



NR 3/2025. STAN NA DZIEŃ 10 MARCA 2025 r.

BIULETYN PRAWNY

ZMIANY PRAWNE NA RYNKU FUNDUSZY

BIULETYN PRAWNY

I. Akty prawne dotyczące rynku Funduszy

1. Prawo krajowe

- 1.1. Ustawa z dnia 9 stycznia 2025 r. o zmianie ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, ustawy o Krajowej Administracji Skarbowej oraz ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu;
- 1.2. Rozporządzenie Ministra Finansów z dnia 25 lutego 2025 r. zmieniające rozporządzenie w sprawie szczegółowych zasad sporządzania przez jednostki inne niż banki, zakłady ubezpieczeń i zakłady reasekuracji skonsolidowanych sprawozdań finansowych grup kapitałowych.

2. Projekty ustaw/rozporządzeń

- 2.1. Projekt ustawy z dnia 10 lutego 2025 r. o systemach sztucznej inteligencji;
- 2.2. Projekt ustawy z dnia 10 stycznia 2025 r. o ogólnym bezpieczeństwie produktów;
- 2.3. Projekt ustawy z dnia 27 lutego 2025 r. o uchyleniu ustawy o Centralnej Informacji Emerytalnej;
- 2.4. Projekt ustawy z dnia 13 grudnia 2024 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw;
- 2.5. Projekt ustawy z dnia 5 lutego 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji;
- 2.6. Projekt ustawy z dnia 31 stycznia 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa;
- 2.7. Projekt ustawy z dnia 10 stycznia 2025 r. o rynku kryptoaktywów;

3. Komunikaty, wydarzenia i stanowiska organów nadzoru

- 3.1. Działalność nadzorcza Komisji Nadzoru Finansowego:
 - 3.1.1. Biuletyn Kwartalny. Rynek OFE 4/2024;
 - 3.1.2. Informacje o rynku IKZE według stanu na 31 grudnia 2024 roku;

3.1.3. Informacje o rynku IKE według stanu na 31 grudnia 2024 roku;

3.1.4. Dane kwartalne TFI - IV kwartał 2024 roku;

3.2. PFR Portal PPK: Biuletyn miesięczny Pracowniczych Planów Kapitałowych - nr 40 lutego 2025;

3.3. Stanowisko UKNF dot. stosowania Rozporządzenia DORA przez TFI oraz zarządzających ASI;

II. Obszar zmian

1. Prawo krajowe. Nowe przepisy wchodzące w życie.

1.1. Ustawa z dnia 9 stycznia 2025 r. o zmianie ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, ustawy o Krajowej Administracji Skarbowej oraz ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

Status: Weszła w życie – 26 lutego 2025 r.

Źródło: dziennikustaw.gov.pl/DU/rok/2025/pozycja/172

Ustawa dotyczy zmiany trzech aktów prawnych:

1. Ustawy sankcyjnej (dotyczącej przeciwdziałania wspieraniu agresji na Ukrainę).
2. Ustawy o Krajowej Administracji Skarbowej (KAS).
3. Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Zmiany mają na celu dostosowanie krajowego porządku prawnego do najnowszych unijnych regulacji oraz uszczelnienie systemu sankcyjnego wobec podmiotów wspierających agresję na Ukrainę.

Zmiany w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

1. Rozszerzenie uprawnień Generalnego Inspektora Informacji Finansowej (GIIF):

- GIIF będzie miał nowe zadanie polegające na sprawowaniu kontroli nad przestrzeganiem sankcji wynikających z rozporządzeń unijnych (765/2006, 269/2014, 833/2014) oraz ustawy sankcyjnej.
- Możliwość żądania dodatkowych informacji i dokumentów od instytucji obowiązanych w celu monitorowania zgodności z przepisami.

2. Wprowadzenie nowych obowiązków dla przedsiębiorców:

- Przedsiębiorcy dokonujący transakcji międzynarodowych zostaną zobowiązani do identyfikacji ryzyka związanego z eksportem towarów podwójnego zastosowania i weryfikacji kontrahentów.

- Konieczność odbioru oświadczeń od kontrahentów zagranicznych na temat dalszych odbiorców towarów.

3. Nowe środki kontroli:

- GIIF oraz Komisja Nadzoru Finansowego (KNF) będą miały możliwość pozyskiwania informacji zwrotnych od naczelników urzędów celno-skarbowych dotyczących kar pieniężnych nakładanych za naruszenie przepisów sankcyjnych.

4. Uszczelnienie systemu sankcji:

- Penalizacja działań zmierzających do obchodzenia sankcji, w tym nieświadomych naruszeń przepisów.
- Rozszerzenie katalogu kar za naruszenia oraz wprowadzenie kar administracyjnych.

5. Typ uprzywilejowany przestępstwa:

- Wprowadzenie możliwości łagodniejszego traktowania sprawców naruszeń, jeśli niski stopień społecznej szkodliwości czynu to uzasadnia.

6. Uwzględnienie zmienionych przepisów UE:

- Dostosowanie krajowych regulacji do nowych rozporządzeń unijnych w zakresie środków ograniczających (np. zarządzanie zamrożonymi aktywami).

1.2. Rozporządzenie Ministra Finansów z dnia 25 lutego 2025 r. zmieniające rozporządzenie w sprawie szczegółowych zasad sporządzania przez jednostki inne niż banki, zakłady ubezpieczeń i zakłady reasekuracji skonsolidowanych sprawozdań finansowych grup kapitałowych

Status: Weszło w życie - 7 marca 2025 r.

Źródło: dziennikustaw.gov.pl/DU/2025/275

Rozporządzenie Ministra Finansów z dnia 25 września 2009 r. w sprawie szczegółowych zasad sporządzania przez jednostki inne niż banki, zakłady ubezpieczeń i zakłady reasekuracji skonsolidowanych sprawozdań finansowych grup kapitałowych (Dz.U. z 2017 r. poz. 676), zwane dalej „rozporządzeniem”, jest wykonaniem upoważnienia ustawowego zawartego w art. 81 ust. 2 pkt 3 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598 oraz z 2024 r. poz. 619, 1685 i 1863), zwanej dalej „ustawą o rachunkowości”.

W odniesieniu do jednostek określonych w art. 1 pkt 30a lit. a ustawy o rachunkowości przez przychody netto ze sprzedaży towarów i produktów rozumie się przychody netto ze sprzedaży towarów i produktów, z uwzględnieniem dotacji, opustów, rabatów i innych zwiększeń lub zmniejszeń, bez podatku od towarów i usług oraz innych podatków bezpośrednio związanych z obrotem.

Z uwagi na usunięcie z kategorii przychodów netto ze sprzedaży przychodów ze sprzedaży materiałów, wprowadzana jest zmiana w tym zakresie załącznika nr 3 do ww. rozporządzenia

„Skonsolidowany rachunek zysków i strat”, zarówno w przypadku wariantu kalkulacyjnego, jak i wariantu porównawczego.

2. Projekty ustaw/rozporządzeń.

2.1. Projekt ustawy z dnia 10 lutego 2025 r. o systemach sztucznej inteligencji

Status: Uzgodnienia – 26 lutego 2025 r.

Źródło: legislacja.gov.pl/projekt/12390551/katalog/13087895#13087895

Celem projektowanej ustawy jest stworzenie systemu sprawowania nadzoru nad systemami sztucznej inteligencji w Polsce zgodnego z ramami prawnymi ustanowionymi rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), zwanego dalej „rozporządzeniem 2024/1689” albo „aktem o AI”.

Zgodnie z zasadami prawa europejskiego rozporządzenie obowiązuje w Unii od dnia 1 sierpnia 2024 r. W dniu 2 lutego 2025 r. w życie weszły przepisy dotyczące systemów zakazanych. W dniu 2 sierpnia 2025 r. zaczną obowiązywać przepisy dotyczące organów notyfikujących i jednostek notyfikowanych oraz kar za naruszenia przepisów podstawie naruszenia przepisów o zakazanych praktykach w zakresie AI. Projektowana ustawa określa organizację i sposób sprawowania nadzoru krajowego nad rynkiem systemów sztucznej inteligencji oraz modeli sztucznej inteligencji ogólnego przeznaczenia.

W Polsce nie istnieje organ spełniający wymagania Aktu o AI, dlatego projekt ustawy przewiduje powołanie **Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji** („Komisja”). Komisja ma być niezależnym organem nadzoru rynku AI, odpowiedzialnym za egzekwowanie przepisów rozporządzenia, kontrolę systemów AI oraz podejmowanie działań edukacyjnych i regulacyjnych. Będzie działać w modelu nadzoru zintegrowanego, na wzór Komisji Nadzoru Finansowego. Komisja będzie kolegialnym organem z przewodniczącym i jego zastępcami. W jej skład wejdą przedstawiciele kluczowych organów (m.in. UOKiK, KNF, UKE, Rzecznik Praw Dziecka). Głównymi zadaniami Komisji będą: kontrola przestrzegania przepisów AI, podejmowanie decyzji w sprawach naruszeń i nakładanie kar, monitorowanie rozwoju AI i wsparcie dla innowacji, prowadzenie rejestru skarg i zgłoszeń incydentów związanych z AI, współpraca z instytucjami UE i innymi krajami.

Nowe mechanizmy nadzoru będą opierać się na:

- Kontrola nad systemami AI – możliwość przeprowadzania kontroli, także zdalnie, oraz prowadzenie postępowań administracyjnych.
- Postępowanie przed Komisją – jednoinstancyjne, z możliwością odwołania do Sądu Okręgowego w Warszawie (Sąd Ochrony Konkurencji i Konsumentów).
- Zgłaszanie poważnych incydentów – obowiązek raportowania poważnych zagrożeń związanych z systemami AI.
- Komisja będzie mogła nakładać administracyjne kary pieniężne za naruszenia przepisów Aktu o AI.

- Możliwość zawarcia układu w sprawie nadzwyczajnego złagodzenia sankcji, jeśli naruszenie zostanie szybko usunięte.

Minister Cyfryzacji będzie organem notyfikującym jednostki oceniające zgodność systemów AI. Polskie Centrum Akredytacji (PCA) będzie odpowiedzialne za akredytację tych jednostek.

Zakłada się tworzenie „piaskownic regulacyjnych”, gdzie firmy (szczególnie MŚP i startupy) będą mogły testować systemy AI oraz możliwość udzielania pomocy finansowej dla badań nad AI oraz programów wspierających innowacje.

Projekt przewiduje dostosowanie kilku istniejących ustaw, m.in.:

- Kodeksu postępowania cywilnego,
- Ustawy o ochronie danych osobowych,
- Ustawy o radiofonii i telewizji.

Komisja ma rozpocząć działalność w 2025 r. Minister Cyfryzacji wyznaczy Pełnomocnika ds. organizacji Biura Komisji. Projekt przewiduje stopniowe rozszerzanie kompetencji Komisji do 2027 r., zgodnie z harmonogramem Aktu o AI.

Planowane wejście ustawy w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem art. 115 i art. 116, które wchodzi w życie z dniem następującym po dniu ogłoszenia.

2.2. Projekt ustawy z dnia 10 stycznia 2025 r. o ogólnym bezpieczeństwie produktów

Status: Przekazano do Komitetu ds. Europejskich – 18 lutego 2025 r.

Źródło: legislacja.rcl.gov.pl/projekt/12387803

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2023/988 z 10 maja 2023 r. w sprawie ogólnego bezpieczeństwa produktów, które zastępuje Dyrektywę 2001/95/WE z 3 grudnia 2001 r., wprowadza nowe zasady dotyczące bezpieczeństwa produktów w Unii Europejskiej. Nowe przepisy zostały opracowane w odpowiedzi na zmieniające się warunki rynkowe, w szczególności rozwój sprzedaży internetowej i globalizacji łańcuchów dostaw, co stworzyło nowe wyzwania dla bezpieczeństwa produktów konsumenckich.

- Główne założenia Rozporządzenia 2023/988:

1) Wzmocnienie ochrony konsumentów:

Rozporządzenie wprowadza nowe zasady mające na celu zwiększenie ochrony konsumentów przed niebezpiecznymi produktami na rynku unijnym. W szczególności dotyczy to produktów sprzedawanych online i przez platformy e-commerce, które nie zawsze są objęte takimi samymi standardami bezpieczeństwa jak produkty sprzedawane tradycyjnie.

2) Szerszy zakres stosowania:

Nowe rozporządzenie obejmuje wszystkie produkty konsumpcyjne wprowadzane na rynek unijny, które mogą stanowić zagrożenie dla zdrowia i bezpieczeństwa konsumentów. Dotyczy to nie tylko

produktów fizycznych, ale także cyfrowych, co odzwierciedla rosnące znaczenie produktów połączonych z internetem.

3) Nowe obowiązki dla przedsiębiorców:

1. Śledzenie i wycofywanie produktów: Wprowadzono bardziej rygorystyczne wymogi dotyczące identyfikowalności produktów, co ma ułatwić szybkie wycofywanie niebezpiecznych towarów z rynku. Przedsiębiorcy będą zobowiązani do utrzymywania szczegółowych danych o produktach oraz ich dostawcach przez określony czas.
2. Monitoring rynku: Platformy internetowe i pośrednicy będą zobowiązani do monitorowania oferowanych na ich platformach produktów i podejmowania działań w przypadku wykrycia niezgodności z wymaganiami bezpieczeństwa.

4) Obowiązki związane z platformami e-commerce:

Rozporządzenie wprowadza nowe obowiązki dla platform sprzedaży internetowej. Platformy będą musiały zapewnić skuteczny mechanizm do szybkiego reagowania na zgłoszenia dotyczące niebezpiecznych produktów, usuwania ich z ofert i powiadamiania konsumentów o zagrożeniu. Celem jest zwiększenie odpowiedzialności pośredników w handlu elektronicznym.

5) Wprowadzenie “zgodności cyfrowej”:

W rozporządzeniu uwzględniono bezpieczeństwo produktów cyfrowych i połączonych z internetem (tzw. smart products), co oznacza, że przedsiębiorstwa muszą zapewnić, że aktualizacje oprogramowania czy systemów nie wprowadzają nowych zagrożeń bezpieczeństwa.

6) Kary za nieprzestrzeganie przepisów:

W celu zwiększenia skuteczności nowego systemu przewidziano surowsze kary finansowe za nieprzestrzeganie przepisów. Grzywny mogą wynosić do 4% rocznych przychodów przedsiębiorcy, co ma na celu zniechęcenie do wprowadzania na rynek niebezpiecznych produktów.

- Zmiany w stosunku do Dyrektywy 2001/95/WE:

1) Zastąpienie dyrektywy przez rozporządzenie:

Wprowadzenie rozporządzenia zamiast dyrektywy oznacza, że przepisy te będą bezpośrednio stosowane we wszystkich państwach członkowskich UE, bez konieczności transpozycji do prawa krajowego. Zapewnia to bardziej jednolite stosowanie przepisów w całej Unii.

2) Lepsza adaptacja do współczesnych realiów rynkowych:

Rozporządzenie odpowiada na wyzwania związane z globalizacją, rosnącą liczbą produktów importowanych spoza UE oraz rozwojem sprzedaży internetowej. Nowe przepisy mają na celu skuteczniejsze eliminowanie zagrożeń związanych z nowymi technologiami i globalnymi łańcuchami dostaw.

3) Nowe narzędzia cyfrowe:

W ramach nowego systemu nadzoru rynkowego przewidziano także narzędzia cyfrowe umożliwiające lepsze monitorowanie i wykrywanie niebezpiecznych produktów, w tym systemy wczesnego ostrzeżenia i lepszą wymianę informacji pomiędzy organami państw członkowskich.

Podsumowując, rozporządzenie 2023/988 ma na celu dostosowanie regulacji dotyczących bezpieczeństwa produktów do współczesnych wyzwań rynkowych, w tym cyfryzacji, globalizacji oraz wzrostu handlu elektronicznego. Zastępując Dyrektywę 2001/95/WE, nowe przepisy mają na celu zapewnienie wyższego poziomu ochrony konsumentów w całej Unii Europejskiej.

Planowane wejście ustawy w życie po upływie 14 dni od dnia ogłoszenia.

2.3. Projekt ustawy z dnia 27 lutego 2025 r. o uchyleniu ustawy o Centralnej Informacji Emerytalnej

Status: Przekazano do Stałego Komitetu Rady Ministrów – 5 marca 2025 r.

Źródło: legislacja.gov.pl/projekt/12392802/katalog/13102725#13102725

Ustawa z dnia 7 lipca 2023 r. o Centralnej Informacji Emerytalnej (Dz.U. 2023 poz. 1941), zwana dalej „ustawą o CIE”, wprowadziła rozwiązania, które nie zapewniły kompleksowej realizacji założonego celu, jakim jest poprawa świadomości emerytalnej i zachęta do efektywnego oszczędzania na przyszłość.

Przewidywane wydatki na utrzymanie systemu CIE są wysokie, a szacunkowe wykorzystanie przez obywateli (ok. 5 mln użytkowników w ciągu 5 lat) uznano za niewystarczające. Wiele informacji emerytalnych jest już dostępnych poprzez Zakład Ubezpieczeń Społecznych (ZUS), Polski Fundusz Rozwoju (PFR) oraz inne instytucje. Analizowane dane wskazują, że poziom partycypacji w dobrowolnych programach emerytalnych jest niewielki, a CIE nie zmieniłoby istotnie tych trendów. Ponadto, istnieją obawy związane z ochroną informacji finansowych obywateli oraz zdolnością mniejszych instytucji do spełnienia wymogów technicznych.

Projekt ustawy dotyczy uchylenia ustawy o CIE oraz wprowadzenia zmian w wielu innych ustawach, które były związane z funkcjonowaniem tego systemu. System ten miał umożliwiać obywatelom dostęp do kompleksowych danych o ich oszczędnościach emerytalnych, obejmujących zarówno obowiązkowe, jak i dobrowolne formy oszczędzania na emeryturę. Jednak analiza kosztów wykazała, że korzyści płynące z tego systemu byłyby niewspółmierne do wydatków budżetowych, wobec tego proponuje się likwidację Centralnej Informacji Emerytalnej

W związku z uchyleniem ustawy o CIE konieczne stało się usunięcie oraz modyfikacja odpowiednich zapisów z innych aktów prawnych, m.in. z:

- ustawy z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych
- ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe
- ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych
- ustawy z dnia 22 maja 2003 r. o nadzorze ubezpieczeniowym i emerytalnym
- ustawy z dnia 20 kwietnia 2004 r. o indywidualnych kontaktach emerytalnych oraz indywidualnych kontaktach zabezpieczenia emerytalnego
- ustawy z dnia 20 kwietnia 2004 r. o pracowniczych programach emerytalnych

- ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi
- ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi
- ustawy z dnia 24 września 2010 r. o ewidencji ludności
- ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej
- ustawy z dnia 4 października 2018 r. o pracowniczych planach kapitałowych
- ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju
- ustawy z dnia 27 stycznia 2022 r. o dokumentach paszportowych

Planowane wejście ustawy w życie po upływie 14 dni od dnia ogłoszenia.

2.4. Projekt ustawy z dnia 13 grudnia 2024 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw

Status: Przekazano do Stałego Komitetu Rady Ministrów – 25 lutego 2025 r.

Źródło: legislacja.rcl.gov.pl/projekt/12383101/katalog/13045617#13045617

4 października 2022 r. przyjęte zostało przez Radę do Spraw Gospodarczych i Finansowych (ECOFIN) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), zwane dalej „rozporządzeniem 2022/2065”.

W ramach prac wdrożeniowych rozporządzenia 2022/2065 rekomenduje się nowelizację ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, stanowiącej implementację dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), zmienianej przepisami rozporządzenia 2022/2065. Prace wdrożeniowe wymagać będą również nowelizacji innych aktów prawnych, w których zawarte są odesłania do zmienianych przepisów ww. ustawy o świadczeniu usług drogą elektroniczną, jak i odpowiednich przepisów sektorowych.

Nowelizacja ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną przewiduje:

- 1) uchylenie przepisów dotyczących zasad wyłączenia odpowiedzialności usługodawców z tytułu świadczenia usług drogą elektroniczną, które stanowią implementację dyrektywy 2000/31/WE, w zakresie zmienianym przez rozporządzenie 2022/2065, a które wraz z wejściem w życie rozporządzenia 2022/2065 będą stosowane bezpośrednio w państwach członkowskich;
- 2) wskazanie Prezesa UKE jako właściwego organu sprawującego nadzór nad stosowaniem przepisów rozporządzenia 2022/2065 oraz powierzenie mu roli koordynatora ds. usług cyfrowych w rozumieniu rozporządzenia 2022/2065. Wraz z wejściem w życie ustawy nowelizującej kompetencje Prezesa UKE rozszerzone zostaną o obowiązki organu nadzorczego oraz koordynatora ds. usług cyfrowych wskazane w rozporządzeniu 2022/2065, m.in. konieczność przeprowadzania kontroli nad podmiotami zobowiązanymi do przestrzegania przepisów rozporządzenia 2022/2065, nakładanie administracyjnych kar

- pieniężnych, współpraca z koordynatorami innych państw członkowskich oraz z Radą Usług Cyfrowych i Komisją Europejską;
- 3) wskazanie Prezesa Urzędu Ochrony Konkurencji i Konsumentów, zwanego dalej „Prezesem UOKiK”, jako właściwego organu sprawującego nadzór nad stosowaniem przepisów rozporządzenia 2022/2065 w zakresie swojej właściwości, określonej przepisami ustawy;
 - 4) uregulowanie zasad i trybu certyfikacji organów pozasądowego rozstrzygania sporów;
 - 5) uregulowanie zasad i trybu przyznawania statusu zaufanego podmiotu sygnalizującego;
 - 6) uregulowanie zasad i trybu przyznawania statusu zweryfikowanego badacza;
 - 7) określenie zasad prowadzenia postępowania kontrolnego związanego z przestrzeganiem przepisów rozporządzenia 2022/2065 przez podmioty do tego zobowiązane;
 - 8) uregulowanie kwestii dotyczących administracyjnych kar pieniężnych możliwych do nałożenia przez właściwe organy w związku ze stwierdzeniem nieprzestrzegania przepisów rozporządzenia 2022/2065 przez podmioty do tego zobowiązane. Maksymalne wartości dotyczące wymierzanych kar pieniężnych wprost wynikają z rozporządzenia 2022/2065;
 - 9) uregulowanie kwestii wydawania nakazów podjęcia działań przeciwko nielegalnym treściom oraz nakazów udostępniania informacji o usługobiorcy;
 - 10) zmiany w innych ustawach wymagane ujednoczeniem przepisów ze względu na zmianę odesłań spowodowanych uchynieniem rozdziału 3 nowelizowanej ustawy.

Planowane wejście w życie po upływie 30 dni od dnia ogłoszenia.

2.5. Projekt ustawy z dnia 5 lutego 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji

Status: Przekazano do Komisji Prawniczej – 19 lutego 2025 r.

Źródło: legislacja.gov.pl/projekt/12384252/katalog/13053526#13053526

Projekt ustawy wynika z wdrożenia Rozporządzenia (UE) 2022/2554 (tzw. DORA – Digital Operational Resilience Act), które wprowadza regulacje dotyczące zarządzania ryzykiem ICT w sektorze finansowym.

KNF będzie odpowiedzialna za nadzorowanie zgodności instytucji finansowych z wymaganiami DORA. Organ ten uzyska nowe uprawnienia do inspekcji i audytów w zakresie systemów ICT w podmiotach nadzorowanych oraz możliwość wydawania decyzji nakazujących podjęcie określonych działań, jeśli podmiot nie spełnia wymagań. KNF będzie współpracować z krajowymi organami cyberbezpieczeństwa (CSIRT MON, CSIRT NASK, CSIRT GOV) w zakresie wymiany informacji o cyberzagrożeniach i koordynacji działań w sytuacjach kryzysowych. KNF będzie centralnym punktem raportowania incydentów i przekaże informacje do:

- CSIRT MON (wojskowe centrum cyberbezpieczeństwa).
- CSIRT NASK (cyberbezpieczeństwo sektora cywilnego i prywatnego).
- CSIRT GOV (cyberbezpieczeństwo administracji publicznej).

Banki, domy maklerskie, firmy ubezpieczeniowe, instytucje płatnicze i inne podmioty objęte regulacją będą musiały dostosować swoje systemy ICT do nowych standardów. Każda instytucja musi wdrożyć ramy zarządzania ryzykiem ICT, obejmujące:

- Identyfikację ryzyk związanych z ICT.
- Wdrożenie polityki odporności cyfrowej.
- Zarządzanie danymi i ochroną przed incydentami cybernetycznymi.

Zarząd każdej instytucji będzie odpowiedzialny za strategię odporności cyfrowej oraz za zapewnienie zgodności systemów ICT z nowymi przepisami.

Planowane jest wprowadzenie jednolitych zasad zgłaszania poważnych incydentów ICT do KNF oraz krajowych organów cyberbezpieczeństwa. Zgłoszenia muszą być realizowane w trzech etapach: Zawiadomienie wstępne – do 24 godzin od wykrycia incyduentu, Raport szczegółowy – w ciągu 72 godzin od zgłoszenia incyduentu oraz Raport końcowy – maksymalnie 30 dni od zakończenia incyduentu. Incydenty będą klasyfikowane według skali wpływu na klientów i działalność instytucji.

Nowe regulacje wymagają od instytucji finansowych prowadzenia rejestru incydentów ICT, obejmującego wszystkie zgłoszone zdarzenia, nawet te mniejszej skali.

Każda instytucja finansowa musi oceniać ryzyko związane z korzystaniem z usług zewnętrznych dostawców ICT. Dostawcy kluczowych usług ICT (np. przetwarzanie w chmurze, centra danych) będą podlegać nadzorowi UE i KNF. Obowiązkowe audyty dostawców ICT przez instytucje finansowe w celu oceny ich bezpieczeństwa. Instytucje finansowe będą zobowiązane do prowadzenia rejestru wszystkich umów ICT z dostawcami. Możliwość wymuszenia zmiany dostawcy ICT, jeśli usługi nie spełniają nowych standardów bezpieczeństwa.

Wprowadzenie mechanizmu nadzoru nad kluczowymi dostawcami ICT na poziomie UE. Europejskie Urzędy Nadzoru Finansowego (EBA, ESMA, EIOPA) uzyskają prawo do inspekcji kluczowych dostawców technologicznych (np. firm chmurowych). Możliwość wydania decyzji nakazujących ograniczenie korzystania z usług ryzykownego dostawcy ICT.

KNF będzie mogła nakładać sankcje finansowe za niezgodność z nowymi regulacjami. Możliwość publikowania ostrzeżeń publicznych dotyczących naruszeń przepisów. Sankcje mogą dotyczyć zarówno firm, jak i ich zarządów. Możliwe kary dla instytucji finansowych i dostawców ICT: kary administracyjne za brak zgodności z wymogami, zakaz pełnienia funkcji kierowniczych dla osób odpowiedzialnych za naruszenia bezpieczeństwa ICT, obowiązek wdrożenia działań naprawczych pod nadzorem KNF.

Planowane wejście w życie w dniu następującym po dniu ogłoszenia, z wyjątkami.

2.6. Projekt ustawy z dnia 31 stycznia 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa

Status: Przekazano do Stałego Komitetu Rady Ministrów – 5 marca 2025 r.

Źródło: legislacja.rcl.gov.pl/projekt/12385350

Zakres przedmiotowy projektowanej ustawy wynika ze ścisłego związku tych przepisów z rozporządzeniem 2019/881. Projektowana ustawa określa organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego

systemu, a także sposób sprawowania nadzoru, kontroli i koordynacji w zakresie stosowania przepisów ustawy.

Najważniejszym celem ustawy jest zapewnienie wzajemnego uznawania certyfikatów cyberbezpieczeństwa w UE. Certyfikat wydany w Polsce będzie automatycznie honorowany we wszystkich krajach Unii. Ustawa definiuje strukturę krajowego systemu certyfikacji cyberbezpieczeństwa oraz wskazuje podmioty wchodzące w jego skład:

- Minister właściwy do spraw informatyzacji – centralny organ odpowiedzialny za nadzór nad certyfikacją cyberbezpieczeństwa (pełniący rolę krajowego organu ds. certyfikacji).
- Polskie Centrum Akredytacji (PCA) – krajowa jednostka akredytująca, nadzorująca kompetencje i działanie podmiotów certyfikujących w systemie.
- Jednostki oceniające zgodność – akredytowane podmioty (np. laboratoria, firmy certyfikujące) przeprowadzające ocenę zgodności produktów, usług i procesów ICT z wymaganiami bezpieczeństwa.
- Dostawcy produktów, usług i procesów ICT – podmioty (producenci, importerzy, dystrybutorzy lub inne jednostki wprowadzające na rynek) poddające swoje wyroby lub usługi procesowi certyfikacji.

Krajowy system certyfikacji został zaprojektowany jako dobrowolny – podmioty prywatne (przedsiębiorcy, producenci) nie są zobligowane do uzyskiwania certyfikatów, a obowiązki wynikające z ustawy dotyczą tylko tych, którzy dobrowolnie zdecydują się przystąpić do procesu certyfikacji. Dotyczy to zarówno firm ubiegających się o certyfikaty, jak i jednostek oceniających zgodność chcących je wydawać – uczestnictwo w systemie jest kwestią wyboru i chęci spełnienia określonych standardów.

Przewidziano również możliwość rozszerzenia certyfikacji na nowe obszary w drodze krajowych programów. Minister właściwy ds. informatyzacji może ustanawiać krajowe schematy certyfikacji, które pozwolą certyfikować nie tylko produkty, usługi czy procesy ICT, ale też np. kompetencje osób (specjalistów) w dziedzinie cyberbezpieczeństwa oraz systemy zarządzania cyberbezpieczeństwem w organizacjach.

Planowane wejście ustawy w życie po upływie miesiąca od dnia ogłoszenia.

2.7. Projekt ustawy z dnia 10 stycznia 2025 r. o rynku kryptoaktywów

Status: Przekazano do Komisji Prawniczej – 5 marca 2025 r.

Źródło: legislacja.rcl.gov.pl/projekt/12382311/katalog/13040429#13040429

Projekt ustawy zakłada m.in. wprowadzenie zmian w ustawie z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (dalej „UFI”).

Zostanie dodany przepis, który uprawnia towarzystwo funduszy inwestycyjnych do świadczenia usług w zakresie kryptoaktywów, o których mowa w art. 60 ust. 5 rozporządzenia 2023/1114 na zasadach określonych w tym rozporządzeniu. Projekt wprowadza także zmiany polegające na umożliwieniu zamkniętym funduszom inwestycyjnym nabywanie do swojego portfela

inwestycyjnego oferowanych publicznie lub dopuszczonych do obrotu tokenów powiązanych z aktywami lub tokenów będących e- pieniądzem.

Dodaje się oferowane publicznie lub dopuszczone do obrotu tokeny powiązane z aktywami lub tokeny będące e-pienniądzem wyemitowane przez jeden podmiot do katalogu czynności, odnośnie do których wierzytelności wobec tego podmiotu i udziały w tym podmiocie nie mogą stanowić łącznie więcej niż 20 % wartości aktywów funduszu.

Ponadto projekt przewiduje, że oferowane publicznie lub dopuszczone do obrotu ww. aktywa nie mogą stanowić więcej niż 20% wartości aktywów funduszu inwestycyjnego zamkniętego, jednocześnie wyemitowane przez jeden podmiot oferowane publicznie lub dopuszczone do obrotu tokeny powiązane z aktywami lub tokeny będące e-pienniądzem nie mogą stanowić więcej niż 10% wartości aktywów funduszu.

Zmiana ustawy ma na celu doprecyzowanie, że w 20% limicie waluty obcej jednego państwa lub euro względem wartości aktywów danego funduszu inwestycyjnego uwzględnia się również wartość tokenów powiązanych z walutami obcymi lub euro. Zmiana ta ma pozwolić towarzystwom funduszy inwestycyjnych na poszerzenie oferty w zakresie oferowanych na krajowym rynku funduszy inwestycyjnych oraz na dalszą dywersyfikację portfela inwestycyjnego tych funduszy.

Zgodnie z projektowanym przepisem fundusze inwestycyjne zamknięte będą mogły nabywać wyłącznie kryptoaktywa oferowane publicznie lub dopuszczone do obrotu na zasadach określonych w rozporządzeniu 2023/1114.

Nowelizacja ma również precyzować sytuację, w której fundusz inwestycyjny zamknięty zamierza dokonywać lokat, m.in. określając warunki jakie powinien spełniać jego statut. Art. 154 UFI także ma być zmieniony – określając w ust 1, że przy stosowaniu limitów inwestycyjnych, o których mowa w art. 145 ust. 3, 3a, 4 lub 7, fundusz inwestycyjny zamknięty jest obowiązany uwzględniać wartość również oferowanych publicznie lub dopuszczonych do obrotu tokenów powiązanych z aktywami lub tokenów będących e-pienniądzem.

Planowane wejście ustawy w życie po upływie 14 dni od dnia ogłoszenia.

3. Komunikaty, wydarzenia i stanowiska organów nadzoru

3.1. Działalność nadzorcza Komisji Nadzoru Finansowego:

3.1.1. Biuletyn Kwartalny. Rynek OFE 4/2024

Urząd Komisji Nadzoru Finansowego informuje, że w serwisie internetowym dostępny jest Biuletyn Kwartalny. Rynek OFE 4/2024.

Źródło: knf.gov.pl/?articleId=92842&p_id=18

3.1.2. Informacje o rynku IKZE według stanu na 31 grudnia 2024 roku

Urząd Komisji Nadzoru Finansowego informuje, że w serwisie internetowym dostępne są Informacje o rynku IKZE według stanu na 31 grudnia 2024 roku.

Źródło: knf.gov.pl/?articleId=92780&p_id=18

3.1.3. Informacje o rynku IKE według stanu na 31 grudnia 2024 roku

Urząd Komisji Nadzoru Finansowego informuje, że w serwisie internetowym dostępne są Informacje o rynku IKE według stanu na 31 grudnia 2024 roku.

Źródło: knf.gov.pl/?articleId=92778&p_id=18

3.1.4. Dane kwartalne TFI - IV kwartał 2024 roku

Urząd Komisji Nadzoru Finansowego informuje, że w serwisie internetowym dostępne są Dane kwartalne TFI - IV kwartał 2024 roku.

Źródło: knf.gov.pl/?articleId=92731&p_id=18

3.2. PFR Portal PPK: Biuletyn miesięczny Pracowniczych Planów Kapitałowych

W serwisie internetowym PFR Portal PPK dostępny jest Biuletyn Pracowniczych Planów Kapitałowych za luty 2025 r.

Źródło: mojeppk.pl/pliki/repozytorium-plikow/materialy-do-pobrania/pdf/Biuletyn-PPK-02-2025.pdf

3.3. Stanowisko UKNF dot. stosowania Rozporządzenia DORA przez TFI oraz zarządzających ASI

Urząd Komisji Nadzoru Finansowego opublikował na stronie stanowisko dot. stosowania Rozporządzenia DORA przez TFI oraz zarządzających ASI.

Źródło: knf.gov.pl/?articleId=92526&p_id=18

Kontakt

Jeżeli nie chcą Państwo otrzymywać tego typu korespondencji w przyszłości, prosimy o przekazanie takiej informacji na adres dsm@finat.pl
