICT odbywa się w świetle zasady proporcjonalności, z uwzględnieniem charakteru, skali, stopnia złożoności i znaczenia zależności w zakresie ICT

Zasady dotyczące wymiany informacji

- podmioty finansowe mogą wymieniać między sobą informacje o cyberzagrożeniu i wyniki analiz takiego cyberzagrożenia, w tym oznaki naruszenia integralności systemu, taktykę, techniki i procedury

**odpowiednie rozdzielenie i niezależność funkcji zarządzania ryzykiem związanym z ICT, funkcji kontroli oraz funkcji audytu wewnętrznego, zgodnie z modelem trzech linii obrony lub wewnętrznym modelem zarządzania ryzykiem i kontroli ryzyka.*

DZP

DORA | Terminarz

- 28 listopada 2022 r. Rada UE przyjęła Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego (ang. *Digital Operational Resilience Act*)

- Rozporządzenie weszło w życie 16 stycznia 2023 r. i będzie obowiązywać od 17 stycznia 2025 r.

- Dla prawidłowego stosowania DORA do 17 stycznia 2024 r. mają zostać wydane przez właściwe unijne organy dodatkowe nadzorcze regulacyjne standardy techniczne (RTS)

- Europejskie Urzędy rozpoczęły w dniu 19 czerwca 2023 r. konsultacje społeczne w sprawie pierwszej partii standardów technicznych, które zakończyły się 11 września 2023 r.

DORA

Pierwszy pakiet RTS

Pierwszy pakiet regulacyjnych standardów technicznych został przygotowany na podstawie mandatów przewidzianych w art. 15 i art. 16 ust. 3 DORA

Z uwagi na ich spójność merytoryczną i tematyczną, rozporządzenia DORA zostały one połączone w jeden projekt standardów technicznych.

Co istotne:

Wytyczne zawarte w RTS uzupełniają i uszczegóławiają wymogi w zakresie zarządzania ryzykiem w obszarze ICT, uregulowane w Rozporządzeniu DORA. Nie są one w żadnym wypadku przepisami „konkurencyjnymi" do regulacji DORA i nie powinny być interpretowane w oderwaniu od DORA.

DORA

Obszary regulacji RTS

- doprecyzowanie elementów, które należy uwzględnić w politykach, procedurach, protokołach i narzędziach w zakresie bezpieczeństwa ICT
- doprecyzowanie elementów kontroli praw zarządzania dostępem oraz związanej z nimi polityki zasobów ludzkich określającej prawa dostępu, procedury przyznawania i cofania praw, monitorowanie nietypowych zachowań w odniesieniu do ryzyka związanego z ICT
- doprecyzowanie elementów umożliwiających szybkie wykrywanie nietypowych działań oraz kryteriów uruchamiania procesów wykrywania incydentów związanych z ICT i reagowania na nie
- doprecyzowanie elementów strategii na rzecz ciągłości działania w zakresie ICT

DORA

Obszary regulacji RTS

- doprecyzowanie testowania planów ciągłości działania w zakresie ICT
- doprecyzowanie elementów planów reagowania i przywracania sprawności ICT
- doprecyzowanie treści i formatu sprawozdania z przeglądu ram zarządzania ryzykiem związanym z ICT
- doprecyzowanie elementów, jakie należy ująć w ramach zarządzania ryzykiem związanym z ICT w przypadku uproszczonych ram zarządzania ryzykiem związanym z ICT

DORA

Wytyczne zawarte w RTS (art. 15)

- opracowanie, udokumentowanie i wdrożenie polityki zarządzania zasobami ICT
- opracowanie, udokumentowanie i wdrożenie kompleksowej polityki szyfrowania i kontroli kryptograficznej
- posiadanie polityk, procedur, protokołów i narzędzi wspierających zarządzanie bezpieczeństwem sieci (m.in. segregacja oraz segmentacja systemów i sieci teleinformatycznych z uwagi na krytyczność wspieranych funkcji, a także z uwzględnieniem klasyfikacji i ogólnego profilu ryzyka zasobów teleinformatycznych, które z tych systemów i sieci korzystają)

DORA

Wytyczne zawarte w RTS (art. 15)

- opracowanie, udokumentowanie i wdrożenie polityki w zakresie nabywania, rozwoju i utrzymania systemów ICT, obejmujące w szczególności środki mające na celu ograniczenie ryzyka niezamierzonej zmiany lub celowej manipulacji systemami ICT na wszystkich etapach użytkowania (podczas rozwoju, utrzymywania oraz wdrażania w środowisku produkcyjnym)
- udokumentowanie procedur operacyjnych ICT, w tym zarządzania zasobami (także w zakresie ich optymalizacji), monitorowania przepustowości i wydajności oraz zarządzania podatnościami i poprawkami

DORA

Wytyczne zawarte w RTS (art. 15)

- operacyjne aspekty bezpieczeństwa ICT, w tym kwestia zarządzania przepustowością i wydajnością sieci oraz systemów.
- wytyczne do zarządzania projektami ICT, w aspekcie m.in.. rozwoju, pozyskiwania i utrzymania systemów ICT.
- wprowadzono konieczność przygotowania i wdrożenia polityki bezpieczeństwa fizycznego i środowiskowego, która ma zawierać postanowienia w zakresie bezpieczeństwa pomieszczeń, centrów danych i sprzętu komputerowego.

Obszary RTS (art. 16)

Zarządzanie ryzykiem ICT

- polityka obejmująca jasne określenie ról i obowiązków;
- klasyfikacja informacji i zasobów ICT
- proces zarządzania ryzykiem ICT;
- proces zarządzania incydentami związanymi z ICT
- bezpieczeństwo fizyczne i środowiskowe

Ograniczanie ryzyka

- procesy związane z dostępem logicznym i fizycznym
- monitorowanie i zarządzanie zasobami ICT
- ochrona danych
- testowanie bezpieczeństwa ICT
- nabywanie, rozwój i utrzymanie systemów ICT

Zarządzanie ciągłością działania ICT

- analizy wpływu na działalność
- opracowywanie, planów ciągłości działania ICT
- zatwierdzanie planów ciągłości działania ICT
- testowanie planów ciągłości działania ICT

Raportowanie ram zarządzania ryzykiem ICT

- dokonywanie przeglądu ram zarządzania ryzykiem ICT
- obowiązek przedstawienia przeglądu ram zarządzania ryzykiem ICT na żądanie organu nadzoru finansowego

DORA

Pozostałe wytyczne

- RTS w sprawie kryteriów kwalifikacji incydentów związanych z ICT (art. 18 ust. 3 DORA),
- RTS w sprawie szczegółowej treści polityki umownej dla korzystania z zewnętrznych usług ICT wspierających krytyczne lub istotne funkcje (art. 28 ust. 10 DORA),
- ITS w sprawie ustanowienia standardowych wzorów rejestru informacji o zewnętrznych dostawcach usług ICT art. 28 ust. 9 DORA).

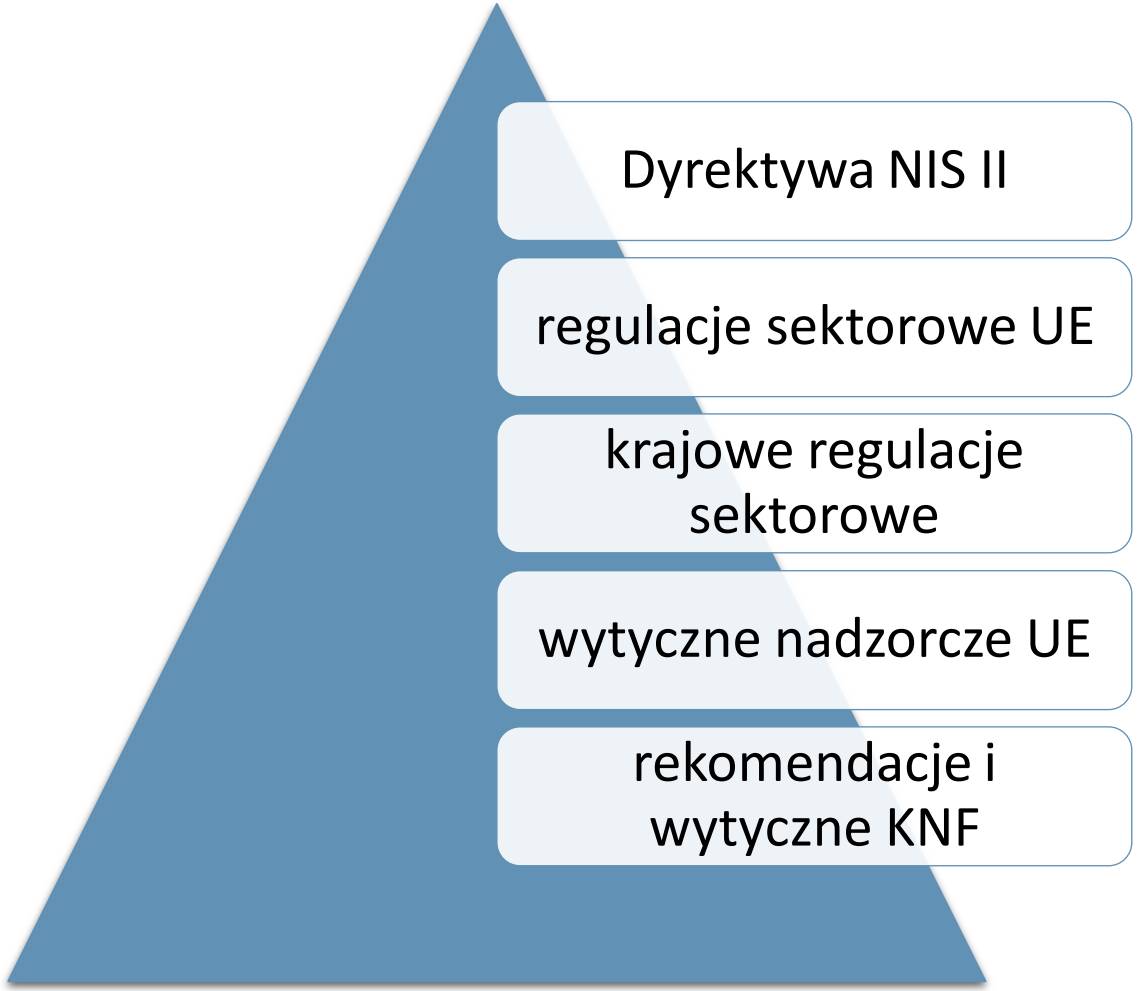
DORA

Otwarte konsultacje drugiego pakietu (08.12.2023-04.03.2024)

- RTS w sprawie dookreślenia treści zgłoszeń i szczegółowych terminów raportowania incydentów związanych z ICT (art. 20 lit a DORA),
- ITS w sprawie dookreślenia formatów, wzorów i procedur raportowania incydentów związanych z ICT (art. 20 lit b DORA),
- RTS w sprawie dookreślenia szczegółowych zasad przeprowadzania testów penetracyjnych i nadzoru nad nimi, z uwzględnieniem standardu TIBER-EU (art. 26 ust. 11 DORA)
- RTS w sprawie elementów do dookreślenia w przypadku zlecania podwykonawstwa usług ICT wspierających krytyczne lub istotne funkcje (art. 30 ust. 5 DORA),
- RTS w sprawie harmonizacji zasad sprawowania nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT (art. 41 ust. 1 DORA).

23 stycznia 2024 – wysłuchanie publiczne

DORA a regulacje szczególne



DORA | Wdrożenie

FAZA I - AUDYT

- analiza dokumentacji i procedur
- opracowanie szczegółowego planu fazy wdrożenia

FAZA II - IMPLEMENTACJA

- dostosowanie dokumentacji i procedur
- przeprowadzenie klasyfikacji informacji, systemów i procesów biznesowych - przegląd i aktualizacja
- opracowanie procedury testowania operacyjnej odporności cyfrowej
- opracowanie struktury organizacyjnej dostosowanej do wielkości operacji i bezpieczeństwa IT oraz złożoności infrastruktury teleinformatycznej
- przygotowanie opisu zadań na poszczególnych stanowiskach w obszarze zarządzania ryzykiem IT i bezpieczeństwa IT
- przygotowanie opisu procesów w obszarze zarządzania ryzykiem i bezpieczeństwa IT

FAZA III – UTRZYMANIE I MONITORING

- bieżąca weryfikacja wdrożenia
- zapewnienie zgodności działania z rozporządzeniem DORA

DZP

DORA | Dlaczego jest tak istotna?

Motyw 12:

„(…)Przepisy dotyczące ryzyka operacyjnego, jeżeli zostały szerzej rozwinięte w unijnych aktach prawnych, często sprzyjały tradycyjnemu ilościowemu podejściu do zwalczania ryzyka (polegającemu na określeniu wymogu kapitałowego na potrzeby pokrycia ryzyka związanego z ICT), a nie ukierunkowanym przepisom jakościowym dotyczącym zdolności w zakresie ochrony, wykrywania, powstrzymywania, przywracania sprawności i odbudowy w odniesieniu do incydentów związanych z ICT lub zdolności w zakresie sprawozdawczości i testowania cyfrowego. (…)”

DZP

Dziękuję za uwagę. Zapraszam

Paweł Rudolf
Counsel

Jak nas znaleźć w sieci?

Nasze profile w social mediach.

www.dzp.pl

Blogi DZP: Life Sciences, IP, Prawo pracy, Podatki, Compliance

LinkedIn: DZP LinkedIn Profile

Facebook: DZP Life Sciences Law Blog

Youtube: DZP more than law

DZP

Biuro w Warszawie
Rondo ONZ 1
00-124 Warszawa
T + 48 22 557 76 00
F + 48 22 557 76 01

Biuro w Poznaniu
ul. Paderewskiego 8
61-770 Poznań
T + 48 61 642 49 00
F + 48 61 642 49 50

Biuro we Wrocławiu
ul. Św. Mikołaja 7
50-125 Wrocław
T + 48 71 712 47 00
F + 48 71 712 47 50