Finat

NR 8/2025. STAN NA DZIEŃ 11 SIERPNIA 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 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa;

1.2. Ustawa z dnia 9 lipca 2025 r. zmieniającą ustawę o zmianie ustawy o rachunkowości, ustawę o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym oraz niektórych innych ustaw;

1.3. Ustawa z dnia 25 czerwca 2025 r. o zmianie ustawy o podatku dochodowym od osób fizycznych oraz ustawę o podatku dochodowym od osób prawnych;

1.4. Ustawa z dnia 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji;

1.5. Ustawa z dnia 5 sierpnia 2025 r. o uchyleniu ustawy o Centralnej Informacji Emerytalnej;

1.6. Ustawa z dnia 9 lipca 2025 r. o zmianie ustawy o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi;

1.7. Ustawa z dnia 25 czerwca 2025 r. o zmianie ustawy o podatku dochodowym od osób prawnych.

2. Projekty ustaw/rozporządzeń

2.1. Projekt ustawy z dnia 3 lipca 2025 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw;

2.2. Projekt ustawy z dnia 8 lipca 2025 r. o ogólnym bezpieczeństwie produktów.

3. Komunikaty, wydarzenia i stanowiska organów nadzoru

3.1. Działalność nadzorcza Komisji Nadzoru Finansowego:

3.1.1. Wartość aktywów netto funduszy zdefiniowanej daty (PPK) wg stanu na koniec II kwartału 2025;

3.1.2. Dane miesięczne OFE - czerwiec 2025 rok;

3.2. PFR Portal PPK: Biuletyn miesięczny Pracowniczych Planów Kapitałowych - nr 45 lipiec 2025.

II. Obszar zmian

1. Prawo krajowe. Nowe przepisy wchodzące w życie.

1.1. Ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa

Status: Wejdzie w życie – 28 sierpnia 2025 r.

Źródło: isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250001017

Ustawa wprowadza w Polsce rozwiązania mające na celu stworzenie i funkcjonowanie spójnego, dobrowolnego systemu oceny i potwierdzania zgodności w zakresie bezpieczeństwa produktów, usług, procesów i systemów informacyjno-komunikacyjnych oraz kompetencji osób fizycznych w obszarze cyberbezpieczeństwa. Jej uchwalenie wynika z konieczności dostosowania prawa krajowego do unijnego rozporządzenia 2019/881, czyli tzw. aktu o cyberbezpieczeństwie.

System certyfikacji, który ustawa ustanawia, obejmuje określony zestaw podmiotów i procedur. W jego skład wchodzi minister właściwy do spraw informatyzacji pełniący funkcję krajowego organu do spraw certyfikacji cyberbezpieczeństwa, Polskie Centrum Akredytacji, jednostki oceniające zgodność, a także dostawcy, którzy poddają swoje produkty, usługi lub procesy ICT ocenie zgodności, podmioty certyfikujące swoje systemy zarządzania cyberbezpieczeństwem oraz osoby fizyczne weryfikujące swoje kompetencje w tym zakresie.

Certyfikacja może być prowadzona w ramach europejskich programów certyfikacji, które obowiązują w całej Unii, lub w ramach krajowych schematów tworzonych w Polsce, gdy dany obszar nie jest objęty programem unijnym.

Udział w systemie jest **dobrowolny**, więc dostawca, który nie ubiega się o certyfikat, nie ma żadnych obowiązków wynikających z tej ustawy. Certyfikaty wydawane są na okres **od dwóch do pięciu lat** i mogą dotyczyć zarówno aspektów technicznych, takich jak dostępność, autentyczność, integralność czy poufność danych, jak i organizacyjnych, obejmujących cały system zarządzania cyberbezpieczeństwem w danej instytucji. Mogą być również przyznawane osobom fizycznym jako potwierdzenie ich wiedzy i praktycznych umiejętności w dziedzinie cyberbezpieczeństwa.

Ustawa przewiduje szereg obowiązków, które pojawiają się, jeżeli taki podmiot zdecyduje się wejść do krajowego systemu certyfikacji cyberbezpieczeństwa. W momencie, gdy dostawca zgłosi swój produkt, usługę lub proces do certyfikacji, pojawia się cały zestaw wymagań. Pierwszym z nich jest **zawarcie umowy z jednostką oceniającą zgodność**. Umowa musi szczegółowo określać, co jest przedmiotem certyfikacji, w jakim programie lub schemacie (europejskim czy krajowym) jest ona prowadzona, jaki jest poziom zaufania w przypadku certyfikacji europejskiej, a także zakres certyfikacji oraz zobowiązania stron. Istotnym elementem umowy jest sposób ochrony

przekazywanych informacji, w szczególności tajemnic handlowych i przedsiębiorstwa, danych poufnych oraz praw własności intelektualnej.

Dostawca ma obowiązek udostępnić jednostce oceniającej zgodność wszelką niezbędną dokumentację techniczną, informacje o produkcie, usłudze lub procesie, a także próbki lub dostęp do środowiska, w którym działa dane rozwiązanie, jeżeli jest to wymagane do przeprowadzenia badań i audytów.

Po uzyskaniu certyfikatu dostawca musi utrzymywać zgodność certyfikowanego elementu z wymaganiami schematu przez cały okres jego ważności. Jeżeli zostaną wykryte podatności lub inne istotne problemy bezpieczeństwa, dostawca ma obowiązek niezwłocznie poinformować o tym jednostkę, która wydała certyfikat, oraz – w razie potrzeby – podjąć działania zaradcze. W sytuacji, gdy jednostka certyfikująca stwierdzi niezgodności, dostawca jest zobowiązany w ciągu **14 dni** przedstawić propozycję działań naprawczych, a następnie **w ciągu dwóch miesięcy** je zrealizować. Niewykonanie tego obowiązku lub utrudnianie weryfikacji może skutkować cofnięciem certyfikatu.

Niewywiązywanie się z obowiązków może skutkować nałożeniem kary finansowej, której wysokość w przypadku dostawców może wynieść nawet do dwudziestokrotności przeciętnego wynagrodzenia – na przykład za nieprzekazanie informacji ministrowi w terminie, nieudostępnienie unijnej deklaracji zgodności, nieprzekazanie próbek produktu lub brak realizacji obowiązków publicznego udostępniania dodatkowych informacji o cyberbezpieczeństwie.

1.2. Ustawa z dnia 9 lipca 2025 r. zmieniającą ustawę o zmianie ustawy o rachunkowości, ustawę o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym oraz niektórych innych ustaw

Status: Wejdzie w życie – 12 sierpnia 2025 r.

Źródło: isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250001020

9 lipca 2025 r. uchwalono ustawę dostosowującą polskie przepisy do dyrektywy UE 2025/794, która wprowadza **dwuletnie odroczenie** obowiązku raportowania informacji o zrównoważonym rozwoju (ESG) dla części przedsiębiorstw.

- **Duże jednostki** (druga fala) będą raportować pierwszy raz w 2028 r. za rok 2027.
- **Małe i średnie spółki giełdowe** (trzecia fala) – w 2029 r. za rok 2028.

W związku z przesunięciem terminów uchylono dotychczasową możliwość dodatkowego odroczenia raportowania dla trzeciej fali, bo stała się zbędna.

1.3. Ustawa z dnia 25 czerwca 2025 r. o zmianie ustawy o podatku dochodowym od osób fizycznych oraz ustawę o podatku dochodowym od osób prawnych

Status: Wejdzie w życie – 1 stycznia 2026 r.

Źródło: isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250001022

Przyjęta ustawa modyfikuje przepisy podatkowe od 1 stycznia 2026 r. i obejmuje trzy kluczowe obszary:

1. **Specjalna Strefa Ekonomiczna i Polska Strefa Inwestycji** – w przypadku cofnięcia zezwolenia lub uchylenia decyzji o wsparciu przedsiębiorca traci prawo do zwolnienia z PIT/CIT i musi zapłacić podatek od dochodu uzyskanego w ramach cofniętego przywileju.
2. **Spółki jawne** – zniesienie obowiązku corocznego składania informacji o wspólnikach, jeśli ich skład się nie zmienił.
3. **Podatkowe grupy kapitałowe** – likwidacja sankcji utraty statusu podatnika CIT za transakcje z podmiotami powiązanymi spoza grupy na warunkach nierynkowych.

1.4. Ustawa z dnia 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji

Status: Weszła w życie – 7 sierpnia 2025 r.

Źródło: isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250001069

Ustawa z 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji wdraża do polskiego prawa m.in. rozporządzenie DORA (UE 2022/2554).

Podmioty objęte ustawą – w tym banki, instytucje płatnicze, firmy inwestycyjne, zakłady ubezpieczeń, fundusze inwestycyjne oraz ich kluczowi dostawcy ICT – muszą wdrożyć kompleksowe systemy zarządzania ryzykiem ICT. Obejmuje to identyfikowanie zagrożeń i podatności, ocenę i dokumentowanie ryzyka, procedury minimalizujące skutki incydentów, a także plany ciągłości działania i odtwarzania po awarii. Wymagana jest również regularna aktualizacja polityk bezpieczeństwa.

Jednym z filarów ustawy jest obowiązek raportowania incydentów ICT. Poważne zdarzenia należy niezwłocznie zgłaszać do Komisji Nadzoru Finansowego (KNF), która przekaże informacje do właściwego zespołu CSIRT (MON, NASK lub GOV). Procedura obejmuje wstępne powiadomienie, raporty etapowe oraz raport końcowy po rozwiązaniu incydentu.

Regulacje wprowadzają także wymóg testowania i monitorowania systemów. Instytucje mają obowiązek przeprowadzania regularnych testów penetracyjnych i innych form weryfikacji odporności systemów ICT. Większe podmioty muszą korzystać z zaawansowanych testów zgodnych z wytycznymi TIBER-EU lub równoważnych, realizowanych przez niezależnych specjalistów.

Kolejnym obszarem jest nadzór nad dostawcami zewnętrznymi ICT. Instytucje muszą klasyfikować dostawców, identyfikować tych o krytycznym znaczeniu i zawierać z nimi umowy zawierające szczegółowe zapisy o bezpieczeństwie, audytach, dostępie do danych i ciągłości działania.

Niezbędne jest monitorowanie jakości i bezpieczeństwa świadczonych usług oraz informowanie KNF o zawarciu lub rozwiązaniu umowy z dostawcą krytycznym.

DORA nakłada też wymóg prowadzenia i udostępniania dokumentacji dotyczącej zarządzania ryzykiem ICT oraz przygotowywania sprawozdań potwierdzających realizację wymogów. KNF otrzymuje szerokie uprawnienia kontrolne, obejmujące dostęp do pomieszczeń, systemów i dokumentów, żądanie danych telekomunikacyjnych czy nakładanie działań naprawczych.
Niewykonanie obowiązków wynikających z DORA – takich jak brak raportów, niewdrożenie procedur czy utrudnianie kontroli – może skutkować nałożeniem sankcji finansowych. Ich wysokość zależy od rodzaju naruszenia i charakteru podmiotu.

1.5. Ustawa z dnia 5 sierpnia 2025 r. o uchyleniu ustawy o Centralnej Informacji Emerytalnej

Status: Przekazano Prezydentowi do podpisu – 6 sierpnia 2025 r.

Źródło:
sejm.gov.pl/Sejm10.nsf/PrzebiegProc.xsp?id=3C32534949A24CF9C1258C9D00574FE5

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.

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

1. Dodanie nowego art. 192c do ustawy o organizacji i funkcjonowaniu funduszy emerytalnych
• Otwarty fundusz emerytalny może przekazywać elektronicznie do ZUS dane, o których mowa w art. 50b ustawy o systemie ubezpieczeń społecznych – w celu realizacji zadań ZUS.

2. Zmiana art. 105 ustawy – Prawo bankowe
• Uchylenie ust. 2c.
• Dodanie ust. 2d – banki prowadzące IKE lub IKZE mogą przekazywać dane do ZUS w celu realizacji zadań wynikających z art. 50b ustawy o systemie ubezpieczeń społecznych.

3. Rozszerzenia definicji „podmiotu zainteresowanego"
W nowelizowanej ustawie dodaje się do definicji:
• podmioty prowadzące IKE/IKZE,
• podmioty prowadzące PPE (m.in. TFI, ubezpieczyciele, zagraniczni zarządzający),

• PTE zarządzające OFE,
• spółkę prowadzącą Ewidencję PPK.

4. Zmiany w ustawie o systemie ubezpieczeń społecznych
a) Art. 50:
• Dodanie ust. 1ba – informacje o hipotetycznej emeryturze przekazywane są osobom, które ukończyły 35 lat na dzień 31 grudnia poprzedniego roku.
• Nowe brzmienie ust. 1c – szczegóły wyliczania emerytury z uwzględnieniem składek i miesięcy ubezpieczenia.
• Nowy ust. 1ha – informacje mogą być przekazywane przez aplikację mObywatel
b) Nowe artykuły 50b–50f:
• Art. 50b – ZUS może udostępniać przez mObywatela:
  - dane o zgromadzonych środkach z różnych form oszczędzania emerytalnego (IKE, IKZE, PPE, OFE, PPK, KRUS),
  - informacje o składkach, jednostkach uczestnictwa, instrumentach finansowych,
  - inne dane potrzebne do wyliczenia świadczeń.
• Art. 50c – KRUS i podmioty zainteresowane mogą przekazywać dane do ZUS (za zgodą osoby).
• Art. 50d – ZUS prowadzi ewidencję tych danych i przetwarza je.
• Art. 50e – ZUS jest administratorem danych zgodnie z RODO.
• Art. 50f – stosuje się przepisy o ochronie danych osobowych (art. 34 i 79 u.s.u.s.).

5. Dodanie art. 17b w ustawie o pracowniczych programach emerytalnych
• Instytucja finansowa może elektronicznie przekazywać dane do ZUS w celach z art. 50b.

6. Dodanie art. 22g w ustawie o pracowniczych planach kapitałowych
• Zarządzający (np. PFR Portal PPK) może przekazywać dane do ZUS.

7. Zmiany w ustawie o aplikacji mObywatel
• Rozszerzenie uprawnień operatora portalu i ZUS do przetwarzania oraz przekazywania danych, dokumentów i informacji.

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

1.6. Ustawa z dnia 9 lipca 2025 r. o zmianie ustawy o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi

Status: Przekazano Prezydentowi do podpisu – 4 sierpnia 2025 r.

Źródło: sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=1305

Celem ustawy jest ułatwienie łączenia niepublicznych funduszy inwestycyjnych zamkniętych, których organem jest to samo towarzystwo funduszy inwestycyjnych, poprzez złagodzenie wymogów w zakresie konieczności uzyskiwania zgody zgromadzenia inwestorów na połączenie.

Zgodnie z art. 208zzi ust. 7 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (Dz. U. z 2024 r. poz. 1034 i 1863 oraz

z 2025 r. poz. 146), dalej „ustawa o funduszach inwestycyjnych", połączenie funduszy inwestycyjnych zamkniętych, zarządzanych przez to samo towarzystwo funduszy inwestycyjnych, wymaga zgody zgromadzenia inwestorów funduszu przejmowanego oraz funduszu przejmującego, a w przypadku połączenia przez utworzenie nowego funduszu inwestycyjnego, zgody zgromadzenia inwestorów funduszu przejmowanego. Uchwała udzielająca zgody wymaga oddania głosów za połączeniem przez uczestników reprezentujących 2/3 ogólnej liczby certyfikatów inwestycyjnych.

W niniejszej ustawie przewidziano złagodzenie wymogów w zakresie konieczności uzyskiwania zgody zgromadzenia inwestorów na połączenie niepublicznych funduszy inwestycyjnych zamkniętych, których organem jest to samo towarzystwo funduszy inwestycyjnych. Zmiany w tym zakresie zakładają:

1) obniżenie z 2/3 do połowy wymaganego progu głosów ogólnej liczby certyfikatów inwestycyjnych danego funduszu za połączeniem – zmiana art. 208zzi ust. 8 ustawy o funduszach inwestycyjnych,
2) rezygnację z wymogu oddania głosów przez uczestników reprezentujący łącznie co najmniej połowę ogólnej liczby certyfikatów inwestycyjnych danego funduszu, w sytuacji gdy pomimo dwukrotnie prawidłowo zwołanego zgromadzenia inwestorów oddano mniej niż połowę głosów reprezentujących liczbę certyfikatów inwestycyjnych danego funduszu – w takim przypadku zgoda na połączenie zostanie udzielona, jeżeli głosy za połączeniem odda co najmniej połowa uczestników obecnych lub reprezentowanych podczas głosowania.

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

1.7. Ustawa z dnia 25 czerwca 2025 r. o zmianie ustawy o podatku dochodowym od osób prawnych

Status: Przekazano Prezydentowi do podpisu – 27 lipca 2025 r.

Źródło: sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=1233

Projektowana zmiana polega na uchyleniu art. 27c ustawy CIT i oznacza zniesienie obowiązku publikacji (przez największych podatników CIT) informacji o realizowanej strategii podatkowej.

Zwolnieniem będą objęte wszystkie obowiązki dotyczące informacji o realizowanej strategii podatkowej, tj. nie tylko obowiązki sporządzania i podawania do publicznej wiadomości informacji o realizowanej strategii podatkowej, ale również obowiązek przekazywania do naczelnika urzędu skarbowego informacji o adresie strony internetowej, na której informacje o realizowanej strategii podatkowej zostały zamieszczone.

Uchylenie art. 27c ustawy CIT będzie równoznaczne ze zniesieniem obowiązku udostępniania informacji na stronie internetowej za poszczególne lata (art. 27c ust. 6). Zgodnie z aktualnie obowiązującymi przepisami informacja raz zamieszczona na stronie internetowej ma być dostępna dla zainteresowanych przez kolejne lata. Tym samym po wejściu w życie ustawy

zniesiony zostanie również obowiązek zapewnienia dostępu do informacji zamieszczonych na stronie internetowej za lata poprzednie.

Planowane wejście w życie w dniu następującym po dniu ogłoszenia.

2. **Projekty ustaw/rozporządzeń.**

2.1. Projekt ustawy z dnia 3 lipca 2025 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw

Status: Przekazano do Stałego Komitetu Rady Ministrów – 8 sierpnia 2025 r.

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

Projekt ustawy, którego celem jest pełne „podpięcie" polskiego systemu pod unijny Akt o usługach cyfrowych (DSA). W praktyce projekt wskazuje polskie organy, tworzy szybkie procedury nakazowe, daje ścieżki odwoławcze i wprowadza sankcje – tak, by DSA dało się realnie egzekwować w Polsce.

Szybkie nakazy wobec treści i decyzji platform.
Pojawia się krótka procedura, w której prokurator, Policja, usługobiorca albo „zaufany podmiot sygnalizujący" mogą uzyskać decyzję nakazującą:

1) zablokowanie dostępu do nielegalnych treści, albo
2) uchylenie ograniczeń nałożonych przez hosting, gdy moderacja była nietrafiona.

Właściwy jest UKE (co do zasady) albo KRRiT (dla platform wideo).

Koordynatorem ds. usług cyfrowych zostaje Prezes UKE; obok niego jako „właściwe organy" działają Prezes UOKiK (wątek konsumencki w DSA) i KRRiT (platformy udostępniania wideo). Między organami przewidziano współpracę, a spory kompetencyjne rozstrzyga Prezes Rady Ministrów. Przy UKE powstaje też społeczna Krajowa Rada ds. Usług Cyfrowych.

Nowe „statusy" i certyfikacje:

- Certyfikacja podmiotów ADR (pozasądowe rozstrzyganie sporów) – certyfikuje UKE na 5 lat;
- Zaufane podmioty sygnalizujące – tryb nadawania i cofania statusu, coroczne sprawozdania, możliwe zawieszenie statusu; KE prowadzi publiczną bazę.
- Zweryfikowani badacze – UKE nadaje status do dostępu do danych bardzo dużych platform/wyszukiwarek na potrzeby badań ryzyk systemowych.

Adresaci usług mogą składać skargi do Prezesa UKE na naruszenia obowiązków z DSA; projekt przewiduje też roszczenia odszkodowawcze przeciw dostawcom usług pośrednich, z dedykowaną ścieżką sądową. Orzeczenia organów z obszaru DSA zaskarża się do SOKiK (SO Warszawa).

Aktualizowane są definicje (m.in. „usługa pośrednia", „platforma", „wyszukiwarka", „obrót").

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

2.2.Projekt ustawy z dnia 8 lipca 2025 r. o ogólnym bezpieczeństwie produktów

Status: Przekazano do Komisji Prawniczej – 21 lipca 2025 r.

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

Projekt ustawy ustanawia krajowe ramy stosowania rozporządzenia (UE) 2023/988 w sprawie ogólnego bezpieczeństwa produktów (GPSR). Ma charakter „proceduralny": nie tworzy nowych, równoległych wymogów technicznych wobec produktów, lecz wyznacza organy właściwe, tryby działania, instrumenty nadzorcze, zasady współpracy krajowej i unijnej oraz sankcje administracyjne.

Adresatami są producenci, importerzy, dystrybutorzy, upoważnieni przedstawiciele, dostawcy internetowych platform handlowych oraz dostawcy usług społeczeństwa informacyjnego. Centralną rolę otrzymuje Prezes UOKiK, który – wraz z wojewódzkimi inspektoratami Inspekcji Handlowej jako organami kontroli – tworzy system nadzoru rynku w obszarze GPSR.

Projekt przewiduje cykliczne, dwa razy do roku, ogłaszanie przez Prezesa PKN wykazu Polskich Norm transponujących normy europejskie uznane przez Komisję na potrzeby GPSR – co ułatwia przedsiębiorcom powoływanie się na „domniemanie bezpieczeństwa".

Wprowadzono także wymóg, aby instrukcje, ostrzeżenia i określone informacje dla konsumentów były dostępne w języku polskim.

Przewidziano „wystąpienia informacyjne" – możliwość zwrócenia się przez Prezesa UOKiK lub WIIH o wyjaśnienia bądź dokumenty bez wszczynania formalnego postępowania. Każdy będzie mógł przekazywać organowi informacje o produktach niebezpiecznych lub niezgodnych, a organ odpowie pisemnie. Kontrola obejmuje zarówno sprzedaż stacjonarną, jak i na odległość, z możliwością zdalnego sprawdzenia ofert oraz zakupu kontrolnego pod ukrytą tożsamością (także z rejestracją obrazu i dźwięku). Organy mogą żądać dokumentów dotyczących łańcucha dostaw i wbudowanego oprogramowania oraz pobierać próbki – w tym próbkę kontrolną.

W toku postępowań w sprawie produktów stwarzających podejrzenie „poważnego ryzyka" Prezes UOKiK uzyskuje kompetencję do natychmiastowego, tymczasowego zakazu udostępniania lub oferowania towaru. Decyzje merytoryczne mogą nakazywać usunięcie zagrożeń, doprowadzenie produktu do zgodności, zapewnienie właściwych ostrzeżeń po polsku, określać warunki udostępniania, a w razie potrzeby zarządzać wycofanie z obrotu, odzyskanie (recall) i środki naprawcze wobec konsumentów (naprawa, wymiana, zwrot ceny), a w skrajnych przypadkach – zakaz udostępniania lub zniszczenie. W relacjach z pośrednikami cyfrowymi projekt dopuszcza zobowiązanie dostawcy platformy do usunięcia treści lub wyświetlenia ostrzeżenia na interfejsie, a wobec dostawców usług społeczeństwa informacyjnego – nieodpłatne ograniczenie dostępu do interfejsu, jeśli podmiot oferujący produkt ignoruje decyzje organu. Przewidziano publikację treści decyzji Prezesa UOKiK (z poszanowaniem tajemnic ustawowo chronionych) wraz z informacją o ich prawomocności.

Projekt likwiduje dotychczasowe krajowe rejestry produktów niebezpiecznych – ich funkcję przejmują unijne narzędzia Safety Gate i ICSMS.

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. Wartość aktywów netto funduszy zdefiniowanej daty (PPK) wg stanu na koniec II kwartału 2025

Urząd Komisji Nadzoru Finansowego informuje, że w serwisie internetowym dostępny jest artykuł o wartości aktywów netto funduszy zdefiniowanej daty (PPK) wg stanu na koniec II kwartału 2025."

Źródło: knf.gov.pl/?articleId=94516&p_id=18

3.1.2. Dane miesięczne OFE – czerwiec 2025 rok

Urząd Komisji Nadzoru Finansowego informuje, że w serwisie internetowym dostępne są Dane miesięczne OFE za czerwiec 2025 roku.

Źródło: knf.gov.pl/?articleId=94514&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 lipiec 2025 r.

Źródło: mojeppk.pl/pliki/repozytorium-plikow/materialy-do-pobrania/pdf/Biuletyn-PPK-07-2025_-45-.pdf

Kontakt

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