Warszawa, 31 grudnia 2024 roku

Stanowisko UKNF dotyczące stosowania przez podmioty finansowe Rozporządzenia DORA

Rozporządzenie DORA[1], którego celem jest zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych oraz uregulowanie świadczenia usług ICT na rzecz podmiotów finansowych, będzie stosowane od 17 stycznia 2025 roku. Rozporządzenie DORA weszło w życie 16 stycznia 2023 roku i przewidywało 2-letni okres na dostosowanie się podmiotów finansowych do wymogów wynikających z jego przepisów. Okres ten kończy się 16 stycznia 2025 roku.

Rozporządzenie DORA jest aktem bezpośrednio stosowanym i nie wymaga odrębnej transpozycji do prawa krajowego. Obecny brak przepisów krajowych zapewniających stosowanie rozporządzenia DORA nie wstrzymuje obowiązku przestrzegania przez podmioty finansowe[2] wszelkich wymogów wynikających z przepisów rozporządzenia DORA.

Począwszy od 17 stycznia 2025 roku aktualizują się także zadania Komisji Nadzoru Finansowego (KNF) jako właściwego organu (organu nadzoru), wynikające z bezpośrednio stosowanych przepisów rozporządzenia DORA. KNF jest organem właściwym z mocy przepisów rozporządzenia DORA we wszystkich przypadkach, gdy na mocy obowiązujących przepisów krajowych została wyznaczona jako organ właściwy w rozumieniu przepisów aktów prawa UE wymienionych w art. 46 lit. a-q rozporządzenia DORA, z zastrzeżeniem kompetencji Europejskich Urzędów Nadzoru (EUN).

Stosowanie rozporządzenia DORA od 17 stycznia 2025 roku

EUN opublikowały 4 grudnia 2024 roku stanowisko dotyczące stosowania rozporządzenia DORA[3], zgodnie z którym:

1) w związku z tym, że rozporządzenie DORA wraz z aktami wykonawczymi[4] będzie miało zastosowanie od 17 stycznia 2025 roku, EUN wezwały podmioty finansowe oraz zewnętrznych dostawców usług ICT do przyspieszenia przygotowań w celu zapewnienia ich gotowości do stosowania wymogów tego rozporządzenia;

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011. Dz. Urz. UE L 333 z 27.12.2022, str. 1. Dziennik Urzędowy UE serii L z tekstem rozporządzenia DORA jest dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022R2554.

[2] Podmioty, o których mowa w art. 2 ust. 1 lit. a-t rozporządzenia DORA, z wyłączeniem podmiotów, o których mowa w art. 2 ust. 3 rozporządzenia DORA, zwane dalej „podmiotami finansowymi".

[3] https://www.eba.europa.eu/sites/default/files/2024-12/0133f341-fcf5-48d1-812b-d0a66e2b3e8c/JC%202024%2099_ESAs%20Public%20Statement%20on%20DORA%20application%20%281%29.pdf

[4] https://www.knf.gov.pl/dla_rynku/dora

2) ze względu na to, że rozporządzenie DORA będzie stosowane od 17 stycznia 2025 roku, EUN podkreślają znaczenie przyjęcia przez podmioty finansowe solidnego i ustrukturyzowanego podejścia zapewniającego terminowe wywiązywanie się ze swoich obowiązków;

3) EUN oczekują, że podmioty finansowe w odpowiednim czasie zidentyfikują i usuną luki związane z wdrożeniem rozporządzenia DORA, przy czym wymagania tego rozporządzenia nie są zupełnie nowe i część z nich obowiązuje podmioty od wielu lat w związku z wcześniejszymi oczekiwaniami nadzorczymi, rekomendacjami lub wytycznymi sektorowymi w obszarach zarządzania ryzykiem ICT, zgłaszania incydentów i outsourcingu[5];

4) EUN przyznają, że w przypadku niektórych podmiotów finansowych, które do tej pory podlegały w mniejszym zakresie sektorowym wymogom dotyczącym operacyjnej odporności cyfrowej, zapewnienie zgodności z rozporządzeniem DORA może wymagać większego zaangażowania i nakładu czasu oraz pracy;

5) EUN i właściwe organy udzielały i będą nadal udzielać wskazówek w celu wsparcia sprawnego wdrażania rozporządzenia DORA;

6) podmioty finansowe powinny przygotować się do nowych obowiązków sprawozdawczych, w tym w szczególności opracować rejestry ustaleń umownych dotyczących zewnętrznych dostawców usług ICT (rejestry informacji), które właściwe organy są zobowiązane zebrać od podmiotów finansowych i przekazać do EUN do 30 kwietnia 2025 roku[6];

7) opracowując rejestry informacji podmioty finansowe powinny stosować wymogi wynikające z rozporządzenia 2024/2956[7], a także rozważyć wykorzystanie wniosków wyciągniętych z ćwiczeń Dry run przeprowadzonych w 2024 roku;

8) podmioty finansowe powinny być również gotowe do klasyfikowania i zgłaszania poważnych incydentów związanych z ICT od daty rozpoczęcia stosowania rozporządzenia DORA;

9) biorąc pod uwagę profil ryzyka, wielkość, skalę i złożoność działalności poszczególnych podmiotów finansowych, właściwe organy powinny być gotowe do

[5] Na przykład: Wytyczne EUNB dotyczące zarządzania ryzykiem związanym z bezpieczeństwem ICT (EBA/GL/2019/04), Wytyczne EUNB dotyczące ustaleń w zakresie outsourcingu (EBA/GL/2019/02), Wytyczne EUNB dotyczące zgłaszania poważnych incydentów na podstawie drugiej dyrektywy w sprawie usług płatniczych (EBA/GL/2021/03), Wytyczne EIOPA dotyczące bezpieczeństwa ICT i zarządzania ICT (EIOPA-BoS-20/60), wytyczne ESMA dotyczące outsourcingu do dostawców usług w chmurze (ESMA50-164-4285) oraz Wytyczne EIOPA dotyczące outsourcingu do dostawców usług w chmurze (EIOPA-BoS-20-002).

[6] https://www.esma.europa.eu/sites/default/files/2024-11/ESA_2024_22_Decision_on_reporting_of_information_for_CTPP_designation.pdf

[7] Rozporządzenie wykonawcze Komisji (UE) 2024/2956 z dnia 29 listopada 2024 r. ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) DORA w odniesieniu do standardowych wzorów na potrzeby rejestru informacji.

sprawowania nadzoru w zakresie wymogów wynikających z rozporządzenia DORA w oparciu o analizy ryzyka i z uwzględnieniem strategicznych priorytetów nadzorczych EUNB, ESMA i EIOPA[8], które podkreślają operacyjną odporność cyfrową;

10) EUN będą kontynuowały współpracę z właściwymi organami w celu wypracowania pragmatycznego i ukierunkowanego na wyniki oraz terminowego podejścia do wdrażania rozporządzenia DORA;

11) EUN zapraszają zewnętrznych dostawców usług ICT, którzy uważają, że mogą spełniać kryteria krytyczności opublikowane w maju 2024 roku[9], do oceny ich struktury operacyjnej pod kątem wymogów rozporządzenia DORA, przy czym pierwsze wyznaczenie kluczowych zewnętrznych dostawców usług ICT planowane jest w drugiej połowie 2025 roku.

Urząd Komisji Nadzoru Finansowego (UKNF) opublikował Priorytety nadzorcze UKNF na 2025 rok[10], w ramach których również podkreśla się znaczenie osiągnięcia operacyjnej odporności cyfrowej sektora finansowego poprzez skuteczny i efektywny nadzór nad ryzykiem związanym z ICT podmiotów rynku finansowego zgodnie z rozporządzeniem DORA.

Poszczególne obowiązki i uprawnienia wynikające z przepisów rozporządzenia DORA aktualizują się 17 stycznia 2025 roku (art. 64 akapit drugi rozporządzenia DORA), niezależnie od braku przepisów krajowych zapewniających stosowanie rozporządzenia DORA[11]. Mając na uwadze obecny stan prac legislacyjnych[12] nad projektem ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emisji europejskich zielonych obligacji (UC11)[13], należy spodziewać się co najmniej kilkunastotygodniowego przesunięcia terminu uchwalenia i wejścia w życie przepisów prawa krajowego względem terminu rozpoczęcia stosowania przepisów rozporządzenia DORA.

UKNF oczekuje, że działania dostosowawcze podmiotów finansowych w zakresie wdrożenia wymogów rozporządzenia DORA zostaną zrealizowane najpóźniej do 17 stycznia 2025 roku.

Ponadto UKNF oczekuje, że począwszy od dnia rozpoczęcia stosowania rozporządzenia DORA podmioty finansowe będą stosowały się do sposobu i trybu wykonywania określonych obowiązków informacyjnych i sprawozdawczych zgodnie z niniejszym stanowiskiem, w zakresie:

(1) obowiązku posiadania identyfikatora LEI;

[8] EIOPA: https://www.eiopa.europa.eu/document/download/0df4b1d5-245c-4814-b171-ae98d7f8999f_en?filename=JC%202024%2099_ESAs%20Public%20Statement%20on%20DORA%20application.pdf, ESMA: https://www.esma.europa.eu/press-news/esma-news/esma-put-cyber-risk-new-union-strategic-supervisory-priority, EUNB: https://www.eba.europa.eu/sites/default/files/2024-07/ef6cf1ab-94fe-453f-9e4d-37231153cfac/2025%20EBA%20ESEP.pdf
[9] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32024R1502
[10] https://www.knf.gov.pl/knf/pl/komponenty/img/Priorytety_nadzorcze_UKNF_na_2025.pdf
[11] https://legislacja.gov.pl/projekt/12384252/katalog/13053526#13053526
[12] Aktualnie projekt nadal pozostaje na etapie prac toczących się w ramach rządowego procesu legislacyjnego.
[13] Zwany dalej „projektem ustawy (UC11)" lub „przepisami krajowymi".

(2) pierwszych obowiązków sprawozdawczych od 17 stycznia 2025 roku;

(3) zgłaszania poważnych incydentów związanych z ICT oraz znaczących cyberzagrożeń;

(4) prowadzenia i przekazania rejestru informacji dotyczącego umów z zewnętrznymi dostawcami usług ICT.

Jest to podyktowane koniecznością zapewnienia maksymalnej efektywności przepisów prawa Unii Europejskiej i ułatwi późniejsze przestrzeganie dodatkowych wymogów przewidzianych prawem krajowym.

(1) Obowiązek posiadania identyfikatora LEI

Na potrzeby realizowania obowiązków wynikających z rozporządzenia DORA, w tym obowiązków sprawozdawczych, podmioty finansowe są zobowiązane do posiadania identyfikatora LEI[14] od 17 stycznia 2025 roku. Identyfikator ten stanowić będzie niezbędny element sprawozdawczości, a jego uzupełnienie będzie konieczne dla przekazania formularzy sprawozdawczych do KNF jako właściwego organu, a następnie do przekazania części z nich przez KNF do Europejskich Urzędów Nadzoru.

Z uwagi na powyższe istotne jest, aby podmioty finansowe objęte wymogami Rozporządzenia DORA, które nie posiadają jeszcze identyfikatora LEI, wystąpiły o jego uzyskanie i uzyskały go przed 17 stycznia 2025 roku, tj. przed datą rozpoczęcia stosowania omawianego rozporządzenia.

Identyfikator LEI jest nadawany przez uprawnione do tego licencjonowane jednostki. Szczegółowe informacje o identyfikatorze LEI oraz o możliwościach jego uzyskania, w tym lista podmiotów nadających te kody (numery), znajdują się na stronie internetowej Global Legal Entity Identifier Foundation (GLEIF)[15] – podmiotu nadzorującego globalny system nadawania tych kodów.

W Polsce kod LEI można uzyskać za pośrednictwem Krajowego Depozytu Papierów Wartościowych SA (KDPW)[16].

(2) Pierwsze obowiązki sprawozdawcze od 17 stycznia 2025 roku

Kategorie podmiotów finansowych zobowiązanych do stosowania przepisów rozporządzenia DORA, a tym samym realizowania obowiązków sprawozdawczych, zostały określone w art. 2 oraz art. 16 rozporządzenia DORA.

Realizacja obowiązków sprawozdawczych przez podmioty finansowe ma na celu:

[14] LEI (ang. *Legal Entity Identifier*) – Identyfikator podmiotu prawnego (LEI) to złożony z 20 znaków kod alfanumeryczny oparty na normie ISO 17442 opracowanej przez Międzynarodową Organizację Normalizacyjną (ISO). Jest powiązany z kluczowymi informacjami umożliwiającymi jednoznaczną identyfikację podmiotów prawnych uczestniczących w transakcjach finansowych i innych oficjalnych interakcjach. Każdy kod LEI zawiera informacje o strukturze własnościowej podmiotu.
[15] https://www.gleif.org/pl/
[16] https://lei.kdpw.pl/

1) wymianę danych w postaci elektronicznej pomiędzy podmiotami finansowymi a KNF w zakresie wykonywania przez nie obowiązków określonych w przepisach rozporządzenia DORA;
2) umożliwienie KNF sprawowania nadzoru nad rynkiem finansowym w zakresie operacyjnej odporności cyfrowej poprzez realizację procesu komunikacji, sprawozdawczości oraz rozbudowanej analityki danych w sposób zautomatyzowany, niezawodny, ujednolicony oraz bezpieczny.

Obowiązki sprawozdawcze powinny być realizowane przez podmioty finansowe wyłącznie w postaci elektronicznej z wykorzystaniem systemów teleinformatycznych wskazanych przez UKNF, za pośrednictwem udostępnionych formularzy sprawozdawczych, a także w określonych terminach.

Nie wszystkie obowiązki sprawozdawcze będą wymagane już od 17 stycznia 2025 roku. W pierwszej kolejności podmioty finansowe powinny być przygotowane do realizowania obowiązków sprawozdawczych, w szczególności w zakresie obejmującym:

1) **SPR-PF-03**_Sprawozdanie obejmujące kopie wyników testów ciągłości działania w zakresie ICT lub podobnych testów[17];
2) **SPR-PF-07**_Wstępne powiadomienie i sprawozdanie dotyczące poważnych incydentów ICT;
3) **SPR-PF-08**_Sprawozdanie śródokresowe dotyczące poważnych incydentów ICT;
4) **SPR-PF-09**_Sprawozdanie końcowe dotyczące poważnych incydentów ICT;
5) **SPR-PF-10**_Sprawozdanie dotyczące powiadomienia o znaczącym cyberzagrożeniu;
6) **SPR-PF-18**_Sprawozdanie dotyczące pełnego rejestru informacji lub innego zakresu informacji zgodnie z żądaniem;
7) **SPR-PF-19**_Sprawozdanie dotyczące planowanych ustaleń umownych obejmujących korzystanie z usług ICT wspierających krytyczne lub istotne funkcje;
8) **SPR-PF-20**_Sprawozdanie dotyczące planowanych ustaleń umownych obejmujących korzystanie z usług ICT wspierających funkcje, które stały się krytyczne lub istotne;
9) **SPR-PF-22**_Powiadomienie o przystąpieniu (lub utracie członkostwa) do wymiany informacji o cyberzagrożeniach w zaufanych społecznościach podmiotów finansowych;
10) **SPR-PF-23**_Sprawozdanie na potrzeby sprawowania nadzoru, prowadzenia dochodzeń i nakładania sankcji - dokumenty lub dane przekazywane w ramach nadzoru bieżącego;
11) **SPR-PF-24**_Sprawozdanie na potrzeby sprawowania nadzoru, prowadzenia dochodzeń i nakładania sankcji - dokumenty lub dane przekazywane w ramach kontroli.

[17] Obowiązek sprawozdawczy ma zastosowanie tylko do centralnych depozytów papierów wartościowych.

Ze względu na konieczność dalszego przekazywania w postaci cyfrowej sprawozdań przez właściwe organy krajowe do EUN, kluczowe znaczenie będzie miało sprawozdawanie przez podmioty finansowe zgłoszeń dotyczących poważnych incydentów związanych z ICT oraz rejestrów informacji dotyczących umów z zewnętrznymi dostawcami usług ICT.

Sprawozdawanie informacji dotyczących umów z zewnętrznymi dostawcami usług ICT do EUN będzie miało istotne znaczenie w procesie wyznaczania kluczowych zewnętrznych dostawców usług ICT.

Obowiązki sprawozdawcze określone w rozporządzeniu DORA powinny być rozumiane jako wszelkiego rodzaju informacje, dane i sprawozdania związane z realizacją obowiązków wynikających z rozporządzenia DORA oraz aktów wykonawczych.

Zestawienie obowiązków i formularzy sprawozdawczych obejmuje zakres zgodnie z informacją zamieszczoną na stronie https://www.knf.gov.pl/dla_rynku/dora, w sekcji „Sprawozdawczość DORA”[18], a także w przewidzianych do tego systemach teleinformatycznych UKNF, z zastrzeżeniem, że liczba i zakres formularzy sprawozdawczych może ulec zmianie ze względu na brak części aktów wykonawczych do rozporządzenia DORA oraz przepisów krajowych.

Terminy składania poszczególnych sprawozdań mogą wynikać z przepisów prawa, pism okólnych i komunikatów KNF lub UKNF, a także z obowiązków sprawozdawczych nakładanych w drodze decyzji przez EUN (Europejski Urząd Nadzoru Bankowego, Europejski Urząd Nadzoru Giełd i Papierów Wartościowych oraz Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych) na organy właściwe, w tym KNF.

Rozpoczęcie pełnienia przez KNF funkcji właściwego organu w ramach rozporządzenia DORA istotnie zmieni proces sprawozdawczy oraz komunikację, a także wymianę informacji pomiędzy podmiotami finansowymi, organami krajowymi i organami unijnymi.

Zautomatyzowane pozyskiwanie, rejestrowanie, przetwarzanie i analizowanie nowego zakresu danych, które nie były dotychczas wymagane od podmiotów finansowych, uwzględniając znaczne zwiększenie skali pozyskiwanych danych i informacji w stosunku do stanu dotychczasowego, nie będzie możliwe bez odpowiednich systemów i narzędzi IT. Zautomatyzowana analiza danych pozyskiwanych od podmiotów finansowych, wyliczanie odpowiednich wskaźników oraz ich dalsze przetwarzanie będzie niezbędne do wykonywania zadań nadzorczych i przekazywania wybranych informacji do podmiotów finansowych oraz EUN.

Zapewnienie odpowiedniego sposobu wymiany informacji między KNF a podmiotami finansowymi stanowi jeden z kluczowych warunków skutecznego sprawowania nadzoru nad realizowaniem przez podmioty finansowe obowiązków wynikających z rozporządzenia DORA. Przy znacznej liczbie sprawozdawanych danych istotne będzie przekazywanie przez podmioty finansowe określonych i ustrukturyzowanych danych w postaci cyfrowej, a także w odpowiednim formacie. Dzięki temu możliwa będzie ich sprawna analiza dla potrzeb

[18] https://www.knf.gov.pl/dla_rynku/dora/sprawozdawczosc_dora

sprawowanego nadzoru, ale także realizowanie na szczeblu europejskim założeń współpracy właściwych organów krajowych z EUN.

W celu umożliwienia sprawowania nadzoru nad rynkiem finansowym niezbędne będzie korzystanie przez podmioty finansowe z systemów oraz narzędzi teleinformatycznych udostępnionych przez UKNF, tak aby możliwa była realizacja procesu komunikacji, sprawozdawczości oraz analityki danych w sposób zautomatyzowany, ustrukturyzowany, niezawodny, ujednolicony, bezpieczny, a także zgodny z wytycznymi nadzoru europejskiego.

Obowiązki sprawozdawcze powinny być realizowane w postaci elektronicznej z wykorzystaniem kanałów komunikacji, w tym systemów teleinformatycznych i narzędzi teleinformatycznych udostępnionych przez UKNF, takich jak:

1) System Sprawozdawczości DORA;
2) System do zgłaszania poważnych incydentów związanych z ICT;
3) kanał do komunikacji i wymiany informacji w zakresie testów TLPT, uzgodniony z podmiotem finansowym realizującym test.

UKNF udostępnia dodatkowe informacje dotyczące kanałów komunikacji przeznaczonych do przekazywania poszczególnych formularzy sprawozdawczych na stronie https://www.knf.gov.pl/dla_rynku/dora, w sekcji „Sprawozdawczość DORA”[19].

(3) Zgłaszanie poważnych incydentów związanych z ICT oraz znaczących cyberzagrożeń

Zgodnie z rozporządzeniem DORA „incydent związany z ICT"[20] definiuje się jako: „pojedyncze zdarzenie lub seria powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, które zagrażają bezpieczeństwu sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy”.

Natomiast „poważny incydent związany z ICT”[21] to: „incydent związany z ICT o dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne lub istotne funkcje podmiotu finansowego”.

Przepisy rozporządzenia DORA uwzględniają zarówno zdarzenia obejmujące cyberataki, jak i incydenty o charakterze operacyjnym, przez co zdarzenia takie mogą obejmować również awarie systemów oraz inne zakłócenia technologiczne.

Rozporządzenie DORA przewiduje szereg kryteriów w zakresie klasyfikacji poważnych incydentów związanych z ICT, które obejmują:

[19] https://www.knf.gov.pl/dla_rynku/dora/sprawozdawczosc_dora
[20] Zgodnie z art. 3 pkt 8 rozporządzenia DORA.
[21] Zgodnie z art. 3 pkt 10 rozporządzenia DORA.

1) liczbę lub znaczenie klientów lub kontrahentów finansowych oraz (w stosownych przypadkach) kwotę lub liczbę transakcji, których dotyczy incydent związany z ICT, oraz to czy taki incydent spowodował skutki reputacyjne;

2) krytyczność usług, których dotyczy incydent związany z ICT, w tym transakcji i operacji podmiotu finansowego;

3) czas trwania incydentu związanego z ICT, w tym przerwę w świadczeniu usług;

4) utratę danych w wyniku incydentu związanego z ICT w kontekście dostępności, autentyczności, integralności lub poufności danych;

5) skutki gospodarcze incydentu związanego z ICT, w szczególności bezpośrednie oraz pośrednie koszty i straty;

6) zasięg geograficzny incydentu związanego z ICT, w szczególności, jeżeli dotyczy on więcej niż dwóch państw członkowskich.

Dodatkowo w art. 18 ust. 3 lit. a rozporządzenia DORA przewidziano, że doprecyzowanie wymienionych kryteriów, w tym określenie progów istotności w celu ustalania poważnych incydentów związanych z ICT, następuje w drodze wydania regulacyjnych standardów technicznych, jako aktu wykonawczego do rozporządzenia DORA[22]. Zatem klasyfikacja incydentów związanych z ICT, a w szczególności ocena wystąpienia poważnego incydentu związanego z ICT, powinna następować w oparciu o treść definicji „poważnego incydentu związanego z ICT" oraz zastosowanie kryteriów klasyfikacji i progów istotności sprecyzowanych w ramach regulacyjnych standardów technicznych.

Rozporządzenie DORA przewiduje wyłączenie obowiązku zgłaszania incydentów zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/2366 (dyrektywa PSD2) w stosunku do dostawców usług płatniczych objętych zakresem stosowania rozporządzenia DORA.

Oznacza to, że podmioty nadzorowane, objęte do tej pory wymogiem raportowania incydentów na podstawie dyrektywy PSD2, będą zobowiązane do zgłaszania poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami zgodnie z rozporządzeniem DORA. Ma to na celu zmniejszenie obciążenia administracyjnego i wyeliminowanie powielających się obowiązków w zakresie zgłaszania incydentów w przypadku niektórych podmiotów finansowych (prowadzących działalność w zakresie usług płatniczych).

Z tym rozwiązaniem skorelowane są także zmiany dyrektywy PSD2 dokonane w ramach dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2556 z dnia 14 grudnia 2022 r. w sprawie zmiany dyrektyw 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE,

[22] Rozporządzenie delegowane Komisji (UE) 2024/1772 z dnia 13 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria klasyfikacji incydentów związanych z ICT i cyberzagrożeń, progi istotności i szczegółowe informacje dotyczące zgłaszania poważnych incydentów.

2014/59/UE, 2014/65/UE, (UE) 2015/2366 oraz (UE) 2016/2341 w odniesieniu do operacyjnej odporności cyfrowej sektora finansowego.

Operatorzy usług kluczowych, do czasu uchwalenia przepisów implementujących dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 (dyrektywa NIS2), powinni równolegle, niezależnie od zgłaszania poważnych incydentów związanych z ICT zgodnie z rozporządzeniem DORA, przekazywać zgłoszenia incydentów poważnych w sposób przewidziany w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Przekazywanie zgłoszeń dotyczących incydentów jest kluczowe dla długofalowego procesu budowania bezpieczeństwa i odporności na cyberataki, szczególnie w sektorze finansowym. Dzięki temu możliwe jest szybkie podjęcie działań, co często może pomóc w minimalizacji negatywnych skutków zdarzenia dla danej organizacji oraz jej klientów. Informacje o incydentach pozwalają także na analizę przyczyn i wzorców zagrożeń, co przyczynia się do budowania lepszych strategii ochrony w przyszłości oraz daje możliwość prewencyjnego zabezpieczenia instytucji potencjalnie narażonych na taki sam lub podobny atak.

(4) Prowadzenie i przekazanie rejestru informacji dotyczącego umów z zewnętrznymi dostawcami usług ICT

Prowadzenie rejestru informacji w odniesieniu do wszystkich ustaleń umownych dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT, o którym mowa w art. 28 ust. 3 rozporządzenia DORA, pozostaje jednym z istotnych obowiązków ciążących na podmiotach finansowych na mocy omawianego rozporządzenia.

W kontekście przekazywania rejestru informacji do właściwego organu istotne znaczenie ma opublikowana 15 listopada 2024 roku wspólna decyzja EUN dotycząca raportowania przez właściwe organy do EUN informacji niezbędnych do wyznaczania kluczowych zewnętrznych dostawców usług ICT[23].

Z powyższej decyzji wynika m.in., że właściwe organy będą zobowiązane pozyskać od podmiotów finansowych rejestry informacji w terminie umożliwiającym przekazanie zebranych danych do EUN przed 30 kwietnia 2025 roku. W związku z powyższym KNF planuje zwrócić się na początku kwietnia 2025 roku, w oparciu o art. 28 ust. 3 akapit czwarty rozporządzenia DORA, do podmiotów finansowych z żądaniem przekazania rejestrów informacji do KNF, tak aby KNF mogła terminowo zrealizować obowiązek przekazania zebranych rejestrów informacji do EUN. Na planowany termin na przekazanie rejestru informacji do KNF w 2025 roku będzie miała również wpływ okoliczność, że KNF dokonywać będzie walidacji danych przedkładanych w ramach rejestrów informacji oraz wzywać będzie podmioty finansowe do niezwłocznego uzupełnienia ewentualnych brakujących danych bądź poprawy błędów. We wskazanej powyżej decyzji podkreślono również, że przekazywane w 2025 roku do właściwych organów rejestry informacji powinny zawierać dane aktualne na 31 marca 2025 roku.

[23] https://www.eba.europa.eu/publications-and-media/press-releases/esas-announce-timeline-collect-information-designation-critical-ict-third-party-service-providers

Należy także podkreślić, że 3 grudnia 2024 roku opublikowane zostało rozporządzenie wykonawcze Komisji (UE) 2024/2956 z dnia 29 listopada 2024 r. ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych wzorów na potrzeby rejestru informacji. Ma ono kluczowe znaczenie z perspektywy obowiązków związanych z prowadzeniem rejestru informacji, gdyż precyzuje, jakie dane powinny się w nim znaleźć, a w konsekwencji, jakie informacje będą przekazywane w tym zakresie do właściwego organu.

Uchylenie lub odwołanie dotychczasowych aktów o charakterze tzw. *soft law*

W związku z rozpoczęciem stosowania przepisów rozporządzenia DORA planowane jest uchylenie rekomendacji i wytycznych KNF dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, mających zastosowanie do podmiotów finansowych objętych wymogami rozporządzenia DORA.

Planowane jest uchylenie:

1) Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach;
2) Rekomendacji D-SKOK dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych;
3) Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji;
4) Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych;
5) Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych;
6) Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w podmiotach infrastruktury rynku kapitałowego.

Podobne analizy zbieżności zakresu przedmiotowego wytycznych w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT oraz wytycznych w sprawie outsourcingu do dostawców usług w chmurze obliczeniowej z rozporządzeniem DORA przeprowadzane są przez EUN.

Planowane jest również odwołanie komunikatu UKNF dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej (Komunikatu chmurowego).

Pozwoli to uniknąć wątpliwości interpretacyjnych, które mogłyby wystąpić w związku z rozpoczęciem stosowania przepisów rozporządzenia DORA i spodziewanym uchwaleniem przepisów prawa krajowego oraz jednoczesnym obowiązywaniem dotychczasowych regulacji o charakterze tzw. *soft law*.

Mając na uwadze przybliżenie tematyki związanej z rozporządzeniem DORA, UKNF publikuje na stronie https://www.knf.gov.pl/dla_rynku/dora materiały informacyjne i edukacyjne dotyczące rozporządzenia DORA.