SIERPIEŃ 2025

NEWSLETTER REGULACYJNY

BANKI
TOWARZYSTWA FUNDUSZY INWESTYCYJNYCH
POWSZECHNE TOWARZYSTWA EMERYTALNE
ZARZĄDZAJĄCY ASI
DOMY MAKLERSKIE
INSTYTUCJE PŁATNICZE
SPÓŁKI PUBLICZNE

KRZYSZTOF ROŻKO I WSPÓLNICY
KANCELARIA PRAWNA

WSTĘP

Szanowni Państwo,

pragniemy Państwa zaprosić do lektury sierpniowego numeru Newslettera Regulacyjnego przygotowanego przez Zespół Kancelarii Prawnej Krzysztof Rożko i Wspólnicy.

W niniejszym numerze, zapraszamy do zapoznania się ze zmianami ram prawnych rynku finansowego oraz inicjatywami podejmowanymi w obszarze prawa finansowego oraz nowych technologii.

W tym miesiącu w sposób szczególnych zwracamy Państwa uwagę na wejście w życie ustawy o zmianie ustawy o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, która wprowadziła ułatwienia w zakresie łączenia niepublicznych FIZ, a także na ostatnie zmiany w Prawie bankowym.

Z aktualnie toczących się procesów legislacyjnych, szczególne polecamy śledzić informacje, dotyczące prac związanych z planowanym podwyższeniem stawki podatku dochodowego dla podmiotów sektora bankowego, jak również dotyczące projektowanych zmian w zakresie opodatkowania fundacji rodzinnych.

W niniejszym numerze Newslettera wiele miejsca poświęcamy również aktualnym zagadnieniom z obszaru cyberbezpieczeństwa oraz ochrony danych osobowych.

Zachęcamy do obserwowania naszego profilu na LinkedIn oraz śledzenia informacji na naszej stronie internetowej, na której na bieżąco komentujemy zmiany w przepisach prawa.

Krzysztof Rożko

Wspólnik Zarządzający

oraz Zespół Kancelarii

§ SPIS TREŚCI

NASZE PUBLIKACJE MEDIALNE

Za co odpowiada depozytariusz w funduszu inwestycyjnym? – artykuł r. pr. Nikoli Jadwiszczak – Niedbałki, Wspólnika Kancelarii oraz r. pr. Bartosza Posłusznego opublikowany w dodatku merytorycznym gazety Rzeczpospolita w dniu 29 sierpnia 2025 r.

PROJEKTOWANE ZMIANY PRAWNE:

PROJEKT USTAWY O ZMIANIE USTAWY O PODATKU DOCHODOWYM OD OSÓB PRAWNYCH I USTAWY OD NIEKTÓRYCH INSTYTUCJI FINANSOWYCH

W dniu 29 sierpnia 2025 r. na stronie Rządowego Centrum Legislacji został opublikowany projekt ustawy o podatku dochodowym od osób prawnych i ustawy o podatku od niektórych instytucji finansowych.

Projektowana ustawa przewiduje podwyższenie stawki podatkowej od banków oraz spółdzielczych kas oszczędnościowo-kredytowych. W pewnym uproszczeniu, podatek dochodowy dla w/w podmiotów wynosić ma:

- w roku podatkowym rozpoczynającym się w 2026 r. – 30% podstawy opodatkowania,
- w roku podatkowym rozpoczynającym się w 2027 r. – 26% podstawy opodatkowania,
- w roku podatkowym rozpoczynającym się w 2028 r. i latach kolejnych – 23% podstawy opodatkowania.

Projektowana ustawa przewiduje również zmiany w ustawie z dnia 15 stycznia 2016 r. o podatku od niektórych instytucji finansowych, polegające na obniżeniu stawki tego podatku w odniesieniu do podatników, o których mowa w art. 4 pkt 1-4 tej ustawy, do poziomu 0,0293 % podstawy opodatkowania miesięcznie. W tym zakresie nowelizacja ma wejść w życie z dniem 1 stycznia 2027 r.

W zakresie zmian w ustawie o podatku dochodowym od osób prawnych, projektowana ustawa ma wejść w życie z dniem 1 stycznia 2026 r.

Projekt ustawy dostępny jest pod linkiem.

PROJEKT USTAWY O ZMIANIE USTAWY O PODATKU DOCHODOWYM OD OSÓB PRAWNYCH – ZMIANY W ZAKRESIE OPODATKOWANIA FUNDACJI RODZINNYCH

W dniu 29 sierpnia 2025 r. na stronie Rządowego Centrum Legislacji został opublikowany projekt ustawy o zmianie ustawy o podatku dochodowym od osób prawnych.

Zgodnie z uzasadnieniem, projektowana ustawa stanowić ma odpowiedź na zidentyfikowane mechanizmy wykorzystywania fundacji rodzinnych niezgodnie z celem ustawy o fundacji rodzinnej, wyłączenie w celu uzyskaniu korzyści podatkowych – takich jak odroczenie momentu opodatkowania, całkowite zwolnienie z podatku, czy też obniżenie jego wysokości.

Główne założenia projektu ustawy obejmują:

a) wprowadzenie 3-letniego ograniczenia podatkowego (tzw. „lock-up”) na zbycie wniesionych aktywów,

b) objęcie fundacji rodzinnej opodatkowaniem z tytułu udziału w kontrolowanej jednostce zagranicznej (CFC),

c) doprecyzowanie opodatkowania udziałów w podmiotach zagranicznych transparentnych podatkowo,

d) wyłączenie z preferencji podatkowych dochodów z najmu krótkoterminowego.

Zmiany ustawy o fundacjach rodzinnych mają wejść w życie od początku 2026 roku, a ich zakres ma objąć zarówno nowo zakładane fundacje rodzinne, jak i te istniejące obecnie.

Co istotne 3-letni okres lock up ma mieć zastosowanie także do mienia wniesionego lub przekazanego nieodpłatnie do fundacji rodzinnej lub nabytego przez fundację rodzinną od podmiotu powiązanego, po dniu 31 sierpnia 2025 r.

Projekt ustawy dostępny jest pod linkiem.

ZAŁOŻENIA PROJEKTU USTAWY O OSOBISTYCH KONTACH INWESTYCYJNYCH

W dniu 2 września 2025 r. na stronie Kancelarii Prezes Rady Ministrów zostały opublikowane założenia projektu ustawy o osobistych kontach inwestycyjnych (tzw. „**OKI**”)

Projektowana ustawa ma na celu aktywizację oszczędności gospodarstw domowych, celem ich wykorzystania dla zaspokojenia potrzeb finansowych przedsiębiorstw. Powszechne wykorzystanie OKI ma również zwiększyć płynność rynku kapitałowego.

Jak wskazano w uzasadnieniu, stopa oszczędności w Polsce pozostaje jedną z najniższych w UE i OECD - w I kwartale 2024 r. wyniosła 2,41% wobec średniej unijnej 13,26% (Eurostat). Spowodowane jest to nadmierną alokacją środków finansowych w depozytach bankowych i lokatach o realnym oprocentowaniu bliskim zeru. Na koniec 2024 r. Polacy zgromadzili niemal 1,75 bln zł w formie depozytów bankowych i gotówki, podczas gdy udział inwestycji w instrumenty finansowe o wyższej dochodowości, takie jak akcje, czy obligacje korporacyjne wyniósł ok. 0,6 bln zł (NBP, Eurostat).

OKI ma być przeznaczone dla osób fizycznych i charakteryzować się następującymi cechami:

a) OKI ma być osobiste i dobrowolne, z możliwością wpłaty i wypłaty środków pieniężnych w każdej chwili,

b) aktywa w ramach konta mają być zwolnione z opodatkowania do wartości 100 tys. zł w tym:

- aktywa o charakterze inwestycyjnym (akcje, obligacje i inne instrumenty finansowe dopuszczone do obrotu na rynku regulowanym lub wprowadzone do alternatywnego systemu obrotu, fundusze inwestycyjne) mają korzystać ze zwolnienia w pełnej wysokości (tj. do kwoty 100 tys. zł),

- aktywa o charakterze oszczędnościowym (środki pieniężne, lokaty, obligacje oszczędnościowe) mają korzystać ze zwolnienia do wartości 25 tys. zł.

Nadwyżka wartości aktywów zgromadzonych na OKI ponad limity zwolnione z opodatkowania (tj. 25 tys. zł dla części oszczędnościowej oraz 100 tys. zł dla całości aktywów) podlegać ma opodatkowaniu o szacunkowej stopie wynoszącej od 0,8% do 0,9%.

Na instytucje finansowe prowadzące OKI ma być nałożony obowiązek przekazywania, zarówno oszczędzającemu, jak i organom podatkowym, informacji o wysokości wartości aktywów oraz wpłat na OKI.

Założenia projektu ustawy dostępne są pod linkiem.

PROJEKT USTAWY O SYSTEMACH SZTUCZNEJ INTELIGENCJI ZOSTAŁ PRZYJĘTY PRZEZ KOMITET DO SPRAW EUROPEJSKICH

W dniu 22 sierpnia 2025 r. na stronie Rządowego Centrum Legislacji opublikowano informację o przyjęciu w dniu 4 lipca 2025 r. przez Komitet do Spraw Europejskich projektu ustawy o systemach sztucznej inteligencji.

Jednocześnie opublikowano najnowszą wersję projektu - z dnia 18 sierpnia 2025 r.

Przypomnieć należy, że będący aktualnie w procesie legislacyjnym projekt ma na celu zapewnić stosowanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. 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 również „AI Act". Jest to pierwszy unijny akt, który w sposób kompleksowy reguluje zagadnienie sztucznej inteligencji. Rozpoczęcie stosowania rozporządzenia zostało podzielone na cztery etapy – pierwszy z nich rozpoczął się 2 lutego 2025 r., a r drugi – 2 sierpnia 2025.

Projektowana ustawa ma uregulować takie kwestie, jak organizacja i sposób sprawowania nadzoru nad rynkiem systemów AI i modelami AI ogólnego przeznaczenia, postępowanie ws. naruszenia AI Act i projektowanej ustawy, zasady akredytacji oraz notyfikacji jednostek oceniających zgodność, zgłaszanie poważnych incydentów zaistniałych w związku z wykorzystaniem systemów AI, działania wspierające rozwój systemów AI, a także kary administracyjne za naruszenie AI Act.

Zgodnie z projektem ustawa ma wejść w życie po upływie 14 dni od dnia ogłoszenia, z pewnymi wyjątkami.

Z treścią projektu można zapoznać się pod linkiem.

PROJEKT USTAWY O SPRAWIEDLIWYM DOSTĘPIE DO DANYCH I ICH WYKORZYSTYWANIU

W dniu 11 sierpnia 2025 r. na stronie Kancelarii Prezesa Rady Ministrów opublikowane zostały założenia projektu ustawy (UC114) mającej na celu wdrożenie w Polsce rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854, znanego jako **Data Act (DA)**. Unijny akt prawny, który zacznie obowiązywać 12 września 2025 r., ustanawia ramy prawne dla sprawiedliwego dostępu do danych i ich

wykorzystywania, a także reguluje interoperacyjność usług chmurowych i mechanizmy wymiany danych pomiędzy przedsiębiorstwami, konsumentami oraz administracją publiczną.

Choć DA stosowane będzie bezpośrednio we wszystkich państwach członkowskich, unijny prawodawca pozostawił krajom pewien zakres swobody – w szczególności w zakresie ukształtowania otoczenia instytucjonalnego i regulacyjnego. Polska musi więc przyjąć przepisy, które umożliwią pełne wdrożenie i egzekwowanie nowych zasad.

Nowa ustawa zamiast nowelizacji

Projektodawca wskazał, że obecny system prawny nie przewiduje rozwiązań odpowiadających wszystkim mechanizmom DA. Dlatego rekomendowanym rozwiązaniem jest uchwalenie **nowej ustawy o sprawiedliwym dostępie do danych i ich wykorzystywaniu**. W ustawie znajdą się przepisy proceduralne, organizacyjne oraz dotyczące sankcji administracyjnych, które zostały wprost powierzone państwom członkowskim.

Struktura instytucjonalna

Kluczowym elementem projektu jest wyznaczenie **Prezesa Urzędu Komunikacji Elektronicznej (UKE)** jako:

- **właściwego organu** odpowiedzialnego za stosowanie i egzekwowanie przepisów DA,
- **koordynatora danych**, pełniącego rolę punktu kontaktowego dla podmiotów korzystających z regulacji,
- **organu certyfikującego** instytucje rozstrzygające spory dotyczące dostępu do danych.

Do zadań Prezesa UKE należeć ma m.in. rozpatrywanie skarg, prowadzenie postępowań administracyjnych, nakładanie kar pieniężnych, a także współpraca z organami w innych państwach UE, Komisją Europejską i Europejską Radą ds. Innowacji w zakresie Danych (EDIB). Organ ma również monitorować rynek usług przetwarzania danych, promować wiedzę o prawach i obowiązkach użytkowników oraz pośredniczyć w procesach związanych z dostępem administracji publicznej do danych prywatnych.

Regulacje proceduralne i sankcje

Projektowana ustawa przewiduje przepisy proceduralne powiązane z kompetencjami Prezesa UKE, a także system **administracyjnych kar pieniężnych** za naruszenie DA. Konstrukcja sankcji wzorowana jest na dotychczasowych rozwiązaniach z prawa komunikacji elektronicznej oraz kodeksu postępowania administracyjnego, co ma zapewnić spójność i przewidywalność systemu.

Znaczenie dla rynku

Data Act wprowadzi jednolite, przejrzyste zasady dotyczące wykorzystania danych w Unii Europejskiej. Dla przedsiębiorstw i konsumentów oznacza to łatwiejszy dostęp do danych generowanych przez urządzenia i usługi cyfrowe, możliwość zmiany dostawcy chmury bez dodatkowych opłat oraz większą ochronę przed nieuczciwym ograniczaniem dostępu do informacji. Z kolei administracja publiczna zyska nowe narzędzia pozwalające na korzystanie z danych prywatnych w sytuacjach wyjątkowych, przy zachowaniu gwarancji ochrony interesów gospodarczych i prywatności.

Zgodnie z komunikatem, planowany termin przyjęcia projektu przez Radę Ministrów do IV kwartał 2025 r.

Założenia opublikowane zostały na stronie KPRM pod linkiem.

NOWY PROJEKT USTAWY O ZMIANIE USTAWY – KODEKS SPÓŁEK HANDLOWYCH ORAZ NIEKTÓRYCH INNYCH USTAW – DALSZE DOSTOSOWANIE REGULACJI DO ZMIAN BĘDĄCYCH SKUTKIEM DEMATERIALIZACJI

W dniu 2 września 2025 r. na stronie Rządowego Centrum Legislacji został opublikowany nowy, datowany na dzień 13 sierpnia 2025 r., projekt ustawy o zmianie ustawy – Kodeks spółek handlowych oraz niektórych innych ustaw.

Przypomnieć należy, iż od 1 marca 2021 r. obowiązują przepisy, które regulują powszechną i obligatoryjną dematerializację wszystkich akcji spółek niepublicznych. Celem projektowanych zmian jest usprawnienie wdrożonych rozwiązań w związku ze zwiększeniem bezpieczeństwa obrotu.

Projekt przewiduje m.in.:

- rezygnację z dotychczasowej klasyfikacji na akcje imienne i na okaziciela,
- ujawnianie informacji o podmiocie prowadzącym rejestr akcjonariuszy spółki w Krajowym Rejestrze Sądowym (w przypadku braku zgłoszenia zawarcia umowy z podmiotem prowadzącym rejestr, sąd rejestrowy będzie uprawniony do wszczęcia postępowania przymuszającego do złożenia wniosku o wpis),
- zamieszczenie w rejestrze akcjonariuszy, obok dotychczasowych danych, numeru PESEL albo daty urodzenia akcjonariuszy, a w przypadku osoby niebędącej osobą fizyczną – firmy, numer akcjonariusza we właściwym rejestrze oraz nazwy tego rejestru. Jednocześnie, projekt przewiduje, że informacje o numerze PESEL, dacie urodzenia lub adresie zamieszkania akcjonariusza nie będą udostępniane pozostałym akcjonariuszom,
- nałożenie na zarząd spółki obowiązku zgłaszanych aktualnych danych jej dotyczących w terminie 7 dni od dnia zdarzenia uzasadniającego dokonanie wpisu, pod rygorem nałożenia grzywny,
- wprowadzenie wymogu, aby zgoda na dokonanie wpisu, wyrażona przez osobę, której uprawnienia mają być wykreślone, było składa w formie pisemnej z podpisem notarialnie poświadczonym albo w formie pisemnej w obecności osoby upoważnionej przez podmiot prowadzący rejestr akcjonariuszy albo w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

Zgodnie z projektem, spółki, dla których w dniu wejścia w życie nowelizacji, prowadzony jest rejestr akcjonariuszy albo ich akcje zostały zarejestrowane w depozycie papierów wartościowych, powinny złożyć wniosek o wpis informacji o danym podmiocie ewidencjonującym akcje, w terminie 3 miesięcy od dnia wejścia w życie projektowanej ustawy.

Z nielicznymi wyjątkami, przepisy ustawy mają wejść w życie po upływie 8 miesięcy od dnia ogłoszenia.

Treść projektu ustawy dostępna jest pod linkiem.

PROJEKT USTAWY O ZMIANIE USTAWY O PAŃSTWOWEJ INSPEKCJI PRACY ORAZ NIEKTÓRYCH INNYCH USTAW

W dniu 1 września 2025 r. na stronie Rządowego Centrum Legislacji został opublikowany projekt ustawy o zmianie ustawy o Państwowej Inspekcji Pracy oraz niektórych innych ustaw.

Celem projektowanej ustawy jest wyposażenie Państwowej Inspekcji Pracy w narzędzia umożliwiające bardziej efektywne i skuteczne przestrzeganie przepisów prawa pracy, w postaci uprawnienia do stwierdzenia przez PIP istnienia stosunku pracy w sytuacji, kiedy zawarto umowę cywilnoprawną w warunkach, w których, w świetle art. 22 Kodeksu pracy, powinna być zawarta umowa o pracę.

Zgodnie z projektem, nowe przepisy miałyby obowiązywać od 1 stycznia 2026 r.

Treść projektu dostępna jest pod linkiem.

PROJEKT USTAWY O FUNDUSZU ROZWOJU TECHNOLOGII PRZEŁOMOWYCH

W dniu 1 września 2025 r. na stronie Sejmu RP został opublikowany przedstawiony przez Prezydenta Rzeczypospolitej Polskiej projekt ustawy o Funduszu Rozwoju Technologii Przełomowych.

Projektowana ustawa zakłada utworzenie Funduszu Rozwoju Technologii Przełomowych, którego działanie miałoby być nakierowane na wzmacnianie bezpieczeństwa państwa, w szczególności w zakresie realizacji i wdrażania strategii bezpieczeństwa narodowego, poprzez wspieranie polskiej nauki, administracji, gospodarki i społeczeństwa w rozwijaniu technologii przełomowych.

Projekt zakłada wydzielenie pięciu subfunduszy: naukowo-badawczego, nowoczesnej administracji, bezpieczeństwa cyberprzestrzeni, edukacyjno-popularyzatorskiego oraz wsparcia innowacyjnej gospodarki.

Katalog inicjatyw, które mają być wspierane przez fundusz obejmuje:

- prowadzenie prac badawczych i wdrożeniowych z obszaru technologii przełomowych oraz wdrażanie, w tym poprzez komercjalizację i popularyzację ich wyników,
- transformację cyfrową podmiotów wykonujących zadania publiczne i wdrażanie nowych rozwiązań technicznych służących zwiększeniu efektywności realizacji tych zadań,
- ekspansję zagraniczną przedsiębiorców oraz umiędzynarodowienie prowadzenia badań naukowych,
- poprawę bezpieczeństwa cyberprzestrzeni RP,
- wsparcie rozwoju społeczeństwa informacyjnego, zwiększanie poziomu dostępności cyfrowej oraz przeciwdziałanie wykluczeniu cyfrowemu,
- wsparcie rzetelnej i profesjonalnej edukacji z zakresu nowych technologii, higieny cyfrowej i medialnej, cyberbezpieczeństwa, innowacji, etyki nowych technologii oraz przedsiębiorczości na wszystkich etapach kształcenia,

- rozwój zaplecza infrastrukturalnego jednostek systemu oświaty, podmiotów systemu szkolnictwa wyższego i nauki, podmiotów wykonujących zadania publiczne oraz przedsiębiorców działających w sektorze technologii przełomowych,

- działalność edukacyjną i popularyzatorską z zakresu technologii przełomowych oraz innych nowych technologii, innowacyjności, nauki i transformacji cyfrowej.

Na wspieranie ww. inicjatyw Funduszu ma być przeznaczane do 5 miliardów zł rocznie, z wyjątkiem roku 2026, na który przewidziano kwotę o połowę niższą.

Projekt w dniu 2 września 2025 r. został skierowany do zaopiniowania przez Biuro Legislacyjne oraz Biuro Ekspertyz i Oceny Skutków Regulacji oraz do konsultacji społecznych.

Ustawa ma wejść w życie po upływie 30 dni od dnia ogłoszenia.

Z treścią projektu można zapoznać się pod linkiem.

PROJEKT USTAWY O SZCZEGÓLNYCH ROZWIĄZANIACH SŁUŻĄCYCH REALIZACJI USTAWY BUDŻETOWEJ NA ROK 2026

W dniu 29 sierpnia 2025 r. na stronie Rządowego Centrum Legislacji opublikowano projekt ustawy o szczególnych rozwiązaniach służących realizacji ustawy budżetowej na rok 2026, czyli tzw. ustawy okołobudżetowej. Ustawa okołobudżetowa ma zapewnić prawidłową realizację ustawy budżetowej na 2026 r.

Zgodnie z opublikowanym projektem, zakłada się odmrożenie podstawy wymiaru wynagrodzeń członków zarządzających i organów nadzorczych, o której mowa w art. 1 ust. 3 pkt 11 ustawy z dnia 9 czerwca 2016 r. o zasadach kształtowania wynagrodzeń osób kierujących niektórymi spółkami, która w 2026 r. ma wynosić 4 535,89 zł.

Natomiast podstawa ustalania maksymalnej wysokości wynagrodzenia miesięcznego, o którym mowa w art. 8 ustawy z dnia 3 marca 2000 r. o wynagradzaniu osób kierujących niektórymi podmiotami prawnymi, ma wynieść 6 116,35 zł.

Projekt ma również regulować kwestię upoważnienia Ministra Finansów do przekazywania na polecenie Prezesa Rady Ministrów, skarbowych papierów wartościowych państwowym osobom prawnym w celu finansowania ich dzielności bieżącej i inwestycji, w ramach limitu wynoszącego 1.000.000.000,00 zł.

Projektowana ustawa ma wejść w życie z dniem 1 stycznia 2026 r.

Z treścią projektu można zapoznać się pod linki8em.

PROJEKT USTAWY O ZMIANIE USTAWY O KSIĘGACH WIECZYSTYCH I HIPOTECE ORAZ USTAWY O KRAJOWYM REJESTRZE SĄDOWYM

W dniu 22 sierpnia 2025 r. na stronie Kancelarii Prezesa Rady Ministrów opublikowano założenia ustawy o zmianie ustawy o księgach wieczystych i hipotece oraz ustawy o Krajowym Rejestrze Sądowym (numer projektu: UDER89). Projektowane przepisy są częścią rozwiązań deregulacyjnych.

Projekt przewiduje:

1) możliwość wydawania dokumentów elektronicznych przez Centralną Informację Ksiąg Wieczystych tak, aby nie tylko wydruki odpisu ksiąg wieczystych, wyciągi z ksiąg wieczystych oraz zaświadczenia o zamknięciu ksiąg wieczystych dokonywane za pośrednictwem systemu teleinformatycznego miały moc dokumentów wydawanych przez sąd, ale przede wszystkim moc taką przypisać dokumentom elektronicznym generowanym przez system teleinformatyczny,

2) możliwość wyszukiwania w aplikacji mobilnej mObywatel ksiąg wieczystych po numerze PESEL oraz danych z Krajowego Rejestru Sądowego dotyczących podmiotu wpisanego do rejestru, co ułatwi i usprawni przeglądanie ww. baz danych.

Aplikacja mObywatel zyskać ma dwie nowe funkcjonalności. Za pomocą numeru PESEL użytkownik będzie mógł ustalić numer ksiąg wieczystych, w których ujawniony jest jako właściciel nieruchomości. W analogiczny sposób możliwe będzie ustalenie danych podmiotów w Krajowym Rejestrze Sądowym (rejestrze przedsiębiorców lub rejestrze stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej), z którymi dany użytkownik aplikacji jest powiązany przez PESEL.

Planowana data wejścia w życie ustawy to 31 marca 2026 r. Termin wynika z założeń przedsięwzięcia „Rozwój i zwiększenie dostępności Rejestrów Sądowych - eKRS i EKW", które znalazło się na liście projektów indykatywnych do Inwestycji C2.1.1 Krajowego Planu Odbudowy i Zwiększania Odporności oraz pozwoli na przeprowadzenie procesu legislacyjnego w zakresie niezbędnych nowelizacji aktów wykonawczych wydawanych na podstawie przepisów, których zmianę przewiduje się w projekcie.

Planowany termin przyjęcia projektu przez Radę Ministrów to III kwartał 2025 r.

Więcej informacji można znaleźć pod linkiem.

PROJEKT USTAWY O ZMIANIE USTAWY O DORĘCZENIACH ELEKTRONICZNYCH ORAZ NIEKTÓRYCH INNYCH USTAW

W dniu 22 sierpnia 2025 r. na stronie Rządowego Centrum Legislacji opublikowano projekt ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw. Nowelizacja ma na celu usprawnienia i rozwój funkcjonowania e-Doręczeń, doprecyzowanie aktualnie obowiązujących przepisów oraz wyeliminowanie wątpliwości dotyczących stosowania ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.

Projekt zakłada liczne zmiany, w tym zaklasyfikowanie publicznej usługi e-Doręczeń jako kwalifikowanej usługi rejestrowanego doręczenia elektronicznego oraz rozszerzenie zakresu fikcji doręczenia, która ma objąć również doręczenia między podmiotami niepublicznymi – oznacza to, że w korespondencji pomiędzy

podmiotami niepublicznymi, w przypadku nieodebrania przesyłki w terminie 14 dni od jej wpływu, przesyłka ma być uznawana za skutecznie doręczoną.

W projekcie określono również zasady prowadzenia przez ministra właściwego do spraw informatyzacji Katalogu Podmiotów Publicznych (KPP), zawierającego dane o podmiotach publicznych i podmiotach niepublicznych realizujących zadania publiczne. KPP ma na celu zapewnić wymianę danych i współpracę między KPP a systemami administracji publicznej, a także poprawę dostępności tych danych.

Zmianie mają ulec również przepisy regulujące kwestię e-Doręczeń w przypadku osób wykonujących zawód zaufania publicznego oraz podmiotów niepublicznych wpisanych do KRS i CEiDG, którzy mają być zobowiązani do wymiany korespondencji z podmiotami publicznymi z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub kwalifikowanej usługi rejestrowanego doręczenia elektronicznego (a zatem również do wysyłanie korespondencji - aktualnie obowiązek ten dotyczy jedynie jej odbierania). W przypadku osób wykonujących zawód zaufania publicznego zmieniony ma zostać również zakres informacji wymaganych przy zakładaniu skrzynki do e-Doręczeń.

Zgodnie z projektem zmianie mają ulec również przepisy przejściowe, m.in. ma zostać skrócony termin wymiany korespondencji przez e-PUAP między podmiotami publicznymi (z 30 września 2029 r. do 1 stycznia 2028 roku).

Wspomnieć również należy, że nowelizacja ma objąć ustawę z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, poprzez wprowadzenie wymogu podawanie numeru PESEL w pierwszym piśmie w sprawie, celem identyfikacji adresu do e-Doręczeń strony postępowania administracyjnego.

Projekt został skierowany do uzgodnień, konsultacji publicznych i opiniowania w dniu 22 sierpnia 2025 r. Uwagi do projektu można zgłaszać w terminie 30 dni.

Projektowana ustawa ma wejść w życie po upływie 14 dnia od dnia ogłoszenia, z zastrzeżeniem pewnych wyjątków.

Z treścią projektu można zapoznać się pod linkiem.

PROJEKT UCHWAŁY RADY MINISTRÓW W SPRAWIE PRZYJĘCIA STRATEGII PRZECIWDZIAŁANIA PRANIU PIENIĘDZY ORAZ FINANSOWANIU TERRORYZMU

W dniu 26 sierpnia 2025 r. na stronie Kancelarii Prezesa Rady Ministrów zostały opublikowane założenia projektu uchwały Rady Ministrów w sprawie przyjęcia strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Celem projektu uchwały jest realizacja obowiązku określonego w art. 31 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu („**Ustawa AML**"). Zgodnie z ww. przepisem Generalny Inspektor Informacji Finansowej („**GIIF**"), na podstawie krajowej oceny ryzyka, opracowuje projekt strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, zawierający plan działań ukierunkowanych na ograniczenie ryzyka związanego z praniem pieniędzy oraz finansowaniem terroryzmu.

Projekt zakłada przedstawienie i realizację planu działań, zmierzających do usprawnienia funkcjonowania krajowego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, zgodnie z przewidzianymi terminami.

W założeniu, realizacja celów zawartych w strategii umożliwić ma wykorzystanie przez instytucje i organy posiadanych zasobów, a także pozwolić na osiągnięcie efektu synergii w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

Uwzględnione w projekcie strategii rozwiązania mają przyczyniać się do realizacji poniższych priorytetów:

- harmonizacja i rozwój zasad nadzoru i kontroli nad instytucjami obowiązanymi,
- wdrożenie skutecznego systemu szkoleń i wymiany doświadczeń AML/CFT,
- przegląd i optymalizacja dostępu, trybu, zakresu i jakości wymiany informacji,
- wzmocnienie i zwiększenie skuteczności działania i analiz prowadzonych przez jednostki analityki finansowej (tj. Ministra Finansów jako naczelny organ i GIIF) i jednostki współpracujące zgodnie z zasadami podejścia opartego na ryzyku,
- wzmocnienie struktur przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (dalej „AML/CFT") w instytucjach obowiązanych poprzez przeciwdziałanie zidentyfikowanym ryzykom i wsparcie eksperckie,
- modyfikacja prawa krajowego w związku z identyfikacją nowych ryzyk i lokalnych potrzeb z obszaru AML/CFT oraz konieczności harmonizacji prawa krajowego z prawem UE i innymi standardami międzynarodowymi.

Założenia projektu strategii dostępne są pod linkiem.

W NASZEJ OPINII

DORA – I CO DALEJ?

Rozporządzenie DORA jest stosowane od niemal 9 miesięcy.

Na przełomie 2024 oraz 2025 r. instytucje finansowe mierzyły się z koniecznością wdrożenia nowych wymogów w zakresie odporności cyfrowej.

Jednak samo przygotowanie polityk i procedur oraz wypełnienie odpowiednich rejestrów to dopiero początek – prawdziwym wyzwaniem jest utrzymanie i rozwijanie raz zbudowanego systemu zarządzanie bezpieczeństwem informacji.

Jakie najważniejsze obowiązki związane z utrzymaniem ram zarządzania ryzykiem ICT czekają podmioty finansowe w najbliższym czasie?

Obowiązki raportowe

DORA zawiera szereg obowiązków raportowych, takich jak:

- zgłoszenia zawieranych umów z zewnętrznymi dostawcami usług ICT (art. 28 ust. 3 DORA, formularz SPR-PF-20),
- zestawienia wszystkich ustaleń umownych z zewnętrznymi dostawcami usług ICT (art. 28 ust. 3 DORA, formularz SPR-PF-19),
- raportowanie dot. incydentów związanych z ICT:
  - sprawozdanie dot. rocznych kosztów i strat spowodowanych poważnymi incydentami (art. 11 ust. 10 DORA, formularz SPR-PF-04),
  - wstępne powiadomienie i sprawozdanie dotyczące poważnych incydentów ICT (w szczególności art. 19 ust. 1 DORA, formularz SPR-PF-07),
  - sprawozdanie śródokresowe dotyczące poważnych incydentów ICT (formularz SPR-PF-08),
  - sprawozdanie końcowe dotyczące poważnych incydentów ICT (formularz SPR-PF-09),
- sprawozdanie dot. informacji o zmianach wprowadzonych w następstwie przeglądu po poważnym incydencie związanym z ICT (art. 13 ust. 2 DORA, formularz SPR-PF-05).

Szczególne znaczenie mają jednak obowiązki sprawozdawcze związane z Kluczowymi Wskaźnikami Ryzyka (KRI) dla obszaru ICT. Każdy podmiot finansowy jest zobowiązany do składania kwartalnych (SPR-PF-26) oraz rocznych (SPR-PF-27) ankiet KRI, które pozwolą nadzorcy na systematyczną ocenę poziomu ryzyka technologicznego w sektorze. Raporty te obejmą m.in. dane o incydentach, skuteczności stosowanych mechanizmów bezpieczeństwa, dostępności systemów, a także informacje dotyczące outsourcingu usług ICT.

Kwartalne raporty mają zapewnić bieżący obraz stanu bezpieczeństwa i umożliwić szybką identyfikację trendów lub narastających zagrożeń. Raport roczny stanowi natomiast podsumowanie całego okresu sprawozdawczego, pozwalając KNF oraz europejskim organom nadzoru na prowadzenie pogłębionych analiz porównawczych i wyznaczanie kierunków działań prewencyjnych. Dane te będą przekazywane w jednolitym formacie cyfrowym, co ułatwi ich automatyczne przetwarzanie i integrację na poziomie UE. Regularne raportowanie KRI ma zatem nie tylko charakter nadzorczy, lecz także strategiczny – tworzy podstawę do budowania odporności operacyjnej w całym sektorze finansowym.

Audyty

Rozporządzenie DORA nakłada na podmioty finansowe obowiązek prowadzenia regularnych audytów wewnętrznych w obszarze zarządzania ryzykiem ICT. Celem audytów jest niezależna i obiektywna ocena skuteczności wdrożonych ram bezpieczeństwa, procedur oraz mechanizmów kontroli. Instytucje finansowe muszą zapewnić, aby audyty obejmowały całość procesów ICT, w tym zarządzanie incydentami, ciągłość działania, współpracę z dostawcami zewnętrznymi oraz stosowanie testów odporności.

Zgodnie z art. 6 ust. 6 DORA, ramy zarządzania ryzykiem związanym z ICT podmiotów finansowych innych niż mikroprzedsiębiorstwa powinny być regularnie poddawane audytowi wewnętrznemu przeprowadzanemu przez audytorów zgodnie z planami tych podmiotów finansowych, dotyczącymi audytów. Audytorzy powinni posiadać wystarczającą wiedzę, umiejętności i wiedzę fachową w zakresie ryzyka związanego z ICT oraz cechować się odpowiednią niezależnością. Częstotliwość i przedmiot audytów ICT powinny współmierne do ryzyka związanego z ICT danego podmiotu finansowego. Powyższe oznacza, że każdy podmiot finansowy powinien indywidualnie ocenić, jak często przeprowadzać audyty wewnętrzne swoich ram zarządzania ryzykiem, jednak decyzja zawsze oparta jest o wyniki analizy ryzyka związanego z ICT. Ogólnie przyjętą praktyką jest przeprowadzanie audytów wewnętrznych w zakresie systemu zarządzania bezpieczeństwem informacji co najmniej raz w roku.

Mikroprzedsiębiorstwa zostały wyłączone z obowiązku przeprowadzania regularnych audytów wewnętrznych swoich ram zarządzania ryzykiem ICT, jednak wciąż na mocy art. 6 ust. 5 DORA zobowiązane są do przeprowadzania okresowych przeglądów – „Ramy zarządzania ryzykiem związanym z ICT powinny być dokumentowane i poddawane przeglądowi co najmniej raz w roku, lub okresowo w przypadku mikroprzedsiębiorstw (…)".

Audyt wewnętrzny powinien być prowadzony w cyklach regularnych, zgodnie z przyjętym planem audytowym, ale także w przypadku istotnych zmian w infrastrukturze lub po wystąpieniu poważnych incydentów. Wyniki audytów muszą być dokumentowane i raportowane do organów nadzorczych na żądanie, a także wykorzystywane do wdrażania działań naprawczych i doskonalenia systemu bezpieczeństwa. DORA podkreśla wymóg niezależności funkcji audytu, co oznacza, że kontrola powinna być prowadzona przez jednostkę odrębną od obszarów operacyjnych. W praktyce audyty stają się kluczowym narzędziem zapewnienia zgodności i ciągłego podnoszenia odporności cyfrowej instytucji finansowych.

Przeglądy

Rozporządzenie DORA nakłada na instytucje finansowe obowiązek cyklicznych przeglądów ram zarządzania ryzykiem ICT, które mają zapewnić ich aktualność, skuteczność i zgodność z wymogami regulacyjnymi. Przeglądy powinny obejmować m.in. polityki bezpieczeństwa, procedury reagowania na incydenty, plany ciągłości działania, a także mechanizmy monitorowania usług dostawców zewnętrznych. W zależności od kategorii podmiotu przewidziano różne formy – pełne (SPR-PF-02) lub uproszczone (SPR-PF-06).

Przeglądy w zakresie pełnych ram zarządzania ryzykiem związanym z ICT uregulowane zostały m.in. w ramach art. 6 ust. 5 DORA – ramy zarządzania ryzykiem związanym z ICT powinny być dokumentowane i poddawane **przeglądowi** co najmniej raz w roku, lub okresowo w przypadku mikroprzedsiębiorstw, a także w przypadku wystąpienia poważnych incydentów związanych z ICT oraz zgodnie z instrukcjami nadzorczymi lub wnioskami wynikającymi z odpowiednich testów lub procesów audytu operacyjnej odporności cyfrowej, powinny być one stale ulepszane na podstawie wniosków płynących z wdrażania i monitorowania. Sprawozdanie z przeglądu ram zarządzania ryzykiem związanym z ICT należy przedłożyć właściwemu organowi na jego żądanie.

DORA wymaga, by przeglądy były prowadzone regularnie, co najmniej raz do roku, a także każdorazowo po istotnych incydentach lub zmianach technologicznych. Wyniki muszą być dokumentowane, raportowane na żądanie organów nadzoru i przekładane na konkretne działania naprawcze. Szczególną rolę przypisano organom zarządzającym, które odpowiadają za nadzorowanie procesu i wdrażanie zaleceń wynikających z przeglądów. W praktyce obowiązki te mają zagwarantować, że systemy bezpieczeństwa instytucji nie tylko spełniają wymogi formalne, lecz także stale odpowiadają na ewoluujące zagrożenia cybernetyczne.

Kontrole nadzorcze

Rozporządzenie DORA znacząco wzmacnia uprawnienia organu nadzoru, w zakresie kontroli operacyjnej odporności cyfrowej podmiotów finansowych. Nadzór może prowadzić zarówno kontrole planowe, jak i doraźne – w siedzibach instytucji, a także w formie zdalnej. Zakres obejmuje m.in. weryfikację ram zarządzania ryzykiem ICT, raportowania incydentów, planów ciągłości działania oraz umów z dostawcami zewnętrznymi.

Podmioty finansowe są zobowiązane do udostępniania wszelkiej dokumentacji, danych i systemów niezbędnych do przeprowadzenia kontroli. W toku działań nadzorczych mogą być żądane dodatkowe raporty (np. SPR-PF-23 i SPR-PF-24), a w przypadku stwierdzenia naruszeń – nakładane środki naprawcze lub sankcje. DORA przewiduje również współpracę krajowych organów z europejskimi urzędami nadzoru, co umożliwia prowadzenie skoordynowanych kontroli transgranicznych. W praktyce oznacza to istotne zwiększenie transparentności działań instytucji finansowych oraz konieczność utrzymywania pełnej gotowości do weryfikacji zgodności z wymogami regulacyjnymi.

Incydenty związane z ICT

DORA nakłada na podmioty finansowe szczegółowe obowiązki w zakresie obsługi incydentów ICT, kładąc nacisk na szybkie wykrywanie, klasyfikację i raportowanie zdarzeń. Instytucje muszą wdrożyć procedury umożliwiające natychmiastową identyfikację poważnych incydentów oraz ich ocenę pod kątem wpływu na działalność i klientów. Kluczowe jest obowiązkowe zgłaszanie poważnych incydentów do organu nadzoru – wstępne powiadomienie (SPR-PF-07) powinno zostać przekazane w ciągu 4 godzin od klasyfikacji zdarzenia, a następnie raport śródokresowy (SPR-PF-08) w ciągu 72 godzin i raport końcowy (SPR-PF-09) maksymalnie w ciągu miesiąca.

Oprócz tego instytucje mogą dobrowolnie raportować znaczące cyberzagrożenia (SPR-PF-10), co wspiera wymianę informacji w sektorze. Obowiązki obejmują także dokumentowanie incydentów, analizę przyczyn, podejmowanie działań naprawczych oraz wprowadzanie usprawnień minimalizujących ryzyko ponownego wystąpienia. W ten sposób DORA tworzy jednolity i rygorystyczny system reagowania na incydenty, zwiększający odporność cyfrową całego sektora finansowego.

Szkolenia

Rozporządzenie DORA podkreśla znaczenie kompetencji personelu w budowaniu odporności cyfrowej sektora finansowego, wprowadzając obowiązek regularnych szkoleń w obszarze ICT i cyberbezpieczeństwa. Instytucje finansowe muszą zapewnić, aby pracownicy – od kadry operacyjnej po zarządy – posiadali wiedzę i umiejętności niezbędne do prawidłowego rozpoznawania zagrożeń, reagowania na incydenty oraz stosowania procedur bezpieczeństwa. Szczególny nacisk kładziony jest na szkolenia z zakresu obsługi incydentów, zarządzania ryzykiem ICT, ochrony danych oraz współpracy z dostawcami zewnętrznymi.

Szkolenia powinny być cykliczne, dostosowane do roli pracowników i aktualnych zagrożeń, a ich wyniki dokumentowane. DORA wymaga także, by członkowie organów zarządzających rozumieli skutki decyzji w zakresie odporności cyfrowej i byli świadomi ryzyk technologicznych. Regularne podnoszenie kwalifikacji ma charakter prewencyjny – minimalizuje ryzyko błędów ludzkich i wspiera tworzenie kultury cyberbezpieczeństwa, co wprost przekłada się na lepszą ochronę instytucji oraz jej klientów.

W stosownych przypadkach, zgodnie z art. 13 ust. 6 DORA, w zw. z art. 30 ust. 2 lit. i) podmioty finansowe powinny objąć systemami szkoleń również zewnętrznych dostawców usług ICT.

Wsparcie w realizacji obowiązków

Kancelaria prawna KRWLegal / LegalWell posiada bogate doświadczenie w zakresie wdrożenia wymagań DORA. Kancelaria dysponuje ekspertami, którzy na co dzień wspierają Klientów Kancelarii w realizacji audytów, przeglądów dokumentacji, przesyłaniu sprawozdań do Komisji Nadzoru Finansowego, szkoleniach. Kancelaria KRWLEGAL doradza również w przypadku wystąpienia incydentów i naruszeń bezpieczeństwa informacji.

Autorem komentarza jest: Daniel Niwiński, ekspert ds. cyberbezpieczeństwa w KRWLegal.

OFERTA SZKOLENIOWA

Kancelaria regularnie organizuje szkolenia dla przedstawicieli instytucji działających na rynku finansowych.

Szkolenia są prowadzone w trybie stacjonarnym, w siedzibie Klienta albo w biurze Kancelarii lub w trybie zdalnym.

Tematyka szkolenia uzależniona jest od indywidualnych potrzeb Klienta.

Poniżej prezentujemy wybrane propozycje zagadnień szkoleniowych.

W przypadku zainteresowania naszą ofertą szkoleniową zachęcamy do kontaktu: biuro@krwlegal.pl lub +48 22 29 50 940.

„NADZÓR NAD SYSTEMEM ZARZĄDZANIA RYZYKIEM W DOMU MAKLERSKIM"

I. Uwarunkowania regulacyjne systemu zarządzania ryzykiem w firmie inwestycyjnej;

II. Mechanizmy sprawowania nadzoru nad systemem zarządzania ryzykiem;

III. Wybrane aspekty regulacyjne procesu ICAAP oraz ILAAP;

IV. Ryzyko ESG;

V. Przedstawienie zarysu wymogów kapitałowych zgodnie z IFR;

VI. Konsolidacja wymogu kapitałowego;

VII. Sprawozdawczość w obszarze systemu zarządzania ryzykiem.

„AML/CFT W INSTYTUCJI OBOWIĄZANEJ W PRAKTYCE"

I. Wprowadzenie;

II. Umiejscowienie obszaru AML/CFT w strukturze organizacyjnej instytucji obowiązanej;

III. Ogólna (instytucjonalna) ocena ryzyka w instytucji obowiązanej;

IV. Ocena stosunków gospodarczych;

V. Zarządzanie ryzykiem ML/FT w instytucji obowiązanej;

VI. Obowiązki informacyjne instytucji obowiązanej w zakresie AML/CF;

VII. RODO w AML / CFT.

„ROZPORZĄDZENIE DORA – WYMOGI W ZAKRESIE CYBERBEZPIECZEŃSTWA DLA INSTYTUCJI FINANSOWYCH”

I. Wprowadzenie

- dotychczasowy krajobraz regulacyjny dot. operacyjnej odporności cyfrowej,
- aktualny krajobraz regulacyjny dot. operacyjnej odporności cyfrowej,
- sankcje za naruszenie obowiązków;

II. Zakres przedmiotowy oraz podmiotowy rozporządzenia DORA;

III. Obowiązki i odpowiedzialność organu zarządzającego;

IV. Zarządzaniem ryzykiem związanym z ICT:

- analiza ryzyka jako podstawia zarządzanie ryzykiem związanym z ICT,
- zasada proporcjonalności,
- PDCA,
- zasada rozliczalności,
- DORA a System zarządzania bezpieczeństwem informacji,
- funkcje ram zarządzania ryzykiem ICT,
- normy i standardy bezpieczeństwa ICT,
- strategia operacyjnej odporności cyfrowej,
- regulacje wewnętrzne wymagane przepisami rozporządzenia DORA.

V. Testowanie operacyjnej odporności cyfrowej:

- Wymogi ogólne,
- Testowanie narzędzi i systemów,

- Testowanie zaawansowane,
- Rodzaje testów OOC,
- Dokumentowanie i wykazy.

VI. Zarządzenia incydentami związanymi z ICT:

- Podstawowe obowiązki podmiotu finansowego w ramach zarzadzania incydentami ICT,
- Etapy procesu zarządzania incydentami ICT,
- Klasyfikacja incydentów związanych z ICT,
- Klasyfikacja cyberzagrożeń,
- Obowiązki raportowe,
- Przeglądy incydentów ICT,
- Zarządzanie incydentami ICT – warstwa dokumentacyjna.

VII. Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT:

- Cykl zarządzania umowami z zewnętrznymi dostawcami usług ICT,
- Najważniejsze postanowienia umowne;

VIII. Obowiązki sprawozdawcze:

- Wykaz formularzy sprawozdawczych.

„ZARZĄDZANIE RYZYKIEM ZE STRONY ZEWNĘTRZNYCH DOSTAWCÓW USŁUG ICT NA GRUNCIE ROZPORZĄDZENIA DORA ORAZ AKTÓW WYKONAWCZYCH”

I. **Wprowadzenie i ramy regulacyjne**

- Przegląd Rozporządzenia DORA (UE 2022/2554) – cele, zakres podmiotowy i czasowy,
- Rola aktów wykonawczych (RTS/ITS) w zakresie zarządzania dostawcami ICT;

II. **Identyfikacja i klasyfikacja dostawców ICT**

- Kategorie dostawców zewnętrznych i kryteria istotności usług ICT,
- Mapowanie zależności i łańcucha poddostawców;

III. **Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT**

- Proces due diligence przy wyborze dostawcy ICT,
- Analiza ryzyka przed zawarciem umowy (m.in. bezpieczeństwo, ciągłość działania, lokalizacja danych),
- Ryzyka koncentracji i ryzyka geopolityczne w kontekście usług chmurowych,
- Dokumentowanie oceny i decyzji zarządczych;

IV. **Obowiązki umowne i kontraktowe**

- Minimalne elementy umów z dostawcami ICT zgodnie z DORA,
- Wymogi dotyczące audytów, raportowania i praw kontroli,
- Postanowienia dotyczące strategii wyjścia z usługi i zapewnienia ciągłości usług,
- Wymagania dotyczące podwykonawstwa;

V. **Monitorowanie, testowanie i audyt**

- Mechanizmy ciągłego monitorowania jakości usług ICT,
- Obowiązki raportowe wobec organów nadzoru (KNF),
- Audyty dostawców ICT,
- Współpraca z wewnętrznym audytem i zespołami cyberbezpieczeństwa;

VI. **Reagowanie na incydenty i zarządzanie ciągłością**

- Obowiązki w zakresie zgłaszania incydentów pochodzących od dostawców,
- Eskalacja i role w organizacji,
- Koordynacja komunikacji z organami nadzoru i klientami.

„OBSŁUGA I ZGŁASZANIE INCYDENTÓW ZWIĄZANYCH Z ICT NA GRUNCIE ROZPORZĄDZENIA DORA ORAZ AKTÓW WYKONAWCZYCH”

I. Ramy prawne i definicje

- Podstawy prawne: Rozporządzenie (UE) 2022/2554 (DORA),
- Akty wykonawcze (RTS/ITS) – zakres i znaczenie dla obsługi incydentów ICT,

- Definicje: incydent, poważny incydent, zagrożenie cybernetyczne,
- Powiązania z innymi regulacjami: NIS2, RODO;

II. Klasyfikacja i kryteria istotności incydentów

- Kryteria oceny istotności incydentu,
- Kategorie skutków wystąpienia incydentu,
- Klasyfikacja incydentów,
- Różnica pomiędzy incydentem a poważnym incydentem ICT;

III. Procedura obsługi incydentu ICT

- Etapy obsługi: identyfikacja, analiza, eskalacja, reakcja, zamknięcie,
- Role i odpowiedzialności w organizacji (SOC, CISO, Zarząd, IOD),
- Dokumentowanie i gromadzenie dowodów,
- Współpraca z dostawcami usług ICT i poddostawcami;

IV. Zgłaszanie incydentów do organów nadzoru

- Obowiązki raportowe,
- Struktura i harmonogram raportów:
  - zgłoszenie wstępne,
  - raport pośredni,
  - raport końcowy,
- Zawartość raportu – minimalne wymagania informacyjne,
- Kanały komunikacji i terminy raportowe;

V. Integracja z innymi procesami w organizacji

- Powiązanie zarządzania incydentami z polityką zarządzania ryzykiem ICT,
- Integracja z systemem BCM i planami DRP,
- Integracja z Polityką Ochrony Danych Osobowych i obsługą naruszeń ochrony danych osobowych na gruncie RODO,
- Rola szkoleń wewnętrznych i podnoszenia świadomości pracowników,

- Audyt i testowanie procedur reagowania na incydenty;

VI. Podsumowanie i rekomendacje

- Najczęstsze błędy w obsłudze incydentów ICT,
- Rekomendacje organów nadzoru i dobre praktyki branżowe.

„DZIAŁALNOŚĆ ASI – WYMOGI PRAWNE I NADZORCZE ORAZ PROCES INWESTYCYJNY"

I. Uwarunkowania prawne, regulacyjne i nadzorcze związane z funkcjonowaniem ASI

- Podstawy prawne (przepisy krajowe i unijne) oraz regulacyjne,
- Rodzaje funduszy – AFI vs. UCITS,
- Dopuszczalny przedmiot działalności ASI i ZASI,
- Rodzaje ASI i wewnętrzna konstrukcja,
- ASI i FIZ jako AFI – podstawowe różnice regulacyjne, różnice w konstrukcji, zarzadzaniu, limity inwestycyjne, polityka inwestycyjna,
- ZASI za zezwoleniem oraz tzw. ZASI „rejestrowane", (rozróżnienie, obowiązki, zadania, wymogi regulacyjne),
- Nadzór UKNF nad ZASI,
- Depozytariusz w ASI,
- Inwestor w ASI – profil inwestora zasady klasyfikacji klientów ASI,
- Zlecenie zarządzania ASI – oursourcing regulowany / nieregulowany,
- Wprowadzenie ASI do obrotu,
- Formy inwestowania w ASI – inwestowanie kapitałowe i dłużne;

II. Uwarunkowania prawne działalności ASI w kontekście zarządzania portfelem inwestycyjnym

- Proces inwestycyjny w ASI – podstawowe zasady, polityka i strategia inwestycyjna, struktura majątku ASI,
- Proces dezinwestycyjny w ASI – formy exitów ASI z SPV,

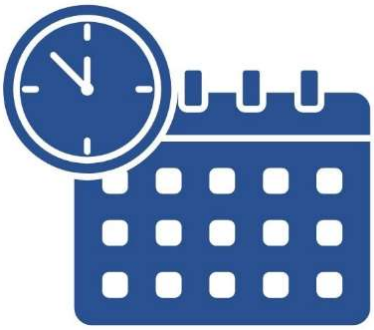
- Podatki w ASI – preferencje podatkowe dla inwestorów, orzecznictwo podatkowe, interpretacje podatkowe, preferencja podatkowa w CIT dla ASI w kontekście obrotu aktywami,

- Wycena instrumentów finansowych pod ASI,

- Obowiązki sprawozdawcze i audyt sprawozdania finansowego / wymogi dot. raportowania przez ASI,

- Koszty operacyjne ponoszone przez ASI.

WAŻNE DATY



9 września 2025 r. – wejście w życie ustawy z dnia 9 lipca 2025 r. o zmianie ustawy o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (Dz. U. z 2025 r. po. 1161);

9 września 2025 r. – wejście w życie ustawy z dnia 5 sierpnia 2025 r. o zmianie ustawy – Prawo bankowe oraz niektórych innych ustaw (Dz.U. z 2025 r. poz. 1170);

9 września 2025 r. – wejście w życie części przepisów ustawy z dnia 5 sierpnia 2025 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Kodeks cywilny oraz niektórych innych ustaw;

18 września 2025 r. – wejście w życie części przepisów ustawy z dnia 5 sierpnia 2025 r. o uchyleniu ustawy o centralnej informacji emerytalnej (Dz. U. z 2025 r. poz. 1216), w tym w zakresie uchylenia ustawy z dnia 7 lipca 2023 r. o Centralnej Informacji Emerytalnej;

29 listopada 2025 r. – wejście w życie ustawy z dnia 25 lipca 2025 r. o zmianie ustawy – Prawo bankowe oraz niektórych innych ustaw (Dz. U. z 2025 r. poz. 1191);

1 stycznia 2026 r. - wejście w życie ustawy z dnia 25 lipca 2025 r. o zmianie ustawy – Prawo zamówień publicznych oraz niektórych innych ustaw (Dz. U. z 2025 r. poz. 1173).

O NAS

KRWLegal / LegalWell jest niezależną Kancelarią prawną skupiającą grupę doświadczonych prawników, którzy poprzez kompleksowe zrozumienie Klienta i jego potrzeb, opracowują dostosowane do potrzeb Klienta rozwiązania. Priorytetem Kancelarii jest odpowiedź na potrzeby Klienta.

KRWLegal / LegalWell jest wiodącą na rynku usług prawnych Kancelarią w zakresie doradztwa klientom prywatnym, w tym zarządzania majątkiem prywatnym i planowania finansowego dla Private Clients, a także przygotowania wejścia na giełdę i pozyskania inwestorów do nowych przedsięwzięć w sektorach nowoczesnej gospodarki.

Kancelaria jest zaangażowana w rozwój rynku kapitałowego w Polsce, w tym bierze czynny udział w pracach legislacyjnych dotyczących funkcjonowania tego rynku.

Nasza oferta obejmuje pomoc w takich działaniach jak przygotowanie transakcji (M&A), obsługa inwestycji kapitałowych, sekurytyzacja, finansowanie i tworzenie startupów, audyt nieruchomości, zachęty MIFID, obsługa funduszy inwestycyjnych i innych instytucji finansowych czy restrukturyzacja zobowiązań. Jednym z wiodących obszarów naszej praktyki jest również doradztwo w obszarze regulacji dotyczących sektora energetycznego, w szczególności w zakresie energetyki alternatywnej (OZE), ochrony środowiska naturalnego i finansowania przedsięwzięć proekologicznych.

Kancelaria aktywnie uczestniczy w prowadzonych projektach, nie ograniczając się wyłącznie do doradztwa prawnego.

Cechą Kancelarii jest otwarta komunikacja z Klientem.

DANE KONTAKTOWE

Krzysztof Rożko i Wspólnicy

Kancelaria Prawna

ul. Wojciecha Górskiego 9, 00-033 Warszawa

tel.: +48 22 295 09 40, tel./fax: +48 22 692 44 74

e-mail: biuro@krwlegal.pl

Zapraszamy również do odwiedzania naszej strony internetowej

oraz śledzenia profilu Kancelarii na

gdzie na bieżąco zamieszczamy informacje o najnowszych zmianach
w środowisku regulacyjnym rynku finansowego.

Zespół Kancelarii Prawnej Krzysztof Rożko i Wspólnicy

WSPÓLNICY

Krzysztof Rożko

Wspólnik Zarządzający

- Fundusze inwestycyjne
- Instytucje finansowe i regulacje rynku finansowego
- Transakcje venture capital/ private equity
- Bankowość i finance
- Finansowanie projektów infrastrukturalnych
- Planowanie podatkowe i zarządzanie majątkiem
- Fuzje i przejęcia (Transakcje M&A)
- Nieruchomości i inwestycje budowlane

Krzysztof.Rozko@krwlegal.pl

+48 22 295 09 40

Mariusz Bagiński

Wspólnik

- Fundusze inwestycyjne
- Instytucje finansowe i regulacje rynku finansowego
- Transakcje venture capital/ private equity
- Bankowość i finance
- Finansowanie projektów infrastrukturalnych
- Prawo spółek i kontrakty handlowe
- Spory korporacyjne
- Planowanie podatkowe i zarządzanie majątkiem
- Fuzje i przejęcia (Transakcje M&A)
- Nieruchomości i inwestycje budowlane

Mariusz.Baginski@krwlegal.pl

+48 22 295 09 40

Tomasz Kamiński

Wspólnik

- Transakcje M&A oraz fuzje i przejęcie
- Prawo nowych technologii
- Cyberbezpieczeństwo
- Prawo spółek i kontrakty handlowe
- Zarządzanie ASI
- Fundusze inwestycyjne
- Transakcje venture capital/ private equity
- Instytucje finansowe i regulacje rynku finansowego
- Tworzenie, finansowanie i obsługa startupów

Tomasz.Kaminski@krwlegal.pl

+48 22 295 09 40

Nikola Jadwiszczak – Niedbałka

Wspólnik

- Fundusze inwestycyjne
- Spory sądowe oraz postępowania sankcyjne dla podmiotów rynku kapitałowego
- Doradztwo regulacyjne dla sektora finansowego i fintech
- Zarządzanie ASI
- Doradztwo w zakresie AML
- Transakcje venture capital/ private equity
- Fundacje rodzinne
- Tworzenie, finansowanie i obsługa startupów

Nikola.Jadwiszczak@krwlegal.pl

+48 22 295 09 40

WYRÓŻNIENIA

NOTA REDAKCYJNA

Niniejszy Newsletter Regulacyjny Kancelarii Prawnej Krzysztof Rożko i Wspólnicy (Kancelaria) to ukazujący się miesięcznie zbiór informacji z zakresu otoczenia prawnego i regulacyjnego instytucji finansowych.

Newsletter Regulacyjny przygotowywany jest przez praktyków zajmujących się obsługą podmiotów prowadzących działalność zarówno na polskim, jak i europejskim rynku kapitałowym.

Kancelaria informuje, że Newsletter Regulacyjny nie stanowi usługi doradztwa prawnego, a także nie jest formą świadczenia pomocy prawnej.

Zespół Kancelarii Prawnej Krzysztof Rożko i Wspólnicy będzie także wdzięczny za przekazywanie wszelkich uwag i sugestii co do treści Newslettera Regulacyjnego.