Rozporządzenie DORA i Wymogi Komisji Nadzoru Finansowego w Polsce

1. Streszczenie

Rozporządzenie o Operacyjnej Odporności Cyfrowej (Digital Operational Resilience Act – DORA) to unijne rozporządzenie mające na celu wzmocnienie zdolności podmiotów finansowych do zapobiegania, minimalizowania i odzyskiwania sprawności po zakłóceniach w gospodarce cyfrowej. Rozporządzenie to jest bezpośrednio stosowane we wszystkich państwach członkowskich Unii Europejskiej, w tym w Polsce. Komisja Nadzoru Finansowego (KNF) pełni rolę głównego organu nadzorczego odpowiedzialnego za monitorowanie zgodności

z DORA w polskim sektorze finansowym. KNF nadzoruje wdrażanie i egzekwowanie wymagań DORA w odniesieniu do polskich podmiotów finansowych. DORA opiera się na pięciu kluczowych filarach, które mają zasadnicze znaczenie dla budowania operacyjnej odporności cyfrowej. Celem niniejszego raportu jest przedstawienie polskim podmiotom finansowym wytycznych dotyczących zgodności z rozporządzeniem DORA pod nadzorem KNF.

2. Rozumienie Rozporządzenia o Operacyjnej Odporności Cyfrowej (DORA)

2.1. Geneza i Cele DORA w Unijnym Krajobrazie Regulacyjnym

Rozporządzenie DORA ma na celu zwiększenie zdolności podmiotów finansowych do przeciwdziałania, minimalizowania i przywracania działalności w obliczu współczesnych zagrożeń dla gospodarki cyfrowej. Geneza DORA wiąże się z rosnącą częstotliwością i złożonością cyberataków wymierzonych w instytucje finansowe. W obliczu coraz bardziej wyrafinowanych metod wykorzystywania luk w zabezpieczeniach przez cyberprzestępców, znacznie wzrosło ryzyko zakłóceń na dużą skalę. Dostrzegając kluczowe znaczenie operacyjnej odporności dla utrzymania stabilności finansowej, Komisja Europejska zaproponowała DORA jako część swojej Strategii Cyfrowych Finansów. Ta inicjatywa legislacyjna ma na celu stworzenie jednolitego, standardowego i spójnego podejścia do odporności cyfrowej we wszystkich państwach członkowskich UE. Głównym celem DORA jest harmonizacja przepisów dotyczących odporności operacyjnej w sektorze finansowym we wszystkich krajach członkowskich UE. Rozporządzenie to wypełnia lukę w dotychczasowych regulacjach, koncentrując się na ryzykach związanych z technologiami informacyjno-komunikacyjnymi (ICT) oraz na odporności operacyjnej, wykraczając poza tradycyjne podejście oparte na alokacji kapitału.

2.2. Kluczowe Filary DORA

DORA opiera się na pięciu kluczowych filarach, które razem tworzą kompleksową strukturę mającą na celu wzmocnienie cyfrowej odporności operacyjnej:

- **Zarządzanie ryzykiem ICT i ład korporacyjny:** Ten filar wymaga od podmiotów finansowych ustanowienia solidnych i elastycznych ram zarządzania ryzykiem ICT, które obejmują strategie, polityki i procedury mające na celu identyfikację, ocenę, monitorowanie i zarządzanie ryzykiem związanym z ICT.
- **Zarządzanie incydentami związanymi z ICT, ich klasyfikacja i raportowanie:** Podmioty finansowe są zobowiązane do wdrożenia procesów monitorowania, zarządzania i raportowania incydentów związanych z ICT, w tym cyberataków. Wymagane jest terminowe zgłaszanie poważnych incydentów do właściwych organów nadzorczych.
- **Testowanie odporności operacyjnej cyfrowej:** Ten filar nakłada na podmioty finansowe obowiązek regularnego testowania ich systemów ICT w celu oceny ich odporności na różnego rodzaju zakłócenia i zagrożenia, w tym przeprowadzania zaawansowanych testów penetracyjnych opartych na analizie zagrożeń (TLPT) dla wybranych podmiotów.
- **Zarządzanie ryzykiem ICT stron trzecich:** W związku z rosnącą zależnością od zewnętrznych dostawców usług ICT, DORA wprowadza zasady zarządzania ryzykiem związanym z tymi podmiotami, w tym wymagania dotyczące należytej staranności, umów oraz monitorowania.
- **Ustalenia dotyczące wymiany informacji:** DORA zachęca do wymiany informacji i danych wywiadowczych na temat cyberzagrożeń między podmiotami finansowymi w celu zwiększenia ogólnej odporności sektora finansowego.

2.3. Zakres Zastosowania

DORA ma szeroki zakres zastosowania i obejmuje różnorodne podmioty finansowe działające na terenie Unii Europejskiej. Przykłady takich podmiotów to instytucje kredytowe, instytucje płatnicze, firmy inwestycyjne, zakłady ubezpieczeń i reasekuracji oraz dostawcy usług w

zakresie kryptoaktywów. Ponadto, DORA ma zastosowanie również do krytycznych dostawców usług ICT trzecich stron (TPP). Należy zauważyć, że zasada proporcjonalności (Artykuł 4) przewiduje pewne wyjątki i uproszczone wdrożenie dla mniejszych przedsiębiorstw.

2.4. Kluczowe Definicje i Ich Implikacje

Zrozumienie kluczowych definicji zawartych w DORA jest niezbędne do prawidłowej interpretacji i wdrożenia jego wymagań. "Cyfrowa odporność operacyjna" oznacza zdolność podmiotu finansowego do budowania, zapewniania i przeglądu swojej integralności i niezawodności operacyjnej. "Ryzyko ICT" obejmuje wszelkie racjonalnie identyfikowalne okoliczności związane z wykorzystaniem sieci i systemów informacyjnych, które, jeśli się zmaterializują, mogą naruszyć bezpieczeństwo tych systemów. "Incydent związany z ICT" to pojedyncze zdarzenie lub seria powiązanych zdarzeń, nieplanowanych przez podmiot finansowy, które naruszają bezpieczeństwo sieci i systemów informacyjnych. "Poważny incydent związany z ICT" to incydent, który ma wysoki negatywny wpływ na sieci i systemy informacyjne wspierające krytyczne lub ważne funkcje podmiotu finansowego. "Znaczące cyberzagrożenie" to cyberzagrożenie, którego charakterystyka techniczna wskazuje, że może potencjalnie doprowadzić do poważnego incydentu związanego z ICT. "Dostawca usług ICT trzeciej strony" to przedsiębiorstwo świadczące usługi ICT. Dokładne definicje tych i innych kluczowych terminów, zawarte w Artykule 3 DORA, mają kluczowe znaczenie dla określenia zakresu obowiązków podmiotów finansowych i dostawców ICT. Na przykład, definicja "krytycznej lub ważnej funkcji" jest kluczowa dla zarządzania ryzykiem związanym z usługami świadczonymi przez strony trzecie.

3. Rola Komisji Nadzoru Finansowego (KNF) w Nadzorze nad DORA

3.1. KNF jako Wyznaczony Organ Właściwy dla DORA w Polsce

Komisja Nadzoru Finansowego (KNF) jest głównym organem odpowiedzialnym za nadzorowanie wdrożenia i egzekwowania rozporządzenia DORA w Polsce. KNF aktywnie przygotowuje się do swojej roli nadzorczej od pierwszego dnia obowiązywania DORA, tj. od 17 stycznia 2025 roku. To proaktywne podejście KNF świadczy o jej zaangażowaniu w zapewnienie zgodności od samego początku, nawet w sytuacji, gdy krajowe przepisy transponujące DORA nie zostały jeszcze w pełni wdrożone.

3.2. Uprawnienia Nadzorcze i Mechanizmy Egzekwowania Dostępne KNF

KNF dysponuje szerokimi uprawnieniami do nadzorowania i egzekwowania DORA, w tym prawem dostępu do dokumentów i danych, przeprowadzania inspekcji na miejscu oraz żądania wyjaśnień. KNF ma również uprawnienia do nakładania środków naprawczych, takich jak nakazanie zaprzestania działań niezgodnych z przepisami. Ponadto, KNF może nakładać kary finansowe za nieprzestrzeganie DORA. Warto również zauważyć, że KNF ma możliwość publicznego informowania o przypadkach nieprzestrzegania przepisów. Te znaczące uprawnienia KNF mają na celu zapewnienie przestrzegania DORA, a podmioty finansowe powinny być świadome potencjalnych konsekwencji braku zgodności.

3.3. Strategiczne Priorytety KNF w Zakresie Cyfrowej Odporności Operacyjnej

KNF uwzględniła skuteczne nadzorowanie ryzyka ICT w swoich priorytetach nadzorczych na rok 2025. Podkreśla to znaczenie, jakie KNF przywiązuje do zapewnienia stabilności unijnego systemu finansowego i bezpieczniejszego korzystania z usług cyfrowych. KNF zwraca również uwagę na kluczową rolę ICT w prawidłowym funkcjonowaniu rynku finansowego. Strategiczne podejście KNF odzwierciedla priorytetowe znaczenie, jakie organ nadzoru przypisuje cyfrowej odporności operacyjnej jako integralnemu elementowi stabilności finansowej.

4. Szczegółowe Wymogi i Oczekiwania KNF w Zakresie DORA

4.1. Analiza Oficjalnych Stanowisk i Opinii KNF dotyczących Wdrożenia DORA

KNF wydała oficjalne oświadczenia dotyczące bezpośredniego stosowania DORA od 17

stycznia 2025 roku, niezależnie od opóźnień w krajowej legislacji. KNF wyraźnie oczekuje, że podmioty finansowe będą gotowe do stosowania DORA od pierwszego dnia. Ponadto, KNF wymaga spełnienia warunków określonych w oświadczeniu Europejskich Urzędów Nadzoru (ESA) dotyczącym stosowania DORA. Stanowisko KNF podkreśla natychmiastowy i nieunikniony charakter obowiązku zgodności z DORA, co skłania podmioty finansowe do priorytetowego traktowania swojej gotowości.

4.2. Obowiązki Związane ze Zgłaszaniem KNF Poważnych Incydentów Związanych z ICT i Znaczących Cyberzagrożeń

KNF aktywnie przygotowuje się do przyjmowania zgłoszeń na podstawie DORA poprzez dedykowane systemy informatyczne. Obowiązki sprawozdawcze będą realizowane elektronicznie za pomocą systemów wskazanych przez KNF. KNF oczekuje otrzymywania wstępnych powiadomień, raportów śródokresowych i raportów końcowych dotyczących poważnych incydentów związanych z ICT. Istnieje również możliwość dobrowolnego zgłaszania KNF znaczących cyberzagrożeń. KNF stworzyła specjalne elektroniczne kanały do zgłaszania incydentów, co podkreśla potrzebę terminowego i wyczerpującego przekazywania informacji.

4.3. Wymogi Dotyczące Prowadzenia i Przekazywania KNF Rejestru Informacji o Ustaleniach Umownych z Dostawcami Usług ICT Trzecich Stron

Podmioty finansowe są zobowiązane do prowadzenia kompleksowego rejestru ustaleń umownych z dostawcami usług ICT trzecich stron (TPP). Właściwe organy muszą przekazać te rejestry do ESA do 30 kwietnia 2025 roku. KNF planuje zażądać przekazania tych rejestrów na początku kwietnia 2025 roku, z danymi aktualnymi na dzień 31 marca 2025 roku. Rejestry te służą do wewnętrznego monitorowania, nadzoru i wyznaczania krytycznych dostawców usług ICT TPP. KNF przywiązuje dużą wagę do rejestru informacji jako kluczowego narzędzia do zarządzania ryzykiem związanym z usługami świadczonymi przez strony trzecie oraz do wkładu w ogólnounijną strukturę nadzoru.

4.4. Stanowisko KNF w Sprawie Stosowania Zasady Proporcjonalności

KNF weryfikuje stosowanie zasady proporcjonalności przez podmioty finansowe podczas przeglądu spójności ram zarządzania ryzykiem ICT. KNF bierze pod uwagę wielkość, profil ryzyka oraz złożoność działalności poszczególnych podmiotów finansowych. Chociaż DORA jest jednolitym rozporządzeniem, KNF będzie nadzorować jego stosowanie w sposób uwzględniający specyfikę każdego podmiotu finansowego.

4.5. Systemy Sprawozdawcze i Kanały Komunikacji Utworzone przez KNF dla Zgodności z DORA

KNF utworzyła "System Sprawozdawczości DORA" do wymiany formularzy sprawozdawczych i komunikacji. Dostępny jest również "System do Obsługi Incydentów DORA" do zgłaszania poważnych incydentów związanych z ICT i znaczących cyberzagrożeń. Ponadto, dla zapytań dotyczących DORA udostępniono dedykowany adres e-mail (konsultacje.dora@knf.gov.pl) oraz infolinię. KNF wdrożyła specjalne systemy i kanały w celu ułatwienia komunikacji i raportowania na podstawie DORA, kładąc nacisk na elektroniczne składanie dokumentów.

5. Wpływ DORA na Istniejące Wytyczne i Regulacje KNF

5.1. Związek Między DORA a Poprzednimi Rekomendacjami KNF (np. Rekomendacja D)

DORA i jej Regulacyjne Standardy Techniczne (RTS) zastąpiły dotychczasowe regulacje sektorowe. KNF planuje uchylić regulacje sektorowe, w tym znaną "Rekomendację D" dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach. KNF podjęła już kroki w celu uchylenia tych rekomendacji. DORA oznacza przejście do jednolitego unijnego frameworka, co prowadzi do dezaktualizacji niektórych dotychczasowych krajowych wytycznych. Podmioty finansowe powinny priorytetowo traktować wymagania DORA w stosunku do zastąpionych rekomendacji krajowych.

5.2. Wycofanie Komunikatu KNF w Sprawie Przetwarzania Informacji w Chmurze Obliczeniowej i Jego Implikacje w Kontekście DORA

KNF wycofała swój Komunikat dotyczący przetwarzania informacji w chmurze obliczeniowej (Komunikat chmurowy) z dniem 17 stycznia 2025 roku. Wycofanie to wynika z pokrywania się zakresu tematycznego z DORA i jej aktami wykonawczymi. Podmioty, które wcześniej podlegały Komunikatowi chmurowemu, ale nie są objęte zakresem DORA, są teraz zwolnione z tych wymagań. Należy zauważyć, że zastosowanie DORA nie ogranicza się do usług chmurowych i obejmuje również chmury prywatne. Wycofanie Komunikatu chmurowego wskazuje, że przepisy DORA dotyczące zarządzania ryzykiem ICT, w tym outsourcingu, stanowią obecnie podstawową ramę regulacyjną dla korzystania z chmury w sektorze finansowym.

5.3. Dostosowanie Krajowych Regulacji do Wymagań DORA

Polska jest w trakcie dostosowywania swojego ustawodawstwa krajowego do DORA. Opublikowano projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego, wdrażający do prawa krajowego rozporządzenie DORA oraz towarzyszącą mu dyrektywę. Projekt ten wyznacza KNF jako organ właściwy oraz określa jej uprawnienia nadzorcze i potencjalne kary. Należy podkreślić, że pomimo braku w pełni wdrożonego ustawodawstwa krajowego, DORA jest bezpośrednio stosowana. Trwające prace legislacyjne w Polsce mają na celu dalsze umocnienie roli KNF i ustanowienie krajowych ram dla egzekwowania przepisów i nakładania kar.

6. Harmonogram i Wdrożenie DORA w Polsce

6.1. Kluczowe Daty Wejścia w Życie i Stosowania DORA

DORA weszła w życie 16 stycznia 2023 roku. Rozporządzenie zacznie być stosowane od 17 stycznia 2025 roku. Dwuroczny okres przejściowy umożliwił podmiotom finansowym przygotowanie się do wdrożenia wymagań DORA.

6.2. Oczekiwania KNF dotyczące Gotowości Podmiotów Finansowych do 17 Stycznia 2025 Roku

KNF wyraźnie oczekuje pełnej gotowości do daty rozpoczęcia stosowania rozporządzenia. KNF podkreśla, że opóźnienia w krajowej legislacji nie stanowią usprawiedliwienia dla braku zgodności. Stanowcze stanowisko KNF wskazuje na obowiązkowe stosowanie DORA od określonej daty.

6.3. Terminy Pierwszych Zgłoszeń i Przekazania Rejestru Informacji do KNF

Pierwsze obowiązki sprawozdawcze na podstawie DORA rozpoczęły się 17 stycznia 2025 roku. Termin przekazania przez KNF rejestru informacji do ESA upływa 30 kwietnia 2025 roku. KNF przewiduje, że zażąda od podmiotów finansowych przekazania rejestrów na początku kwietnia 2025 roku, z danymi aktualnymi na dzień 31 marca 2025 roku. Te konkretne terminy podkreślają natychmiastowe działania, jakie muszą podjąć podmioty finansowe w Polsce, aby spełnić swoje obowiązki wynikające z DORA pod nadzorem KNF.

Tabela 1 przedstawia kluczowe daty wdrożenia DORA w Polsce:

Kluczowy Kamień Milowy	**Data**
Wejście w życie DORA	16 stycznia 2023
Rozpoczęcie stosowania DORA	17 stycznia 2025
Termin przekazania Rejestru Informacji przez KNF do ESA	30 kwietnia 2025

Oczekiwane żądanie KNF dotyczące przekazania Rejestru Informacji	Początek kwietnia 2025
Rozpoczęcie pierwszych obowiązków sprawozdawczych	17 stycznia 2025

7. Wyzwania i Zagadnienia dla Podmiotów Finansowych w Polsce

7.1. Nawigowanie po Złożoności Wymagań Zgodności z DORA

Szeroki zakres i szczegółowe wymagania DORA mogą stanowić wyzwanie dla podmiotów finansowych. Wymagana jest holistyczna strategia cyberbezpieczeństwa i odporności operacyjnej. Ogrom wymagań DORA i ich wzajemne powiązania sprawiają, że konieczne jest strategiczne i dobrze skoordynowane podejście do zapewnienia zgodności.

7.2. Adresowanie Ryzyka Koncentracji ICT i Zależności od Stron Trzecich

Szczególny nacisk kładziony jest na zarządzanie ryzykiem związanym z poleganiem na ograniczonej liczbie dostawców usług ICT trzecich stron (ryzyko koncentracji ICT). Wymagana jest dogłębna należyta staranność, solidne umowy i monitorowanie dostawców zewnętrznych. Niezbędne jest również posiadanie strategii wyjścia i planów awaryjnych dla krytycznych usług świadczonych przez strony trzecie. Rosnąca zależność sektora finansowego od zewnętrznych dostawców technologii sprawia, że zarządzanie ryzykiem związanym z tymi podmiotami jest kluczowym elementem DORA. Podmioty finansowe muszą zapewnić, że ich dostawcy spełniają rygorystyczne standardy.

7.3. Wdrożenie Solidnych Programów Testowania Odporności Operacyjnej Cyfrowej

Konieczne jest regularne testowanie systemów ICT, od podstawowych ocen podatności po zaawansowane testy penetracyjne oparte na analizie zagrożeń (TLPT) dla znaczących podmiotów. Wymagane jest również testowanie planów ciągłości działania i odzyskiwania po awarii. Wyniki testów należy raportować właściwym organom. DORA nakłada obowiązek proaktywnego i rygorystycznego testowania cyfrowej odporności w celu identyfikacji luk w zabezpieczeniach i zapewnienia zdolności do przeciwdziałania zakłóceniom.

7.4. Zapewnienie Skutecznej Komunikacji i Raportowania Incydentów do KNF

Istotne jest ustanowienie jasnych planów komunikacji dla interesariuszy wewnętrznych i zewnętrznych podczas incydentów związanych z ICT. Istnieją szczegółowe terminy i wymagania informacyjne dotyczące zgłaszania poważnych incydentów do KNF. KNF ustanowiła specjalne systemy do zgłaszania incydentów. Jasna i terminowa komunikacja z KNF podczas i po incydentach związanych z ICT ma kluczowe znaczenie dla zgodności z przepisami i skutecznego nadzoru.

8. Kary i Konsekwencje Braku Zgodności Egzekwowane przez KNF

8.1. Przegląd Potencjalnych Kar Finansowych i Sankcji za Niespełnienie Wymagań DORA

KNF ma uprawnienia do nakładania znaczących kar finansowych za nieprzestrzeganie DORA. Kary mogą wynosić do 2% całkowitego rocznego światowego obrotu dla podmiotów finansowych i do 5 milionów euro dla krytycznych dostawców usług ICT TPP. Istnieje również możliwość nakładania kar na osoby fizyczne, takie jak członkowie zarządu. Potencjalne kary finansowe za brak zgodności z DORA są znaczne, co podkreśla wagę przestrzegania przepisów.

8.2. Uprawnienia KNF do Nakładania Środków Naprawczych i Publicznego Informowania o Braku Zgodności

KNF może nakazać zaprzestanie działań niezgodnych z przepisami i zażądać naprawienia uchybień. KNF ma również prawo do wydawania publicznych oświadczeń identyfikujących podmioty nieprzestrzegające przepisów. Oprócz kar finansowych, KNF może podjąć bezpośrednie działania w celu skorygowania braku zgodności, a także może publicznie

informować o naruszeniach, co prowadzi do szkód reputacyjnych.

8.3. Ryzyko Finansowe, Prawne i Reputacyjne Związane z Brakiem Zgodności

Brak zgodności z DORA wiąże się z poważnym ryzykiem, które wykracza poza kary finansowe. Obejmuje potencjalne wyzwania prawne oraz szkody w reputacji i zaufaniu klientów. Brak zgodności z DORA niesie ze sobą znaczące ryzyko, które wykracza poza kary finansowe, potencjalnie wpływając na długoterminową rentowność i reputację podmiotów finansowych. Tabela 2 przedstawia potencjalne kary za brak zgodności z DORA w Polsce:

Rodzaj Podmiotu	Rodzaj Naruszenia	Potencjalna Kara
Podmiot Finansowy	Różne naruszenia	Do 2% rocznego światowego obrotu lub określona kwota w PLN (projekt ustawy wdrażającej przewiduje do 20 869 500 PLN lub 10% rocznego przychodu)
Krytyczny Dostawca Usług ICT Trzeciej Strony	Różne naruszenia	Do 5 000 000 EUR lub 1% średniego dziennego światowego obrotu
Osoby Fizyczne (np. członkowie zarządu)	Różne naruszenia	Do 5 000 000 EUR lub określona kwota w PLN (projekt ustawy wdrażającej przewiduje do 3 042 410 PLN)

9. Wnioski i Rekomendacje

9.1. Podsumowanie Kluczowych Obowiązków Podmiotów Finansowych w Polsce w Kontekście DORA i Nadzoru KNF

Podmioty finansowe w Polsce, podlegające nadzorowi KNF, mają kluczowe obowiązki w zakresie pięciu filarów DORA. Muszą ustanowić i utrzymywać solidne ramy zarządzania ryzykiem ICT, wdrożyć efektywne procesy zarządzania incydentami i raportowania, regularnie testować swoją odporność operacyjną cyfrową, zarządzać ryzykiem związanym z usługami świadczonymi przez strony trzecie oraz uczestniczyć w wymianie informacji o cyberzagrożeniach. Niezbędne jest przestrzeganie szczegółowych wymagań KNF dotyczących raportowania i terminów.

9.2. Strategiczne Rekomendacje dotyczące Osiągnięcia i Utrzymania Zgodności

Zaleca się, aby podmioty finansowe przeprowadziły dogłębną analizę luk w celu oceny swojego aktualnego poziomu zgodności z DORA. Należy opracować kompleksowy plan wdrożenia z jasnymi harmonogramami i podziałem odpowiedzialności. Priorytetem powinno być ustanowienie solidnych ram zarządzania ryzykiem ICT, procesów raportowania incydentów oraz programów testowania odporności. Należy również starannie zarządzać dostawcami usług ICT trzecich stron, w tym przeprowadzać należytą staranność i stosować zabezpieczenia umowne. Warto rozważyć nawiązanie współpracy w zakresie wymiany informacji w zaufanych społecznościach. Należy utrzymywać otwartą komunikację z KNF i korzystać z udostępnionych systemów sprawozdawczych. Kluczowe jest również ciągłe monitorowanie i dostosowywanie się do ewoluujących zagrożeń i oczekiwań regulacyjnych.

Tabela 3 przedstawia kluczowe obowiązki sprawozdawcze wobec KNF na podstawie DORA:

Rodzaj Raportu	Opis	System/Kanał Przekazania
Wstępne powiadomienie o poważnym incydencie ICT	Pierwsza informacja o incydencie	System do Obsługi Incydentów DORA (https://csirt.knf.gov.pl) lub e-mail (incydenty.dora@knf.gov.pl)
Raport śródokresowy o poważnym incydencie ICT	Aktualizacja statusu incydentu	System do Obsługi Incydentów DORA (https://csirt.knf.gov.pl)
Raport końcowy o poważnym incydencie ICT	Raport po analizie przyczyn incydentu	System do Obsługi Incydentów DORA (https://csirt.knf.gov.pl)
Dobrowolne powiadomienie o znaczącym cyberzagrożeniu	Informacja o potencjalnym zagrożeniu	System do Obsługi Incydentów DORA (https://csirt.knf.gov.pl) lub e-mail (incydenty.dora@knf.gov.pl)
Rejestr Informacji o Ustaleniach Umownych z Dostawcami Usług ICT Trzecich Stron	Szczegółowe informacje o umowach z dostawcami ICT	System Sprawozdawczości DORA (https://crp.knf.gov.pl)

W Dzienniku Urzędowym Unii Europejskiej opublikowano akty wykonawcze dotyczące Rozporządzenia DORA:

- Rozporządzenie delegowane Komisji (UE) 2024/1502 z dnia 22 lutego 2024 r., uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie określenia kryteriów wyznaczania zewnętrznych dostawców usług ICT jako kluczowych dla podmiotów finansowych: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1502&qid=1720433556083
- Rozporządzenie delegowane Komisji (UE) 2024/1505 z dnia 22 lutego 2024 r., uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie określenia wysokości opłat nadzorczych pobieranych przez wiodący organ nadzorczy od kluczowych zewnętrznych dostawców usług ICT oraz sposobu ich uiszczania: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1505&qid=1720433556083
- 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 precyzujących kryteria klasyfikacji incydentów związanych z ICT i cyberzagrożeń, progi istotności oraz szczegółowe informacje dotyczące zgłaszania poważnych incydentów: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1772&qid=1720

433556083

- Rozporządzenie delegowane Komisji (UE) 2024/1773 z dnia 13 marca 2024 r., uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych doprecyzowujących szczegółową treść polityki dotyczącej ustaleń umownych w sprawie korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1773&qid=1720433556083
- Rozporządzenie delegowane Komisji (UE) 2024/1774 z dnia 13 marca 2024 r., uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT oraz uproszczone ramy zarządzania tym ryzykiem: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1774&qid=1720433556083
- Rozporządzenie delegowane Komisji (UE) 2025/301 z dnia 23 października 2024 r., uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających treść i terminy przedłożenia wstępnego powiadomienia, sprawozdania śródokresowego i sprawozdania końcowego dotyczących poważnych incydentów związanych z ICT, a także treść dobrowolnego powiadomienia o znaczących cyberzagrożeniach: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L_202500301
- Rozporządzenie wykonawcze Komisji (UE) 2025/302 z dnia 23 października 2024 r., ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych formularzy, wzorów i procedur stosowanych przez podmioty finansowe do zgłaszania poważnych incydentów związanych z ICT i powiadamiania o znaczących cyberzagrożeniach: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L_202500302
- Rozporządzenie delegowane Komisji (UE) 2025/295 z dnia 24 października 2024 r., uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych dotyczących harmonizacji warunków umożliwiających prowadzenie działań nadzorczych: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0295
- 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: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:L_202402956&qid=1733386591974

Niezależnie od opublikowania aktów wykonawczych do Rozporządzenia DORA w Dzienniku

Urzędowym Unii Europejskiej, na stronach Europejskich Urzędów Nadzoru udostępniono wytyczne powiązane z tym Rozporządzeniem:

- Wspólne wytyczne dotyczące współpracy w zakresie nadzoru i wymiany informacji między Europejskimi Urzędami Nadzoru a właściwymi organami na podstawie rozporządzenia (UE) 2022/2554 z dnia 6 listopada 2024 roku (JC/GL/2024/36): https://www.esma.europa.eu/sites/default/files/2024-11/JC-GL-2024-36_Guidelines_on_DORA_oversight_cooperation_PL.pdf

Opublikowane akty wykonawcze, jak również wytyczne i inne materiały, stanowią uzupełnienie przepisów Rozporządzenia DORA i mają istotne znaczenie dla dostosowania działalności podmiotów finansowych do jego wymogów. W celu przybliżenia tematyki związanej z Rozporządzeniem DORA, na tej stronie będą publikowane materiały informacyjne i edukacyjne.

W przypadku pytań i zainteresowania wdrożeniem DORA prosimy o kontakt:

- na adres email: hello@elitecorp.pl
- na numer telefonu: +48 533 755 054