**UZASADNIENIE**

**I. Potrzeba i cel wydania ustawy**

Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego ma na celu wdrożenie do polskiego systemu prawnego oraz zapewnienie stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (zwanego dalej „rozporządzeniem 2022/2554”), a także wdrożenie dyrektywy Parlamentu Europejskiego i Rady 2022/2556 z dnia 14 grudnia 2022 r. w sprawie zmiany dyrektyw 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 oraz (UE) 2016/2341 w odniesieniu do operacyjnej odporności cyfrowej sektora finansowego (zwanej dalej „dyrektywą 2022/2556”).

Przyjęcie rozporządzenia 2022/2554 jest konsekwencją postanowień zawartych w komunikacie Komisji Europejskiej z dnia 8 marca 2018 r. pt. „Plan działania w zakresie technologii finansowej: w kierunku bardziej konkurencyjnego i innowacyjnego europejskiego sektora finansowego” oraz służy realizacji wspólnych zaleceń technicznych Europejskiego Urzędu Nadzoru Bankowego, Europejskiego Urzędu Nadzoru Ubezpieczeń  i Pracowniczych Programów Emerytalnych oraz Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych, opublikowanych w kwietniu 2019 r., w których ww. instytucje wezwały do przyjęcia spójnego podejścia do ryzyka związanego z ICT (technologie informacyjno-komunikacyjne) w sektorze finansów oraz zaleciły wzmocnienie, w sposób proporcjonalny, operacyjnej odporności cyfrowej sektora usług finansowych za pomocą unijnej inicjatywy sektorowej.

Dynamiczny rozwój gospodarki cyfrowej zwiększa wykorzystanie ICT także w sektorze usług finansowych, co powoduje jednak zwiększenie ryzyka związanego z cyberzagrożeniami. Obecnie cyfryzacja ma krytyczne znaczenie dla wykonywania typowych funkcji wszystkich podmiotów finansowych i obejmuje m.in. płatności, w przypadku których coraz bardziej odchodzi się od płatności gotówkowych, a także rozliczanie i rozrachunek papierów wartościowych, operacje udzielania pożyczek i finansowania, etc.

W związku z powyższym rozporządzenie 2022/2554 dokonuje harmonizacji przepisów dotyczących operacyjnej odporności cyfrowej i bezpieczeństwa ICT w obszarze usług finansowych. Z uwagi na dynamiczny rozwój gospodarki cyfrowej, przepisy te mają kluczowe znaczenie dla zapewnienia stabilności finansowej i integralności rynku finansowego. Harmonizacja w tym zakresie ma istotne znaczenie dla obniżenia poziomu ryzyka systemowego, które w zakresie rynku finansowego ma wysoki poziom, z uwagi na wysoki poziom wzajemnych powiązań między podmiotami finansowymi, rynkami finansowymi i infrastrukturami rynku finansowego, w szczególności współzależności między ich systemami ICT, która może powodować rozprzestrzenianie się cyberincydentów.

Rozporządzenie 2022/2554 nakłada obowiązki na podmioty finansowe wskazane w art. 2 ust. 1 lit.  a – t. Jednocześnie art. 2 ust. 3 rozporządzenia 2022/2554 wskazuje podmioty finansowe wyłączone z zakresu jego stosowania (podmioty objęte zakresem projektowanej regulacji wymienione zostały w pkt. II. 5 uzasadnienia).

Dodatkowo rozporządzenie 2022/2554 obejmuje także, zgodnie z art. 2 ust. 1 pkt u, zewnętrznych dostawców usług ICT, na których oddziałuje pośrednio, z uwagi na możliwość wydania decyzji, o której mowa w art. 42 ust. 6 tego rozporządzenia.

Zgodnie z art. 1 rozporządzenia 2022/2554, w zakresie obowiązków nakładanych na podmioty finansowe, reguluje ono:

a) wymogi mające zastosowanie do podmiotów finansowych objętych zakresem regulacji rozporządzenia, w odniesieniu do:

(i) zarządzania ryzykiem związanym z wykorzystaniem technologii informacyjno-komunikacyjnych (ICT);

(ii) zgłaszania poważnych incydentów związanych z ICT właściwym organom oraz dobrowolnego informowania ich o znaczących cyberzagrożeniach;

(iii) zgłaszania właściwym organom przez podmioty finansowe, o których mowa w art. 2 ust. 1 lit. a - d, poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami;

(iv) testowania operacyjnej odporności cyfrowej;

(v) wymiany informacji i analiz w związku z cyberzagrożeniami i podatnościami w tym obszarze;

(vi) środków na rzecz należytego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT;

b) wymogi w odniesieniu do ustaleń umownych zawartych między zewnętrznymi dostawcami usług ICT a podmiotami finansowymi.

Należy podkreślić, że obowiązki określone w rozporządzeniu 2022/2554, co do zasady, stosowane będą przez podmioty finansowe bezpośrednio.

Niektóre przepisy rozporządzenia 2022/2554, w celu zapewnienia ich stosowania, wymagają wdrożenia do prawa krajowego. Przede wszystkim dotyczy to przepisów wyposażających organy właściwe, w rozumieniu art. 46 rozporządzenia 2022/2554, w kompetencje zapewniające skuteczny nadzór nad spełnianiem wymogów i obowiązków nakładanych na podmioty finansowe, w szczególności dotyczy to minimalnych uprawnień, o których mowa w art. 50.

Zmiany wprowadzone dyrektywą 2022/2556, która dokonuje zmian w dyrektywach: 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 oraz (UE) 2016/2341 mają na celu zapewnienie spójności z rozwiązaniami wprowadzanymi rozporządzeniem 2022/2554. Zmiany ww. dyrektyw, odnoszące się do operacyjnej odporności cyfrowej sektora finansowego, wprowadzają odniesienia do rozporządzenia 2022/2554, co zapewnia spójność regulacji na poziomie Unii Europejskiej (UE). Z uwagi na konieczność implementacji postanowień ww. dyrektyw, konieczne jest wprowadzenie odpowiednich zmian, w tym zmian o charakterze wynikowym, w następujących ustawach:

1. ustawie z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych,
2. ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe,
3. ustawie z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi,
4. ustawie z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,
5. ustawie z dnia 19 sierpnia 2011 o usługach płatniczych,
6. ustawie z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego, o Rzeczniku Finansowym i o Funduszu Edukacji Finansowej,
7. ustawie z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej,
8. ustawie z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji.

**2. Dotychczasowy stan prawny**

Unijny sektor finansowy charakteryzuje się wysokim poziomem harmonizacji regulacji za pomocą jednolitego zbioru przepisów i podlega Europejskiemu Systemowi Nadzoru Finansowego. Jednak przepisy dotyczące operacyjnej odporności cyfrowej i bezpieczeństwa ICT w sektorze finansowym nie zostały jeszcze w pełni zharmonizowane. W niektórych obszarach takich jak testowanie operacyjnej odporności cyfrowej, harmonizacja jest ograniczona, w innych obszarach np. w zakresie monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT, brak jest odpowiednich regulacji. Z uwagi na powyższe zdecydowano   
o przyjęciu jednej, czytelnej regulacji UE, która ma na celu uporządkowanie przepisów odnoszących się do operacyjnej odporności cyfrowej i ich uzupełnienie.

W obowiązującym porządku prawnym fragmentaryczne regulacje dotyczące operacyjnej odporności cyfrowej znajdują się w aktach prawnych regulujących poszczególne rodzaje usług finansowych takich jak usługi bankowe, usługi płatnicze, sektor funduszy emerytalnych, sektor funduszy inwestycyjnych czy działalność ubezpieczeniowa i reasekuracyjna.

Kluczowym i pierwszym kompleksowym aktem prawnym na poziomie UE, regulującym kwestie związane z cyberbezpieczeństwem była dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (zwana dalej ,,dyrektywą 2016/1148”), która stanowiła pierwsze horyzontalne ramy w zakresie cyberbezpieczeństwa, mające też zastosowanie do trzech rodzajów podmiotów finansowych, a mianowicie instytucji kredytowych, systemów obrotu i kontrahentów centralnych. Jednak biorąc pod uwagę, że w dyrektywie 2016/1148 określono mechanizm identyfikacji na szczeblu krajowym operatorów usług kluczowych, jedynie niektóre podmioty finansowe zostały objęte jej zakresem stosowania i obowiązkiem spełniania określonych w niej wymogów w zakresie bezpieczeństwa ICT i zgłaszania incydentów. Nowa dyrektywa Parlamentu Europejskiego i Rady 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (zwana dalej „dyrektywą 2022/2555 ”), regulująca zagadnienia z zakresu cyberbezpieczeństwa, ustanawia jednolite kryterium określania podmiotów objętych jej zakresem stosowania (zasada limitu wielkości), przy czym obejmuje nim też wspomniane trzy rodzaje podmiotów finansowych.

Regulacja dyrektywy 2016/1148 została implementowana do polskiego systemu prawnego ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która jest ustawą   
o charakterze horyzontalnym, wprowadzającą rozwiązania o charakterze systemowym, w tym dotyczące organizacji krajowego systemu cyberbezpieczeństwa tj. zadania i obowiązki podmiotów wchodzących w skład tego systemu, określa także sposób sprawowania nadzoru   
i kontroli w zakresie stosowania przepisów ustawy.

W zakresie sektora finansowego regulacja ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (zwanej dalej ,,ustawą o krajowym systemie cyberbezpieczeństwa”), zgodnie z dyspozycjami dyrektywy 2016/1148 i załącznikiem do ustawy, obejmuje instytucje kredytowe objęte rozporządzeniem Parlamentu Europejskiego i Rady nr 575/2013   
w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych.   
W polskim systemie prawa regulacje dotyczące instytucji kredytowych znajdują się w ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe (zwanej dalej „ustawą Prawo bankowe”) i w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych. Załącznik do ustawy o krajowym systemie cyberbezpieczeństwa odwołuje się tutaj do art. 4 ust. 1 pkt 17 ustawy Prawo bankowe. Dodatkowo załącznik odwołuje się do definicji banku krajowego (art. 4 ust. 1 pkt 1 ustawy - Prawo bankowe), oddziału banku zagranicznego (art. 4 ust. 1 pkt 20 ustawy – Prawo bankowe), oddziału instytucji kredytowej (art. 4 ust. 1 pkt 18 ustawy – Prawo bankowe). Zakresem ww. załącznika został też objęty sektor spółdzielczych kas oszczędnościowo-kredytowych, objęty ustawą z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych. W zakresie infrastruktury rynków finansowych załącznik do ustawy, zgodnie z dyrektywą 2016/1148, odwołuje się do operatorów systemu obrotu i kontrahentów centralnych. Przedmiotowy sektor jest regulowany w polskim systemie prawa przez ustawę z dnia 29 lipca 2005 r. obrocie instrumentami finansowymi (zwaną dalej ,,ustawą o obrocie instrumentami finansowymi”). Załącznik do ustawy o krajowym systemie cyberbezpieczeństwa odwołuje się tutaj do podmiotu prowadzącego rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy o obrocie instrumentami finansowymi, obejmuje podmiot wskazany w art. 3 pkt. 49 ustawy o obrocie instrumentami finansowymi oraz podmiot, o którym mowa w art. 48 ust. 7 ustawy o obrocie instrumentami finansowymi.

Rozporządzenie 2022/2554, wdrażane projektowaną ustawą, w porównaniu do ww. dyrektyw 2016/1148 i 2022/2555, zwiększa poziom harmonizacji różnych elementów odporności cyfrowej przez wprowadzenie wymogów w zakresie zarządzania ryzykiem związanym z ICT i zgłaszania incydentów związanych z ICT, które to wymogi są bardziej rygorystyczne w porównaniu z wymogami określonymi w obecnych unijnych przepisach dotyczących usług finansowych. Rozporządzenie 2022/2554 stanowi *lex specialis* względem dyrektywy 2022/2555. Ponadto, w porównaniu do ww. regulacji dyrektyw rozszerzony został katalog podmiotów finansowych objętych zakresem regulacji rozporządzenia 2022/2554, wskazany w art. 2 ust. 1 lit. a–t.

Warto jednak podkreślić, że przepisy rozporządzenia 2022/2554 zakładają utrzymanie silnego związku między sektorem finansowym, a unijnymi horyzontalnymi ramami w zakresie cyberbezpieczeństwa, określonymi obecnie w dyrektywie 2022/2555 (termin na dokonanie transpozycji: 17.10.2024 r.), co ma zasadnicze znaczenie dla zapewnienia spójności z przyjętymi przez państwa członkowskie strategiami w zakresie cyberbezpieczeństwa oraz umożliwienia organom nadzoru finansowego uzyskanie informacji na temat cyberincydentów wpływających na inne sektory objęte tą dyrektywą.

Z uwagi na korelację między przepisami rozporządzenia 2022/2554 a przepisami zarówno dyrektywy 2016/1148, jak i dyrektywy 2022/2555, konieczne jest także wprowadzenie odpowiednich zmian do ustawy o krajowym systemie cyberbezpieczeństwa.

**3. Różnice pomiędzy dotychczasowym, a projektowanym stanem prawnym**

Rozporządzenie 2022/2554 wprowadza jednolity zbiór przepisów i system nadzoru, dotyczący operacyjnej odporności cyfrowej. Dotychczasowe częściowe tylko uwzględnienie przepisów dotyczących ryzyka związanego z ICT na szczeblu UE, powoduje braki, niespójności lub nakładanie się przepisów w istotnych obszarach, takich jak zgłaszanie incydentów związanych z ICT i testowanie operacyjnej odporności cyfrowej. Wprowadzenie zharmonizowanych przepisów w tym obszarze sprzyjać będzie wyeliminowaniu przeszkód dla funkcjonowania rynku wewnętrznego usług finansowych, utrudniających korzystanie ze swobody przedsiębiorczości i swobody świadczenia usług podmiotom finansowym prowadzącym działalność transgraniczną. Wzmocni także ochronę konsumenta korzystającego z usług finansowych.

Ponadto, w celu zapewnienia spójności systemu w zakresie operacyjnej odporności cyfrowej sektora finansowego dyrektywa 2022/2556 wprowadza zmiany do dyrektyw regulujących poszczególne usługi finansowe, które są konsekwencją zmian wprowadzanych rozporządzeniem.

W celu umożliwienia stosowania rozporządzenia 2022/2554 wskazane jest przyjęcie w krajowym porządku prawnym aktu służącego jego stosowaniu. Przyjęto zatem rozwiązanie polegające na opracowaniu projektu o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego.

Kluczowe zmiany związane z koniecznością wdrożenia przepisów rozporządzenia 2022/2554 wprowadzone zostaną do ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (zwanej dalej „ustawą o nadzorze nad rynkiem finansowym”) (art. 5 projektu). Są to zmiany związane z nadaniem kompetencji zapewniających skuteczny nadzór nad spełnianiem wymogów i obowiązków nakładanych na podmioty finansowe, w szczególności dotyczy to minimalnych uprawnień, o których mowa w art. 50 rozporządzenia 2022/2554.

Organem odpowiedzialnym za nadzór nad przestrzeganiem niniejszego rozporządzenia, jako organ nadzoru nad rynkiem finansowym w Polsce, będzie Komisja Nadzoru Finansowego (zwana dalej: ,,KNF”), która:

**●** zostanie uprawniona do przeprowadzania kontroli działalności podmiotów finansowych w rozumieniu rozporządzenia 2022/2554, z wyłączeniem podmiotów, o których mowa w art. 2 ust. 3 tego rozporządzenia. Do ww. kontroli znajdą zastosowanie przepisy regulujące kontrolę danego rodzaju podmiotu finansowego (art. 50 ust. 2 rozporządzenia 2022/2554);

● w przypadku gdy istnieje uzasadnione podejrzenie naruszenia obowiązków określonych w rozporządzeniu 2022/2554 będzie mogła zażądać od przedsiębiorcy telekomunikacyjnego, w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, udostępnienia rejestrów przesyłu danych będących w posiadaniu tego operatora (art. 50 ust. 4 lit. d rozporządzenia 2022/2554);

● w przypadku, gdy działalność podmiotu finansowego objętego zakresem regulacji rozporządzenia 2022/2554, jest wykonywana z naruszeniem obowiązków określonych w tym rozporządzeniu, będzie mogła w drodze decyzji:

1) nakazać osobie fizycznej, osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej zaprzestanie danego zachowania oraz powstrzymanie się od takiego zachowania w przyszłości (art. 50 ust. 4 lit. a rozporządzenia 2022/2554);

2) zakazać osobie odpowiedzialnej za to naruszenie pełnienia funkcji członka zarządu lub rady nadzorczej albo innej funkcji kierowniczej tego podmiotu przez okres nie krótszy niż miesiąc i nie dłuższy niż rok (art. 50 ust. 5 rozporządzenia 2022/2554);

3) nałożyć karę pieniężną (art. 50 ust. 4 lit. c rozporządzenia 2022/2554).

Projektowane przepisy określą sposób określenia wysokości ww. kar pieniężnych nakładanych w przypadku naruszenia przepisów rozporządzenia 2022/2554, w tym przesłanki wpływające na określenie wysokości kary oraz maksymalną wysokość kary pieniężnej, a także zasady udostępnienia informacji o nałożonych karach;

● będzie mogła wydać publiczne oświadczenie, w którym wskaże imię i nazwisko osoby fizycznej albo firmę lub nazwę osoby prawnej, odpowiedzialnych za to naruszenie, oraz charakter tego naruszenia (art. 50 ust. 4 lit. e rozporządzenia 2022/2554);

● zostanie uprawniona do wydawania decyzji, o której mowa w art. 42 ust. 6 rozporządzenia 2022/2554, nakazującej podmiotom finansowym, tymczasowe zawieszenie, w części albo w całości, korzystania z usługi świadczonej przez kluczowego zewnętrznego dostawcę usług ICT lub jej wdrażania do czasu wyeliminowania ryzyka zidentyfikowanego w zaleceniach skierowanych do kluczowych zewnętrznych dostawców usług ICT, a także, w razie potrzeby, nakazania podmiotom finansowym, wypowiedzenia, w części lub w całości, stosownych ustaleń umownych zawartych z kluczowymi zewnętrznymi dostawcami usług ICT.

Ponadto określone zostaną zadania KNF dotyczące realizacji przez podmioty finansowe zaawansowanych testów, o których mowa w art. 26 rozporządzenia 2022/2554 oraz sposób realizacji obowiązków informacyjnych, o których mowa w art. 28 rozporządzenia 2022/2554 przez podmioty finansowe.

Wprowadzona również zostanie podstawa prawna zapewniająca możliwość współpracy oraz wymiany informacji i dokumentów z właściwymi organami w rozumieniu art. 46 rozporządzenia 2022/2554 z państw członkowskich Unii Europejskiej lub państw członkowskich Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stron umowy   
o Europejskim Obszarze Gospodarczym oraz Europejskim Urzędem Nadzoru Bankowego, Europejskim Urzędem Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych   
i Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych, w zakresie niezbędnym do wykonywania obowiązków wynikających z rozporządzenia 2022/2554. Ponadto KNF będzie mogła współpracować oraz wymieniać informacje i dokumenty z odpowiednimi wiodącymi organami nadzorczymi, wyznaczonymi zgodnie z art. 31 ust. 1 lit. b rozporządzenia 2022/2554 oraz Komisją Europejską.

Z uwagi na wskazaną korelację między przepisami rozporządzenia 2022/2554 a przepisami zarówno dyrektywy 2016/1148, jak i dyrektywy 2022/2555, konieczne jest także wprowadzenie odpowiednich zmian do ustawy o krajowym systemie cyberbezpieczeństwa w celu zapewnienia spójności rozwiązań oraz efektywnego działania całego systemu nadzoru. Zmiany tej ustawy określą sposób informowania przez podmioty finansowe organów funkcjonujących w krajowym systemie cyberbezpieczeństwa o poważnych incydentach oraz znaczących zagrożeniach związanych z ICT, a także procedury komunikacji między tymi organami.

Istotną zmianą będzie także zapewnienie możliwości uczestnictwa Przewodniczącego KNF w posiedzeniach Kolegium przy Radzie Ministrów, działającego jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa.

Dodatkowo projektowane zmiany ustawy wprowadzą obowiązek współdziałania zespołów CSIRT MON, CSIRT GOV i CSIRT NASK oraz właściwych organów w rozumieniu rozporządzenia 2022/2554 w zakresie działalności podmiotów finansowych będących podmiotami kluczowymi lub podmiotami ważnymi.

**II. Szczegółowe omówienie przepisów ustawy**

1. zmiany ustawy **z dnia 28 sierpnia 1997 r.** **o organizacji i funkcjonowaniu funduszy emerytalnych** **(art. 1)**

**Art. 1** wprowadza zmiany do ustawy z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych, mające na celu transpozycję przepisów dyrektywy 2022/2556, która zmienia w art. 8 dyrektywę Parlamentu Europejskiego i Rady 2016/2341 z dnia 14 grudnia 2016 r. w sprawie działalności instytucji pracowniczych programów emerytalnych oraz nadzoru nad takimi instytucjami (zwanej dalej „dyrektywą IORP”). Z uwagi na powyższe proponuje się zmianę brzmienia art. 26d ustawy z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych w związku z art. 8 dyrektywy 2022/2556 wprowadzającego zmiany   
w art. 21 ust. 5 dyrektywyIORP, który nakłada obowiązek na pracownicze fundusze emerytalne do opracowania i wprowadzenia planów awaryjnych zgodnie z rozporządzeniem 2022/2554.

2. zmiany w ustawie **z dnia 29 sierpnia 1997 r. – Prawo bankowe (art. 2)**

**Art. 2** wprowadza zmiany do ustawy– Prawo bankowe, mające na celu przede wszystkim transpozycję przepisów dyrektywy 2022/2556 w zakresie art. 4, który zmienia dyrektywę Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniającą dyrektywę 2002/87/WE i uchylającą dyrektywy 2006/48/WE oraz 2006/49/WE(zwaną dalej „dyrektywą 2013/36/UE”).

Wprowadzane do ustawy – Prawo bankowe zmiany obejmują:

1) w art. 4 ust. 1 ustawy – Prawo bankowe w dodawanym pkt 40 przywołana została pełna nazwa rozporządzenia unijnego dot. operacyjnej odporności cyfrowej sektora finansowego z podaniem jego skróconej nazwy, w celu posługiwania się tym skrótem na potrzeby odesłań do rozporządzenia w  dalszych przepisach ustawy (art. 2 pkt 1 projektu);

2) w art. 6a w ust. 1 dodano pkt 3 i 4 ustawy – Prawo bankowe, co ma na celu rozszerzenie katalogu czynności outsourcowanych. Zgodnie z dodanym pkt 3 umożliwione zostanie outsourcowanie zadań związanych z obowiązkami sprawozdawczymi w zakresie zgłaszania poważnych incydentów związanych z ICT i  powiadamiania o znaczących cyberzagrożeniach, a tym samym uwzględnienie art. 19 ust. 5 rozporządzenia 2022/2554, który brzmi*: Podmioty finansowe mogą zlecić w drodze outsourcingu, zgodnie z unijnym i krajowym prawem sektorowym, zadania związane z obowiązkami sprawozdawczymi na mocy niniejszego artykułu zewnętrznemu dostawcy usług. W przypadku takiego outsourcingu podmiot finansowy pozostaje w pełni odpowiedzialny za spełnienie wymogów dotyczących zgłaszania incydentów.* Ponadto,zgodnie z dodanym pkt 4, będzie można również outsourcować zadania związane ze sprawdzaniem zgodności z wymogami dotyczącymi zarządzania ryzykiem związanym z ICT. Dodanie pkt 4 w art. 6a ust. 1 ustawy – Prawo bankowe nawiązuje do art. 6 ust. 10 rozporządzenia 2022/2554, który brzmi: *Podmioty finansowe mogą, zgodnie z unijnym i krajowym prawem sektorowym, zlecić w drodze outsourcingu zadania związane ze sprawdzaniem zgodności z wymogami dotyczącymi zarządzania ryzykiem związanym z ICT przedsiębiorstwom wewnątrz grupy lub przedsiębiorstwom zewnętrznym. W przypadku takiego outsourcingu podmiot finansowy pozostaje w  pełni odpowiedzialny za sprawdzanie zgodności z wymogami dotyczącymi zarządzania ryzykiem związanym z ICT.* Wartym zauważenia jest, że bank pozostaje odpowiedzialny za czynności, które zleca w drodze outsourcingu. Na powyższe wskazują Wytyczne Europejskiego Urzędu Nadzoru Bankowego (EBA) *Wytyczne w sprawie outsourcingu* EBA/GL/2019/02 z dnia 25 lutego 2019 r. tj. ust. 35 Wytycznych: *Outsourcing funkcji nie może skutkować oddelegowaniem odpowiedzialności organu zarządzającego. Instytucje i instytucje płatnicze pozostają w pełni odpowiedzialne za wykonywanie obowiązków regulacyjnych, w tym zdolność do nadzorowania outsourcingu funkcji krytycznych i  istotnych.* Ponadto, warto zwrócić uwagę na art. 6b ust. 2 ustawy – Prawo bankowe, który stanowi o  nieograniczonej odpowiedzialności banku za szkody wyrządzone klientom wskutek niewykonania lub nienależytego umów powierzających wykonywanie czynności w drodze outsourcingu i podoutsourcingu bankowego;

3) zmiana art. 6c ustawy – Prawo bankowe obejmuje:

a) nowe brzmienie ust. 1 pkt 1 ustawy – Prawo bankowe wynika z implementacji art. 4 pkt 3 dyrektywy 2022/2556, który nakłada wymóg posiadania przez instytucje odpowiednich strategii, planów awaryjnych, strategii i planów ciągłości działania, w tym strategii i  planów na rzecz ciągłości działania w zakresie ICT oraz planów reagowania i przywracania sprawności ICT w odniesieniu do technologii, którą wykorzystują do przekazywania informacji. W art. 6c ust. 1 pkt 1 ustawy – Prawo bankowe mowa jest wyłącznie o obowiązku posiadania przez bank i przedsiębiorcę lub przedsiębiorcę zagranicznego, na potrzeby wykonywania czynności w drodze outsourcingu i podoutsourcingu bankowego, planów działania zapewniających ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową, dlatego zasadnym wydaje się rozszerzenie obowiązku posiadanych dokumentów, o dokumenty wynikające ze zmienianej w art. 4 dyrektywy. Przedmiotowe plany ciągłości działania, plany awaryjne, strategie i plany na rzecz ciągłości działania w zakresie ICT, plany reagowania i przywracania sprawności ICT mają na celu w szczególności, uwzględniając przeciwdziałanie ryzyku cyfrowemu, szybkie i sprawne rozwiązywanie incydentów związanych z ICT poprzez ograniczanie szkód oraz priorytetowe traktowanie podjęcia działań naprawczych i wznowienia działalności, z  uwzględnieniem bezpieczeństwa sieci i systemów teleinformatycznych, integralności i poufności danych;

b) dodanie w art. 6c ust. 1 ustawy – Prawo bankowe pkt 4 wynika z implementacji art. 4 pkt 2dyrektywy 2022/2556 tj. zmiany dyrektywy2013/36/UE, nakładającej wymóg posiadania przez instytucje sieci i  systemów teleinformatycznych utworzonych i zarządzanych zgodnie z rozporządzeniem 2022/2554. Z  uwagi na istotną rolę, jaką odgrywają sieci i systemy teleinformatyczne w procesach outsourcingu i  podoutsourcingu bankowego, zasadnym wydaje się, aby podlegały one odpowiednim procedurom, standardom, były zarządzane zgodnie z rozporządzeniem unijnym, mającym na celu wzmocnienie odporności cyfrowej sektora finansowego. Rozporządzenie 2022/2554 porusza m. in. takie kwestie, jak standardy, wymogi, którym muszą sprostać sieci i systemy teleinformatyczne; konieczność posiadania przez instytucje finansowe ram zarządzania ryzykiem związanym z ICT, mechanizmów pozwalających na szybkie wykrywanie problemów związanych z wydajnością sieci ICT i incydentów związanych z ICT; wymóg testowania narzędzi i systemów ICT; obowiązki zewnętrznego dostawcy usług ICT w zakresie bezpieczeństwa ICT;

c) dodanie w art. 6c ustawy – Prawo bankowe ust. 1a dotyczy implementacji art. 4 pkt 3dyrektywy 2022/2556 tj. zmiany dyrektywy 2013/36/UE w zakresie potwierdzenia, że strategie i plany na rzecz ciągłości działania w zakresie ICT oraz plany reagowania i przywracania sprawności ICT są ustanawiane, zarządzane i testowane zgodnie z art. 11 rozporządzenia 2022/2554, aby bank i  przedsiębiorca lub przedsiębiorca zagraniczny, pomimo możliwości wystąpienia zakłóceń w  działalności gospodarczej, mogli w takim przypadku nadal prowadzić działalność i w jak największym stopniu ograniczyć straty poniesione w wyniku takiego zakłócenia;

d) zmiana art. 6c ust. 4 pkt 3 ustawy – Prawo bankowe nawiązuje do zmiany art. 6c ust. 1 pkt 1 ustawy – Prawo bankowe, wynikającej z implementacji dyrektywy 2022/2556, która została wyjaśniona powyżej. KNF w związku ze swoimi uprawnieniami odnośnie powierzania czynności w ramach outsourcingu i podoutsourcingu bankowego będzie mogła żądać od banku dodatkowych dokumentów i wyjaśnień w postaci strategii i planów awaryjnych oraz strategii i planów na rzecz ciągłości działania, w tym w zakresie ICT, oraz planów reagowania i przywracania sprawności ICT w odniesieniu do systemów ICT wspierających wszystkie funkcje w zakresie objętym umową powierzającą wykonywanie czynności;

4) zmiana obejmująca dodanie art. 9cf ustawy – Prawo bankowe zobowiązuje banki do posiadania sieci i systemów teleinformatycznych, które będą ustanowione i zarządzane zgodnie z rozporządzeniem 2022/2554;

5) dodanie w art. 133 ust. 4a ustawy – Prawo bankowe (art. 3 pkt 6), zgodnie z którym w badaniu i ocenie nadzorczej banku KNF będzie uwzględniała wyniki testów operacyjnej odporności finansowej, przeprowadzanych zgodnie z rozdziałem IV rozporządzenia 2022/2554, służy implementacji art. 4 pkt 4 wdrażanej dyrektywy 2022/2556. Przepis ten umożliwi organowi nadzoru skutecznie identyfikować ryzyko związane z wykorzystaniem technologii informacyjno-komunikacyjnych (ICT) oraz monitorowanie zarządzania nim przez podmioty nadzorowane.

**3. zmiany w ustawie z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi**

**Art. 3** wprowadza zmiany do ustawyz dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, mające na celu przede transpozycję przepisów dyrektywy 2022/2556 w zakresie art. 1 i 3 , które zmieniają odpowiednio dyrektywę Parlamentu Europejskiego i Rady 2009/65/WE z dnia 13 lipca 2009 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS) (zwaną dalej „dyrektywą 2009/65/WE”), oraz dyrektywę Parlamentu Europejskiego i Rady 2011/61/UE z dnia 8 czerwca 2011 r. w sprawie zarządzających alternatywnymi funduszami inwestycyjnymi i zmiany dyrektyw 2003/41/WE i 2009/65/WE oraz rozporządzeń (WE) nr 1060/2009 i (UE) nr 1095/2010 (zwaną dalej "dyrektywą 2011/61/UE"). Wdrożenie wymienionych dyrektyw w prawie krajowym zostało dokonane w ustawie z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, a zatem zmiany tych dyrektyw również powinny znaleźć swoje odzwierciedlenie na poziomie nowelizowanej ustawy. Wprowadzane do ustawy zmiany obejmują:

1) dodanie w art. 2 ustawyz dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi pkt 2m ma na celu uzupełnienie słowniczka nowelizowanej ustawy o skróconą nazwę rozporządzenia 2022/2554, w celu posługiwania się tym skrótem na potrzeby odesłań do niego w  dalszych przepisach ustawy;

2) dodanie w art. 48 w ust. 2b ustawyz dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi pkt 1a służy implementacji art. 1 pkt 1 dyrektywy 2022/2556. Artykuł ten zmienia art. 12 ust. 1 akapit drugi lit. a dyrektywy 2009/65/WE zobowiązując właściwe organy spółki zarządzającej, aby spółka taka stosowała racjonalne rozwiązania w zakresie kontroli i bezpieczeństwa na potrzeby elektronicznego przetwarzania danych również w odniesieniu do sieci i systemów informatycznych utworzonych i zarządzanych zgodnie z rozporządzeniem 2022/2554. Zmieniany art. 12 dyrektywy 2009/65/WE określa w szczególności warunki działalności spółek zarządzających, które w prawie krajowym zostały między innymi wdrożone w art. 48 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi. Dodawane przepisy znajdą zastosowanie do towarzystwa funduszy inwestycyjnych, które jest odpowiednikiem krajowym spółki zarządzającej, o której mowa w art. 12 dyrektywy 2009/65/WE. Wyjaśnienia również wymaga, że szczątkowe wymagania w odniesieniu do systemów informatycznych wykorzystywanych przez towarzystwa funduszy inwestycyjnych zawarte są w rozporządzeniu Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 18 listopada 2020 r. w sprawie sposobu, trybu oraz warunków prowadzenia działalności przez towarzystwa funduszy inwestycyjnych (Dz. U. poz. 1605), niemniej kwestia ta, z uwagi na jej istotę wymaga również uregulowania na poziomie ustawy;

3) dodanie w art. 70 l w ust. 2 ustawyz dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi pkt 1a ma na celu wdrożenie art. 3 dyrektywy 2022/2556, który nowelizuje art. 18 dyrektywy 2011/61/UE. Pomimo, że art. 18 dyrektywy 2011/61/UE nadawane jest nowe brzmienie, to faktyczne zmiany w ust. 1 tego przepisu ograniczają się do dodania wymagania, aby zarządzający alternatywnym funduszem inwestycyjnym stosował racjonalne rozwiązania w zakresie kontroli i bezpieczeństwa na potrzeby elektronicznego przetwarzania danych powinny mieć również zastosowanie w odniesieniu do sieci i systemów informatycznych utworzonych i zarządzanych zgodnie z rozporządzeniem 2022/2554. Zmiany w art. 18 ust. 2 ww. dyrektywy skierowane są do Komisji Europejskiej i z tego względu nie podlegają implementacji w nowelizowanej ustawie. Odpowiednikami w prawie krajowym zarządzających alternatywnymi funduszami inwestycyjnymi (ZAFI) są zarządzający ASI, z kolei wymogi organizacyjne w odniesieniu do tych podmiotów zostały sformułowane w nowelizowanej ustawie, co do zasady w art. 70l ustawyz dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi. Podobnie jak w przypadku towarzystw funduszy inwestycyjnych w projekcie przewidziano ustanowienie na poziomie ustawy wymagania aby zarządzający ASI wdrożył rozwiązania techniczne i organizacyjne zapewniające bezpieczeństwo i kontrolę środowiska teleinformatycznego i przetwarzania w nim danych, w tym w odniesieniu do sieci i systemów informatycznych utworzonych i zarządzanych zgodnie z rozporządzeniem 2022/2554.

**4. zmiany w ustawie z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (art. 4)**

**Art. 4** wprowadza zmiany do ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, mające na celu transpozycję przepisów dyrektywy 2022/2556 w zakresie implementacji art. 5 i 6 tej dyrektywy. Przepis art. 5 zmienia dyrektywę 2014/59/UE Parlamentu Europejskiego i Rady 2014/59/UE z dnia 15 maja 2014 r.ustanawiającą ramy na potrzeby prowadzenia działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji w odniesieniu do instytucji kredytowych i firm inwestycyjnych oraz zmieniającą dyrektywę Rady 82/891/EWG i dyrektywy Parlamentu Europejskiego i Rady2001/24/WE, 2002/47/WE, 2004/25/WE, 2005/56/WE, 2007/36/WE, 2011/35/UE, 2012/30/UE i 2013/36/EU oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 i (UE) nr 648/2012 (zwaną dalej „dyrektywą 2014/59/UE”). Przepis art. 6 zmienia dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniającą dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (zwaną dalej "dyrektywą 2014/65/UE"). Wdrożenie wymienionych dyrektyw w prawie krajowym zostało dokonane, co do zasady, w ustawie z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, a zatem zmiany powinny znaleźć swoje odzwierciedlenie na poziomie nowelizowanej ustawy. Wprowadzane do ustawy zmiany obejmują:

1) dodanie w art. 3 pkt 4zg ustawy o obrocie instrumentami finansowymi ma na celu uzupełnienie słowniczka nowelizowanej ustawy o skróconą nazwę rozporządzenia 2022/2554 w celu posługiwania się tym skrótem na potrzeby odesłań do rozporządzenia w  dalszych przepisach ustawy;

2) zmiany przewidziane w art. 74e ust. 1 pkt 1 i 4 oraz ust. 2 ustawy o obrocie instrumentami finansowymi służą wdrożeniu art. 6 pkt 2 dyrektywy 2022/2556, który zmienia art. 17 ust. 1 dyrektywy 2014/65/UE. Zmiana art. 17 ust. 7 lit. a dyrektywy 2014/65/UE nie podlega implementacji gdyż skierowana jest do Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych. Nowelizowany art. 17 dyrektywy 2014/65/UE reguluje kwestie związane z zasadami dokonywania przez firmy inwestycyjne handlu algorytmicznego. Przepisy te zostały transponowane w prawie krajowym w art. 74e nowelizowanej ustawy. W art. 74e ust. 1 pkt 1 ustawy o obrocie instrumentami finansowymi dodano wymaganie, aby zapewnienie odporności i wydajności sieci i systemów teleinformatycznych wykorzystywanych przez firmy inwestycyjne na potrzeby handlu algorytmicznego było zgodne z rozdziałem II rozporządzenia 2022/2554, co odpowiada zmianie dokonanej w art. 17 ust. 1 wierszu pierwszym dyrektywy 2014/65/UE. W art. 74e ust. 1 pkt 4 ustawy o obrocie instrumentami finansowymi dodano wymaganie, aby firma inwestycyjna prowadząca handel algorytmiczny posiadała strategię i plany na rzecz ciągłości działania w zakresie ICT oraz planów reagowania i przywraca sprawności tej technologii, o których mowa w art. 11 rozporządzenia 2022/2554, co wynika z art. 17 ust. 1 akapitu 3 wiersza dwa i trzy dyrektywy 2014/65/UE. Z kolei w art. 74e ust. 2 ustawy o obrocie instrumentami finansowymi nakłada na takie firmy inwestycyjne obowiązek aby monitorowały one działanie urządzeń i systemów teleinformatycznych oraz przeprowadzały testy w zakresie oceny prawidłowości ich działania również w celu identyfikowania i eliminacji potencjalnych lub rzeczywistych naruszeń wymogów, o których mowa w rozdziałach II i IV rozporządzenia 2022/2554;

3) zmiana przewidziana w art. 83a ust. 1 ustawy o obrocie instrumentami finansowymi ma na celu implementację art. 6 pkt 1 lit. a dyrektywy 2022/2556, który zmienia art. 16 ust. 4 dyrektywy 2014/65/UE. W nowelizowanym art. 83a ust. 1, zgodnie z implementowaną dyrektywą, dodany wymóg aby również stosowane przez firmę inwestycyjną systemy oparte na technologii informacyjno-komunikacyjnej (ITC) ustanowione i zarządzane zgodnie z art. 7 rozporządzenia 2022/2554, zapewniały bezpieczeństwo i ciągłość świadczonych przez firmę inwestycyjną usług maklerskich oraz ochronę interesów klientów i informacji poufnych lub stanowiących tajemnicę zawodową. Implementacja art. 6 pkt 1 lit b dyrektywy 2022/2556 zostanie dokonana na poziomie rozporządzenia Ministra Finansów z dnia 29 maja 2018 r. w sprawie szczegółowych warunków technicznych i organizacyjnych dla firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy o obrocie instrumentami finansowymi, i banków powierniczych (Dz. U. poz. 1111).

Zmiany przewidziane w art. 6 pkt 3 i 4 lit. a i b dyrektywy 2022/2556 zostaną zaimplementowane w rozporządzeniu Ministra Finansów z dnia 19 kwietnia 2019 r. w sprawie szczegółowych warunków, jakie musi spełniać rynek regulowany oraz platforma aukcyjna (Dz. U. poz. 726). Natomiast zmiany przewidziane w art. 6 pkt 4 lit. c skierowane są do Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych i nie podlegają implementacji do prawa krajowego;

4) art. 110 zj ust. 3 ustawy określa elementy planu naprawy domu maklerskiego o którym mowa w art. 110zj ust. 1 i 2 ustawy. Zmiana w art. 110zj ust. 3 pkt 16 ustawy, ma na celu implementację art. 5 pkt 2 pkt a) dyrektywy 2022/2556, przewidującym zmianę w pkt 16 sekcji A załącznika do dyrektywy 2014/59/UE oraz doprecyzowuje jeden z elementów planu naprawy uwzględniając odniesienie do sieci i systemów informatycznych utworzonych i zarządzanych zgodnie z rozporządzeniem 2022/2554.

5. **zmiany w ustawie z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (art. 5 )**

**Art. 5** wprowadza zmiany w ustawie z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym mające na celu zapewnienie stosowania przepisów rozporządzenia 2022/2554 określających zadania i uprawienia właściwych organów w rozumieniu art. 46. Art. 46 rozporządzenia 2022/2554 wskazuje, że właściwe organy, zapewniają przestrzeganie niniejszego rozporządzenia, zgodnie z uprawnieniami przyznanymi im na mocy aktów prawnych wymienionych w tym przepisie. W polskim systemie prawnym, dla aktów prawnych wymienionych w ww. przepisie, organem właściwym jest KNF.

● **regulacje o charakterze ogólnym** (art. 5 pkt 1 – 5)

Art. 5 pkt 1 wprowadza zmiany w art. 1 w ust. 2 ustawy o nadzorze nad rynkiem finansowym wskazując, w dodawanym pkt 15, że nadzór nad rynkiem finansowym obejmuje również nadzór w zakresie przewidzianym przepisami rozporządzenia 2022/2554.

Art. 5 pkt 2 wprowadza do ustawy o nadzorze nad rynkiem finansowym art. 3w, który wskazuje, że KNF jest właściwym organem w rozumieniu art. 46 rozporządzenia 2022/2554. Celem projektowanego art. 3w jest wyznaczenie organu odpowiedzialnego za nadzór nad spełnianiem wymogów wynikających z rozporządzenia 2022/2554.

Ponadto w art. 5 pkt 3 ustawy o nadzorze nad rynkiem finansowym proponuje się uzupełnić katalog zadań KNF (dodawany w art. 4 w ust. 1 pkt 3c) o zadanie polegające na podejmowaniu działań mających na celu zapewnienie przestrzegania przepisów rozporządzenia 2022/2554.

Art. 5 pkt 4 projektu ustawy dostosowuje art. 4a ust. 3 ustawy o nadzorze nad rynkiem finansowym, określający maksymalny termin przetwarzania danych osobowych, o których mowa w ust. 1 tego przepisu, do art. 56 ust. 2 rozporządzenia 2022/2554, wskazując, że dane osobowe, o których mowa w art. 4a ust. 1, KNF przetwarza przez okres 25 lat, z wyłączeniem danych osobowych, o których mowa w art. 56 ust. 1 rozporządzenia 2022/2554, które KNF przetwarza przez okres 15 lat.

Art. 5 pkt 5 wprowadza zmiany w art. 17 cc ustawy o nadzorze nad rynkiem finansowym, który w obowiązującym stanie prawnym reguluje uprawnienia KNF dotyczące zapewnienia bezpieczeństwa systemów teleinformatycznych w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Proponuje się uzupełnienie art. 17cc ust. 1 ustawy o nadzorze nad rynkiem finansowym, który stanowi, że w zakresie niezbędnym do wykonywania zadania, o którym mowa w art. 4 ust. 1 pkt 3b, KNF może przekazywać informacje, w tym chronione na podstawie odrębnych ustaw, podmiotowi podlegającemu nadzorowi KNF, jeżeli ich przekazanie jest niezbędne do podjęcia przez ten podmiot działań polegających na przeciwdziałaniu zagrożeniom w zakresie bezpieczeństwa systemów teleinformatycznych, w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Wprowadzane w art. 17cc ust. 1 ustawy o nadzorze nad rynkiem finansowym zmiany mają na celu uwzględnienie możliwości przekazywania przez KNF informacji, o których mowa w art. 17cc ust. 1 również gdy takie przekazanie jest niezbędne do podjęcia przez ten podmiot działań polegających na przeciwdziałaniu zagrożeniom sieci i systemów teleinformatycznych w rozumieniu przepisów rozporządzenia 2022/2554.

Ponadto projektowany art. 17 cc ust. 3 ustawy o nadzorze nad rynkiem finansowym ma na celu rozszerzenie możliwości pozyskiwania przez KNF informacji, dokumentów lub wyjaśnień w zakresie niezbędnym do wykonywania zadania, o którym mowa w art. 4 ust. 1 pkt 3c, co uwzględnia wdrożenie przepisów rozporządzenia, upoważniających właściwe organy do pozyskiwania stosownych informacji w celu zapewnienia przestrzegania postanowień rozporządzenia. Wskazanie podstawy prawnej do żądania od podmiotu podlegającego nadzorowi KNF informacji, dokumentów lub wyjaśnień, w zakresie określonym w przepisach rozporządzenia 2022/2554, jest konieczne dla zapewnienia stosowania przepisów rozporządzenia wskazujących, że podmioty finansowe w rozumieniu rozporządzenia 2022/2554 przedstawiają określone informacje, dokumenty etc. na żądanie organu właściwego w rozumieniu art. 46 rozporządzenia 2022/2554, dotyczy to np. art. 6 ust. 3 i 5, art. 11 ust. 10, art. 13 ust. 2 akapit 2.

Ponadto zmiany art. 17cc ustawy o nadzorze nad rynkiem finansowym obejmują wprowadzenie ust. 4 i 5 nakładających obowiązek przekazywania wskazanych w tym przepisie informacji do KNF, z uwagi na konieczność zapewnienia wdrożenia odpowiednio: art. 45 ust. 3 w zw. z art. 45 ust.1 rozporządzenia 2022/2554 (projektowany art. 17cc ust. 4) oraz art. 11 ust. 9 rozporządzenia 2022/2554 (projektowany art. 17cc ust. 5).

● **szczegółowe regulacje dotyczące nadzoru nad podmiotami finansowymi w zakresie zapewnienia operacyjnej odporności cyfrowej sektora finansowego (art. 5 pkt 6)**

Art. 5 pkt 6 projektu wprowadza do ustawy o nadzorze nad rynkiem finansowym rozdział 2c pt. „Nadzór nad podmiotami finansowymi w zakresie zapewnienia operacyjnej odporności cyfrowej sektora finansowego” (projektowane art. 18 za – 18zi), w którym zostaną umieszczone przepisy szczegółowo regulujące kompetencje i zadania KNF wynikające z rozporządzenia 2022/2554, w szczególności zapewniające wdrożenie art. 26, art. 42 oraz art. 50 i 51.

1. **kontrola działalności podmiotów finansowych, w zakresie zapewnienia operacyjnej odporności cyfrowej sektora finansowego**

Projektowany art. 18za stanowi podstawę do wszczęcia przez KNF kontroli zgodności działalności z przepisami rozporządzenia 2022/2554, w zakresie zapewnienia operacyjnej odporności cyfrowej sektora finansowego, wymienionych w tym przepisie podmiotów finansowych:

1) banku krajowego w rozumieniu art. 4 ust. 1 pkt 1 ustawy – Prawo bankowe,

2) banku zagranicznego w rozumieniu art. 4 ust. 1 pkt 2 ustawy – Prawo bankowe,

3) banku hipotecznego, o którym mowa w ustawie z dnia 29 sierpnia 1997 r. o listach zastawnych i bankach hipotecznych,

4) banku spółdzielczego w rozumieniu art. 2 pkt 1 ustawy z dnia 7 grudnia 2000 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających,

5) banku zrzeszającego w rozumieniu art. 2 pkt 2 ustawy z dnia 7 grudnia 2000 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających,

6) instytucji kredytowej w rozumieniu art. 4 ust. 1 pkt 17 ustawy – Prawo bankowe,

7) Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej, o której mowa w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych,

8) spółdzielczej kasy oszczędnościowo-kredytowej, o której mowa w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych,

9) firmy inwestycyjnej w rozumieniu art. 3 pkt 33 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

10) domu maklerskiego stosującego rozporządzenie nr 575/2013 w rozumieniu art. 4 ust. 1 pkt 44a ustawy – Prawo bankowe,

11) pracowniczego towarzystwa w rozumieniu art. 8 pkt 9 ustawy z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych,

12) zarządzającego ASI w rozumieniu art. 2 pkt 3a ustawy o funduszach inwestycyjnych prowadzącego działalność na podstawie zezwolenia,

13) towarzystwa posiadającego zezwolenie na zarządzanie alternatywnymi funduszami inwestycyjnymi, wydanego na podstawie art. 38 ust. 1 ustawy o funduszach inwestycyjnych,

14) towarzystwa funduszy inwestycyjnych zarządzającego otwartym funduszem inwestycyjnym, o którym mowa w ustawie o funduszach inwestycyjnych,

15) podmiotu prowadzącego system obrotu instrumentami finansowymi w rozumieniu art. 3 pkt 9a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

16) centralnego depozytu papierów wartościowych w rozumieniu art. 3 pkt 21a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

17) CCP w rozumieniu art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

18) zatwierdzonego podmiotu publikującego w rozumieniu art. 3 pkt 33a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

19) zatwierdzonego mechanizmu sprawozdawczego w rozumieniu art. 3 pkt 33c ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

20) administratora w rozumieniu art. 3 pkt 57 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

21) dostawcy świadczącego usługę dostępu do informacji o rachunku w rozumieniu art. 2 pkt 4e ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,

22) instytucji pieniądza elektronicznego w rozumieniu art. 2 pkt 10a ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,

23) krajowej instytucji płatniczej w rozumieniu art. 2 pkt 11 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,

24) zakładu reasekuracji, o którym mowa w ustawie o działalności ubezpieczeniowej i reasekuracyjnej,

25) zakładu ubezpieczeń, o którym mowa w ustawie o działalności ubezpieczeniowej i reasekuracyjnej,

26) pośrednika ubezpieczeniowego w rozumieniu art. 3 ust. 1 pkt 15 ustawy z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń,

27) dostawcy usług finansowania społecznościowego w rozumieniu art. 2 pkt 3 ustawy z dnia 7 lipca 2022 r. o finansowaniu społecznościowym dla przedsięwzięć gospodarczych i pomocy kredytobiorcom,

28) dostawcy usług w zakresie kryptowalut w rozumieniu art. 3 ust. 1 pkt 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz. Urz. L 150 z 9.06.2023, str. 40),

29) agencji ratingowej w rozumieniu art. 3 ust. 1 lit. b rozporządzenia Parlamentu Europejskiego i Rady nr 1060/2009 z dnia 16 września 2009 r. w sprawie agencji ratingowych,

30) repozytorium sekurytyzacji w rozumieniu art. 2 pkt 23 rozporządzenia 2017/2402,

31) repozytorium transakcji w rozumieniu art. 2 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji.

Katalog podmiotów kontrolowanych stanowi odzwierciedlenie w krajowym porządku prawnym, katalogu podmiotów finansowych zobowiązanych do stosowania rozporządzenia 2022/2554, wskazanych w art. 2 ust. 1 tego rozporządzenia.

Zgodnie z projektowanym art. 18za ust. 2 ww. kontroli nie podlegają następujące podmioty finansowe:

1) pracownicze towarzystwo w rozumieniu art. 8 pkt 9 ustawy z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych, które obsługuje pracownicze programy emerytalne liczące łącznie nie więcej niż 15 uczestników;

2) zarządzający ASI w rozumieniu art. 2 pkt 3a ustawy o funduszach inwestycyjnych prowadzący działalność na podstawie wpisu do rejestru zarządzających ASI;

3) podmioty, o których mowa w art. 32 ust. 2 ustawy o funduszach inwestycyjnych;

4) pośrednik ubezpieczeniowy, o którym mowa w art. 3 ust. 1 pkt 15 ustawy z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń, będący mikroprzedsiębiorstwem w rozumieniu art. 3 pkt 60 rozporządzenia 2022/2554, małym przedsiębiorstwem w rozumieniu art. 3 pkt 63 rozporządzenia 2022/2554 lub średnim przedsiębiorstwem w rozumieniu art. 3 pkt 64 rozporządzenia 2022/2554.

Katalog podmiotów wyłączonych z zakresu kontroli ma na celu zapewnienie stosowania art. 2 ust. 3 rozporządzenia 2022/2554, stanowiącego wyłączenie z obowiązku stosowania tego rozporządzenia przez podmioty w nim wymienione.

W tym miejscu należy również wskazać, że ustawodawca krajowy nie zdecydował się na wdrożenie do polskiego porządku prawnego wyłączenia, o którym mowa w art. 2 ust. 4 rozporządzenia 2022/2554, tj. wyłączenia podmiotów, o których mowa w art. 2 ust. 5 pkt 4–23 dyrektywy 2013/36/UE, mających siedzibę na ich odpowiednich terytoriach. W polskim systemie prawnym ww. podmiotom odpowiadają spółdzielcze kasy oszczędnościowo - kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo – kredytowych. Z uwagi na zakres działalności ww. podmiotów, określony art. 3 ww. ustawy, który obejmuje gromadzenie środków pieniężnych wyłącznie swoich członków, udzielanie im pożyczek i kredytów, przeprowadzanie na ich zlecenie rozliczeń finansowych oraz wykonywanie dystrybucji ubezpieczeń na zasadach określonych w ustawie z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń, wyłączenie tych podmiotów z zakresu stosowania wdrażanego rozporządzenia 2022/2554, a co za tym idzie, kontroli, nie wydaje się zasadne, ponieważ zakres czynności kas jest zbliżony do zakresu czynności innych podmiotów finansowych np. banków, które zostały objęte zakresem regulacji rozporządzenia i obarczone są podobnym ryzykiem.

Ponadto przepis art. 18za ustawy o nadzorze nad rynkiem finansowym określi osoby uprawnione do kontroli (art. 18za ust.4) oraz uprawnienia w toku kontroli (art. 18za ust. 5). Katalog uprawnień jest zgodny z przepisem art. 50 rozporządzenia 2022/2554, który wskazuje uprawnienia organu właściwego w rozumieniu art. 46 tego rozporządzenia.

Projektowany art. 18zi ustawy o nadzorze nad rynkiem finansowym wskazuje, że  do kontroli, o której mowa w art. 18za ust. 1ust. 1 tej ustawy, stosuje się przepisy, w zakresie kontroli danego rodzaju podmiotu finansowego.

Wynikiem zmian wprowadzających nowy rodzaj kontroli, określony w projektowanym art. 18za ustawy o nadzorze nad rynkiem finansowym, jest wprowadzenie zmian w art. 20b tej ustawy (art. 5 pkt. 9) określających odpowiedzialność karną za utrudnianie lub udaremnianie przeprowadzenia kontroli.

1. **uprawnienie do żądania udostępnienia rejestrów przesyłu danych**

Ponadto na mocy projektowanego art. 18zb ust. 1 ustawy o nadzorze nad rynkiem finansowym KNF będzie uprawniona, w celu ustalenia, czy doszło do naruszenia przepisów rozporządzenia 2022/2554, w szczególności gdy wyniki kontroli, o której mowa w art. 18za ust. 1 ustawy o nadzorze nad rynkiem finansowym, wskazują na uzasadnione podejrzenie naruszenia, do żądania od przedsiębiorcy telekomunikacyjnego, w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, udostępnienia rejestrów przesyłu danych będących w posiadaniu tego przedsiębiorcy, na jego koszt, za okres, w którym wystąpiła możliwość naruszenia. Wskazane uprawnienie stanowi transpozycję art. 50 ust. 4 lit. d rozporządzenia 2022/2554.

1. **decyzje KNF w przypadku naruszenia obowiązków określonych w rozporządzeniu 2022/2554**

Projektowany art. 18zf ust. 1 ustawy o nadzorze nad rynkiem finansowym wskazuje rodzaje decyzji, jakie KNF może podjąć, gdy działalność podmiotu finansowego, o którym mowa w art. 18za ust. 1, jest wykonywana z naruszeniem przepisów rozdziału II sekcji I oraz sekcji II, z wyłączeniem art. 11 ust. 11, art. 15 oraz art.16 ust. 3, rozdziału III, z wyłączeniem art. 18 ust. 3 i 4, art. 19 ust. 6–8, art. 20–22, rozdziału IV, z wyłączeniem art. 26 ust. 9 –11, rozdziału V sekcji I, z wyłączeniem art. 28 ust. 9 i 10, art. 31 ust. 12 oraz art. 45 ust. 3 rozporządzenia 2022/2554. Należy wskazać, że projektodawca zdecydował, w celu zapewnienia czytelności regulacji, na określenie zakresu odpowiedzialności podmiotów finansowych, poprzez wskazanie przepisów, których naruszenie nie podlega odpowiedzialności, określonej w projektowanym art. 18zf. Należy podkreślić, że zdecydowana większość przepisów rozporządzenia 2022/2554 skierowana jest do podmiotów finansowych i wskazuje obowiązki lub wymogi mające na celu zapewnienie cybrebezpieczeństwa, nie wydaje się zatem zasadne wymienianie wszystkich przepisów poszczególnych rozdziałów rozporządzenia 2022/2554. Przepisy, objęte wyłączeniem, nie stanowią o obowiązkach podmiotów finansowych – są to przede wszystkim przepisy skierowane do organów nadzorczych, o których mowa w art. 31 ust. 1 lit. b oraz organów właściwych w rozumieniu art. 46 rozporządzenia 2022/2554.

Zgodnie z projektowanym art. 18zf ustawy o nadzorze nad rynkiem finansowym KNF może, w drodze decyzji:

1) nakazać osobie fizycznej, osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej zaprzestanie danego zachowania oraz powstrzymanie się od takiego zachowania w przyszłości (art. 50 ust. 4 lit. a rozporządzenia 2022/2554);

2) zakazać osobie odpowiedzialnej za to naruszenie pełnienia funkcji członka zarządu lub rady nadzorczej albo innej funkcji kierowniczej tego podmiotu przez okres nie krótszy niż miesiąc i nie dłuższy niż rok (art. 50 ust. 5 rozporządzenia 2022/2554);

3) nałożyć karę pieniężną (art. 50 ust. 4 lit. c rozporządzenia 2022/2554) do wysokości nieprzekraczającej:

a) w przypadku osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej:

- kwoty 20 869 500 zł lub 10% przychodów netto ze sprzedaży towarów i usług oraz operacji finansowych, a w przypadku zakładu ubezpieczeń lub zakładu reasekuracji – 10% składki przypisanej brutto, wykazanych w ostatnim sprawozdaniu finansowym za rok obrotowy, zatwierdzonym przez organ zatwierdzający, albo

- dwukrotności kwoty korzyści uzyskanych lub strat unikniętych w wyniku tego naruszenia – w przypadku gdy jest możliwe ich ustalenie,

b) w przypadku osoby fizycznej, w tym odpowiedzialnej za to naruszenie, która w tym okresie pełniła obowiązki członka zarządu tego podmiotu – kwoty 3 042 410 zł.

Ponadto KNF będzie mogła wydać publiczne oświadczenie, w którym wskazuje imię i nazwisko osoby fizycznej albo firmę lub nazwę osoby prawnej lub jednostki nieposiadającej osobowości prawnej, odpowiedzialnych za naruszenie, oraz charakter tego naruszenia.

Projektowany art. 18zf ust. 3 ustawy o nadzorze nad rynkiem finansowym określa sposób ustalenia kary pieniężnej, w przypadku gdy osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, o której mowa w ust. 1 pkt 3 lit. a, jest jednostką dominującą albo jednostką zależną jednostki dominującej, która ma obowiązek sporządzać skonsolidowane sprawozdania finansowe zgodnie z ustawą z dnia 29 września 1994 r. o rachunkowości. Zgodnie z tym przepisem karę pieniężną, o której mowa w ust. 1 pkt 3 lit. a, ustala się na podstawie przychodów netto ze sprzedaży towarów i usług oraz operacji finansowych, a w przypadku zakładu ubezpieczeń i zakładu reasekuracji – składki przypisanej brutto, wykazanych w ostatnim rocznym skonsolidowanym sprawozdaniu finansowym zatwierdzonym przez organ zatwierdzający jednostki dominującej. Projektowany art. 18zf ust. 2 ustawy o nadzorze nad rynkiem finansowym jest ściśle związany z ust. 1 i precyzuje jego treść w stosunku do podmiotów sporządzających skonsolidowane sprawozdanie finansowe, wartości kar pozostawiając bez zmian. Kara pieniężna określona w tym przepisie jest obliczana z uwzględnieniem charakteru działalności tych podmiotów. Analogiczne rozwiązanie jest stosowane także w innych regulacjach ustawowych dotyczących podmiotów tego rodzaju.

Decyzje, o których mowa w art. 18zf ust. 1 pkt 1 i 2 ustawy o nadzorze nad rynkiem finansowym, są natychmiast wykonalne, w celu zapewnienia natychmiastowego zaprzestania zachowań stanowiących naruszenie przepisów rozporządzenia 2022/2554, a także w celu odsunięcia od kierowania przedsiębiorstwem osób, które ponoszą odpowiedzialność za decyzje skutkujące naruszeniem.

Komisja, wydając decyzje, o których mowa w art. 18zf ust. 1 ustawy o nadzorze nad rynkiem finansowym, uwzględnia okoliczności, o których mowa w art. 51 ust. 2 rozporządzenia 2022/2554, zgodnie z którym ustalając rodzaj i poziom kary administracyjnej lub środka naprawczego, które mają zostać nałożone na mocy art. 50, właściwe organy biorą pod uwagę zakres, w jakim dane naruszenie ma charakter umyślny lub jest wynikiem zaniedbania, a także wszystkie inne stosowne okoliczności, w tym również, w stosownych przypadkach:

1. istotność i wagę naruszenia oraz czas jego trwania;
2. stopień przyczynienia się osoby fizycznej lub prawnej do naruszenia;
3. sytuację finansową odpowiedzialnej osoby fizycznej lub prawnej;
4. skalę korzyści uzyskanych lub strat unikniętych przez odpowiedzialną osobę fizyczną lub prawną, o ile można je ustalić;
5. straty poniesione przez osoby trzecie w wyniku naruszenia, o ile można je ustalić;
6. poziom współpracy odpowiedzialnej osoby fizycznej lub prawnej z właściwym organem, bez uszczerbku dla konieczności zapewnienia wydania uzyskanych korzyści lub wyrównania strat unikniętych przez tę osobę fizyczną lub prawną;
7. uprzednie naruszenia popełnione przez odpowiedzialną osobę fizyczną lub prawną.

Ponadto, zgodnie z projektowanym art. 18zg ustawy o nadzorze nad rynkiem finansowym decyzje, o których mowa w art. 18zf ust. 1 pkt 3, są udostępniane na stronie internetowej KNF, zgodnie z art. 54 rozporządzenia 2022/2554 przez okres 5 lat, licząc od dnia ich udostępnienia. Obowiązek udostępniania decyzji nakładających kary pieniężne wynika z art. 54 rozporządzenia 2022/2554.

W odniesieniu do nakładanych przez KNF decyzji o karach pieniężnych należy również wskazać, że zgodnie z art. 5 pkt 8 projektu ustawy, który nadaje nowe brzmienie art. 19e ust. 1 i 2 ustawy o nadzorze nad rynkiem finansowym, wpływy z tytułu kar pieniężnych nakładanych przez Komisję na podstawie nowego art. 18zf ust. 1 pkt 3 ustawy o nadzorze nad rynkiem finansowym stanowić będą przychód Funduszu Edukacji Finansowej, o którym mowa w ustawie z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego, o Rzeczniku Finansowym i o Funduszu Edukacji. Projekt uzupełnia przepis art. 19e ustawy o nadzorze nad rynkiem finansowym o odesłanie do projektowanych przepisów dotyczących kar (art. 18zf ust. 1 pkt 3 ustawy o nadzorze nad rynkiem finansowym), które – podobnie jak inne kary nakładane przez KNF – będą przychodem Funduszem Edukacji Finansowej. Konieczne jest uregulowanie przeznaczenia wpływów z tytułu kar nakładanych przez KNF, bo nie są to dochody budżetu (KNF nie jest już dysponentem części budżetowej).

W zakresie środków mających na celu zapewnienie przestrzegania przepisów rozporządzenia 2022/2554 projektowany art. 18ze ustawy o nadzorze nad rynkiem finansowym zapewnia wdrożenie postanowień art. 42 rozporządzenia 2022/2554 w zakresie procedury wydawania decyzji, o której mowa w art. 42 ust. 6 rozporządzenia 2022/2554, nakazującej podmiotom finansowym, jako środek ostateczny, tymczasowe zawieszenie, w części albo w całości, korzystania z usługi świadczonej przez kluczowego zewnętrznego dostawcę usług ICT lub jej wdrażania do czasu wyeliminowania ryzyka zidentyfikowanego w zaleceniach skierowanych do kluczowych zewnętrznych dostawców usług ICT, a także, w razie potrzeby, nakazania podmiotom finansowym, wypowiedzenia, w części lub w całości, stosownych ustaleń umownych zawartych z kluczowymi zewnętrznymi dostawcami usług ICT.

Podejmując decyzję, o której mowa w art. 42 ust. 6 rozporządzenia 2022/2554, KNF określa czas jej obowiązywania. Decyzja ta obowiązuje nie dłużej niż do czasu wyeliminowania ryzyka zidentyfikowanego w zaleceniach, o których mowa o których mowa w art. 35 ust. 1 lit. d rozporządzenia 2022/2554, w odniesieniu do zewnętrznego dostawcy usług ICT w rozumieniu art. 3 pkt 19 rozporządzenia 2022/2554, i jest natychmiast wykonalna. Przedłużenie obowiązywania decyzji będzie wymagało wydania decyzji w tym zakresie. KNF przed wydaniem decyzji może skonsultować się z organami, o których mowa w art. 42 ust. 5 rozporządzenia 2022/2554.

Podejmując ww. decyzję, KNF uwzględnia okoliczności, o których mowa w art. 42 ust. 8 rozporządzenia 2022/2554, zgodnie z którym po otrzymania sprawozdań, o których mowa w art. 35 ust. 1 lit. c, właściwe organy podejmują decyzję, o której mowa w art. 42 ust. 6 tego rozporządzenia, biorąc pod uwagę rodzaj i skalę ryzyka, które nie zostało wyeliminowane przez kluczowego zewnętrznego dostawcę usług ICT, a także istotność braku zgodności, uwzględniając następujące kryteria:

1. wagę braku zgodności i czas jego trwania;
2. kwestię, czy brak zgodności ujawnił poważne słabości w procedurach, systemach zarządzania, zarządzaniu ryzykiem i kontrolach wewnętrznych kluczowego zewnętrznego dostawcy usług ICT;
3. kwestię, czy brak zgodności doprowadził do przestępstwa finansowego lub ułatwił przestępstwo finansowe lub jest w inny sposób związany z takim przestępstwem;
4. kwestię, czy brak zgodności jest wynikiem działania umyślnego lub zaniedbania;
5. kwestię, czy zawieszenie lub wypowiedzenie ustaleń umownych wprowadza ryzyko dla ciągłości działalności gospodarczej danego podmiotu finansowego pomimo wysiłków podejmowanych przez ten podmiot finansowy, by uniknąć zakłócenia w świadczeniu przez niego usług;

|  |
| --- |
| 1. w stosownych przypadkach opinię właściwych organów wyznaczonych lub ustanowionych zgodnie z dyrektywą 2022/2555 jako odpowiedzialne za nadzór nad kluczowym lub ważnym podmiotem objętym zakresem stosowania tej dyrektywy, którzy zostali wyznaczeni jako kluczowy zewnętrzny dostawca usług ICT, o którą zwrócono się na zasadzie dobrowolności zgodnie z art. 42 ust. 5. |

Właściwe organy dają podmiotom finansowym odpowiednio dużo czasu na dostosowanie ustaleń umownych z kluczowymi zewnętrznymi dostawcami usług ICT, aby uniknąć szkodliwych skutków dla ich operacyjnej odporności cyfrowej i umożliwić im wdrożenie strategii wyjścia i planów przejściowych, o których mowa w art. 28 rozporządzenia 2022/2554.

1. **wdrożenie art. 26 (zaawansowane testowanie) i 28 (obowiązki informacyjne podmiotów finansowych w zakresie zarządzania ryzykiem) rozporządzenia 2022/2554**

Projektowany art. 18zc ustawy o nadzorze nad rynkiem finansowym ma na celu zapewnienie wdrożenia art. 28 rozporządzenia 2022/2554, z uwagi na powyższe zobowiązuje podmioty finansowe wymienione w art. 18za ust. 1 tej ustawy do przekazywania informacji i sprawozdań, o których mowa w tym przepisie, organowi właściwemu w rozumieniu art. 46 rozporządzenia 2022/2554, tj. KNF. Zgodnie z projektowanym art. 18zc ust. 1 ustawy o nadzorze nad rynkiem finansowym podmioty finansowe w rozumieniu rozporządzenia 2022/2554, przekazują KNF następujące informacje:

- w terminie do dnia 31 stycznia każdego roku informacje, o których mowa w art. 28 ust. 3 akapit trzeci rozporządzenia 2022/2554,

- o których mowa w art. 28 ust. 3 akapit piąty rozporządzenia 2022/2554, niezwłocznie, nie później niż w terminie 14 dni przed dniem związania się postanowieniami umownymi albo od dnia zmiany funkcji.

Informacje, o których mowa w art. 28 ust. 3 akapit trzeci i piąty rozporządzenia 2022/2554, a także informacje, o których mowa w art. 28 ust. 3 akapit czwarty rozporządzenia 2022/2554, są przekazywane za pośrednictwem systemu teleinformatycznego Komisji.

Terminy wskazane w tym przepisie zapewniają realizację obowiązków informacyjnych w optymalnym czasie, w szczególności obowiązek poinformowania KNF o planowanych ustaleniach umownych dotyczących korzystania z usług ICT wspierających krytyczne lub istotne funkcje oraz o tym, że dana funkcja stała się krytyczna lub istotna, wyznaczony na 14 dni przed dniem związania się postanowieniami umownymi albo zmianą funkcji, jest w ocenie projektodawcy, terminem odpowiednim i wystarczającym dla zapewnienia nadzoru w zakresie wskazanym w art. 28 rozporządzenia 2022/2554.

W celu zapewnienia wdrożenia postawień art. 26 rozporządzenia 2022/2554 proponuje się wprowadzenie art. 18zd ustawy o nadzorze nad rynkiem finansowym regulującego zadania KNF dotyczące przeprowadzenia zaawansowanych testów, o których mowa w art. 26 rozporządzenia 2022/2554, oraz sposób postępowania podmiotów finansowych zobowiązanych do przeprowadzania tych testów.

Ponadto art. 5 pkt 7 wprowadza zmiany art. 19a ustawy o nadzorze nad rynkiem finansowym dotyczącego gospodarki finansowej KNF, dodając ust. 8, zgodnie z którym w przypadku otrzymania zwrotu, o którym mowa w art. 43 ust. 1 rozporządzenia 2022/2554, różnicę, o której mowa w ust. 7 zdanie drugie, pomniejsza się o kwotę tego zwrotu. Ww. rozwiązanie ma na celu wdrożenie przepisów wykonawczych, wydanych na podstawie art. 43 rozporządzenia 2022/2554, z których wynika, że zwrot kosztów, o którym mowa w tym przepisie, może nastąpić także na rzecz organu krajowego – przepis ma skutkować tym, że taki zwrot, jeżeli się pojawi, będzie pomniejszał koszty nadzoru, które pokrywają podmioty nadzorowane – w ten sposób nadwyżka wróci na rynek, a nie będzie dodatkowym przychodem.

Dodatkowo, skutecznej realizacji nadzoru nad podmiotami finansowymi służy wprowadzany art. 18zh ustawy o nadzorze nad rynkiem finansowym dotyczący współpracy międzynarodowej, zgodnie z którym KNF współpracuje oraz wymienia informacje i dokumenty z właściwymi organami w rozumieniu art. 46 rozporządzenia 2022/2554 z państw członkowskich Unii Europejskiej lub państw członkowskich Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stron umowy o Europejskim Obszarze Gospodarczym oraz Europejskim Urzędem Nadzoru Bankowego, Europejskim Urzędem Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych i Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych w zakresie niezbędnym do wykonywania obowiązków wynikających z rozporządzenia 2022/2554. Ponadto KNF współpracuje oraz wymienia informacje i dokumenty z odpowiednimi wiodącymi organami nadzorczymi, wyznaczonymi zgodnie z art. 31 ust. 1 lit. b rozporządzenia 2022/2554 oraz Komisją Europejską.

6. zmiany w ustawie **z dnia 19 sierpnia 2011 r. o usługach płatniczych (art. 6)**

**Art. 6** wprowadza zmiany do ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, mające na celu transpozycję przepisów dyrektywy 2022/2556 w zakresie implementacji art. 7 tej dyrektywy wprowadzającego zmiany do dyrektywy 2015/2366Parlamentu Europejskiego i Rady 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniającej dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE (zwanej dalej „dyrektywą PSD II”). Wprowadzane do ustawy zmiany obejmują:

1) w art. 6 ust. 10 otrzymuje nowe brzmienie z uwagi na konieczność dostosowania wyłączenia z zakresu stosowania ustawy do nowego brzmienia art. 3 lit. j zwierającego odniesienie do technologii informacyjno-komunikacyjnych (ICT);

2) dodanie się art. 32ga ma na celu implementację dodawanego w art. 96 dyrektywy PDSII ust. 7. Zgodnie z projektowanym przepisem art. 32ga dot. przekazywania przez dostawców niezwłocznie KNF lub innemu właściwemu organowi nadzoru informacji o poważnym incydencie operacyjnym lub incydencie związanym z bezpieczeństwem, w tym o charakterze teleinformatycznym, nie stosuje się do dostawców usług płatniczych, o których mowa w art. 4 ust. 2 pkt 3-4, 6, 12;

3) w art. 61 ust. 1 pkt 6 otrzymuje nowe brzmienie w celu uwzględnienia zmian wprowadzonych w art. w art. 5 ust. 1 dyrektywa PSD II w zakresie pkt 2 li. A (i). zgodnie z tymi zmianami rozszerza się zakres opisu systemu zarządzania ryzykiem i kontroli wewnętrznej, o którym mowa w art. 64 ust. 1 pkt 3, dołączanego do wniosku o wydanie zezwolenia, o którym mowa w art. 60 ust. 1 tj. zezwolenia na świadczenie usług płatniczych w charakterze krajowej instytucji płatniczej;

4) zmiany wprowadzone w art. 64a:

a) ust. 1 pkt 4 lit. b otrzymuje nowe brzmienie w celu transpozycji zmian wprowadzonych do art. 5 ust. 1 lit. f dyrektywy PSD II. Zgodnie z art. 64a w skład systemu zarządzania ryzykiem i kontroli wewnętrznej, o którym mowa w art. 64 ust. 1 pkt 3, wchodzi opis procedur monitorowania incydentów związanych z bezpieczeństwem oraz monitorowania i rozpatrywania skarg użytkowników, w tym skarg związanych z bezpieczeństwem, a także działań następczych w przypadku wystąpienia takich incydentów i skarg, wraz z mechanizmem zgłaszania incydentów uwzględniającym obowiązki instytucji płatniczej w zakresie zgłaszania, o których mowa w art. 32g i art. 32h. Nowe brzmienie uwzględnia postanowienia rozporządzenia 2022/2554 i wprowadza zmianę, zgodnie z którą w ww. opisie należy uwzględnić mechanizm zgłaszania incydentów uwzględniający obowiązki instytucji płatniczej w, o których mowa w rozdziale III rozporządzenia 2022/2554;

b) ust. 1 pkt 4 lit. e otrzymuje nowe brzmienie w celu transpozycji art. 5 ust. 1 lit h – podobnie jak w przypadku zmian w art. 64a ust. 1 pkt 4 lit. b, zmiany mają na celu uwzględnienie odniesienia do rozporządzenia 2022/2554 i wskazanie, że opis rozwiązań zapewniających ciągłość działania obejmuje wyczerpujące i dokładne określenie krytycznych operacji oraz określenie skutecznych planów awaryjnych i procedury na rzecz ciągłości działania w zakresie ICT oraz planów reagowania i przywracania sprawności ICT, a także procedury na potrzeby regularnego weryfikowania i przeglądu adekwatności i skuteczności takich planów zgodnie z rozporządzeniem 2022/2554;

c) ust. 3a otrzymuje nowe brzmienie w celu zapewnienia transpozycji zmian w art. 5 ust. 1 akapit trzeci dyrektywy PSD II, mających na celu uwzględnienie odpowiednich postanowień rozporządzenia 2022/2554. Zgodnie z nowym brzmieniem ust. 3a środki kontroli bezpieczeństwa i ograniczania ryzyka, o których mowa w ust. 1 pkt 4 lit. g, wskazują sposób zapewnienia wysokiego poziomu operacyjnej odporności cyfrowej, zgodnie z rozdziałem II rozporządzenia 2022/2554, w szczególności w zakresie bezpieczeństwa technicznego i ochrony danych, w tym w odniesieniu do oprogramowania i systemów ICT stosowanych przez wnioskodawcę lub podmiot, któremu wnioskodawca powierzył wykonywanie całości albo części czynności operacyjnych. Środki te obejmują również środki bezpieczeństwa, o których mowa w dziale IIa ustawy zmienianej.

**7. zmiany w ustawie z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego, o Rzeczniku Finansowym i o Funduszu Edukacji Finansowej (art. 7)**

Art. 7. wprowadza zmiany w art. 43g pkt 1ustawy z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego, o Rzeczniku Finansowym i o Funduszu Edukacji Finansowej o charakterze wynikowym, mające na celu uwzględnienie w przychodach Funduszu Edukacji Finansowej i Rada Edukacji Finansowej wpływów z tytułu projektowanego art. 18zf ust. 1 pkt 3 ustawy o nadzorze nad rynkiem finansowym.

8. **zmiany w ustawie z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (art. 8)**

**Art. 8** wprowadza zmiany w ustawie z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, mające na celu transpozycję przepisów dyrektywy 2022/2556 w zakresie implementacji art. 2, który wprowadza zmiany dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (zwanej dalej „dyrektywą 2009/138/WE”. Wprowadzane do ustawy zmiany obejmują zmianę w art. 47 dodanie ust. 2 i 3 w celu transpozycji zmian wprowadzonych w art. 41 ust. 4 dyrektywy 2009/138/WE. Zgodnie projektowanym przepisem art. 47 ust. 2 ustawy z dnia 11 września 2015 r o działalności ubezpieczeniowej i reasekuracyjnej zakład ubezpieczeń i zakład reasekuracji stosują odpowiednie i współmierne systemy, zasoby i procedury, w szczególności ustanawiają sieci i systemy informatyczne oraz zarządzają nimi zgodnie z rozporządzeniem 2022/2554. Projektowany art. 47 ust. 3 ustawy z dnia 11 września 2015 r o działalności ubezpieczeniowej i reasekuracyjnej wskazuje, że przepisu ust. 2 nie stosuje się do zakładów ubezpieczeń i zakładów reasekuracji, które spełniają warunki, o których mowa w art. 101 ust.  1 pkt 1 - 6 i ust. 2. Przepis art. 101 ust. 4 stosuje się odpowiednio. Odpowiednie stosowanie art. 101 ust. 4 polegałoby na tym, że jeżeli którakolwiek z kwot, o których mowa w art. 101 ust. 1 pkt 1 - 6, zostanie przekroczona w 3 kolejnych latach obrotowych, zakład ubezpieczeń powinien dostosować swoją działalność do wymogów określonych w art. 47 ust. 2 ustawy, począwszy od 4. kolejnego roku obrotowego.

**9. zmiany w ustawie z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji (art. 9)**

Art. 9 wprowadza zmiany do ustawy z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji. Zmiany wprowadzone w art. 81 ust. 1 pkt 3 i pkt 16 ustawy mają na celu implementację art. 5 pkt 1 pkt a i b dyrektywy 2022/2556, przewidującym zmianę art. 10 ust. 7 lit. c i q dyrektywy Parlamentu Europejskiego i Rady 2014/59/UE z dnia 15 maja 2014 r. ustanawiającej ramy na potrzeby prowadzenia działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji w odniesieniu do instytucji kredytowych i firm inwestycyjnych oraz zmieniającej dyrektywę Rady 82/891/EWG i dyrektywy Parlamentu Europejskiego i Rady 2001/24/WE, 2002/47/WE, 2004/25/WE, 2005/56/WE, 2007/36/WE, 2011/35/UE, 2012/30/UE i 2013/36/EU oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 i (UE) nr 648/2012 (zwanej dalej „dyrektywą 2014/59/UE”) i precyzują kwestie, które powinny zostać uwzględniane w kontekście planowania i oceny wykonalności działań w przypadku wszczęcia przymusowej restrukturyzacji, w celu ich dostosowania do unijnych ram operacyjnej odporności cyfrowej.

Ponadto, w art. 87 ustawy z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji zdecydowano się na modyfikację dotychczasowego upoważnienia ustawowego do wydania rozporządzenia poprzez:

-  wykreślenie „oceny wykonalności” i wprowadzenie pojęcia „przeglądu”. „Ocena wykonalności” mieści się w pojęciu „przeglądu”, który odzwierciedla czynność faktyczną podejmowaną przez Bankowy Fundusz Gwarancyjny. W ramach przeglądu (i ewentualnej aktualizacji) jest dokonywana przez Fundusz ocena wykonalności, natomiast sama aktualizacja jest skutkiem oceny planu przez BFG podczas dokonywania przeglądu.

- uwzględnienie określenia minimalnego zakresu analiz przeprowadzanych przez Fundusz, w celu zapewnienia implementacji sekcji C do załącznika do dyrektywy 2014/59/UE, zmienionego dyrektywą 2022/2556.

Dodatkowo w art. 2 ustawy z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji, wprowadza się uzupełnienie zakresu definicji stosowanych w ustawie w taki sposób, że przepisie tym dodaje się pkt 55d, w którym określa się skrót na oznaczenie rozporządzenia 2022/2554.

10. zmiany w ustawie **z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (art. 10)**

**Art. 10** wprowadza zmiany w ustawie o krajowym systemie cyberbezpieczeństwa mające na celu zapewnienie spójności rozwiązań w zakresie cyberbezpieczeństwa.

Art. 10 pkt 1 wprowadza zmiany w art. 2 ustawy o krajowym systemie cyberbezpieczeństwa, który zawiera słownik pojęć stosowanych w ustawie. Proponuje się przez dodanie pkt 11a-11c, pkt 16a oraz pkt 20 uzupełnienie słownika o pojęcia mające znaczenie dla stosowania przepisów rozporządzenia 2022/2554, implementowanych w drodze zmiany ustawy o krajowym systemie cyberbezpieczeństwa. W pkt 11 a wprowadzona zostaje definicja podmiotu finansowego odsyłająca do art. 18za ust. 1 ustawy o nadzorze nad rynkiem finansowym, który wymienia podmioty finansowe, o których mowa w art. 2 ust. 1 rozporządzenia 2022/2554  rozumieniu prawa krajowego; w pkt 11 b - poważnego incydentu związanego z ICT; pkt 11c - skrót na oznaczenie rozporządzenia 2022/2554. Dodawany pkt 16a wprowadza definicję właściwego organu w rozumieniu rozporządzenia 2022/2554, która wskazuje, że tym organem jest KNF; pkt 20 definiuje znaczące cyberzagrożenie.

Art. 10 pkt 2 i 3 wprowadza zmiany, które określą sposób informowania przez podmioty finansowe organów funkcjonujących w krajowym systemie cyberbezpieczeństwa o poważnych incydentach oraz znaczących zagrożeniach związanych z ICT, a także procedury komunikacji między tymi organami:

**● zgłaszanie poważnych incydentów związanych z ICT**

Rozwiązania w tym zakresie (projektowany art. 11a ustawy o krajowym systemie cyberbezpieczeństwa) wskazują na obowiązek podmiotów finansowych zgłaszania poważnych incydentów związanych z ICT, zgodnie z art. 19 ust. 1 rozporządzeniu 2022/2554, a także przekazywania wstępnych powiadomień i sprawozdań, o których mowa w art. 19 ust. 4 rozporządzenia 2022/2554 właściwemu organowi w rozumieniu przepisów rozporządzenia 2022/2554 tj. KNF. Przekazane właściwemu organowi w rozumieniu rozporządzenia 2022/2554 zgłoszenia, wstępne powiadomienia i sprawozdania uznaje się za przekazane również sektorowemu zespołowi cyberbezpieczeństwa, ustanowionemu w urzędzie zapewniającym obsługę tego właściwego organu.

Sektorowy zespół cyberbezpieczeństwa niezwłocznie przekazuje wstępne powiadomienie   
i sprawozdania, pochodzące od podmiotu finansowego będącego podmiotem kluczowym, o którym mowa w art. 3 ust. 1 dyrektywy 2022/2555, lub podmiotem ważnym, o którym mowa w art. 3 ust. 2 dyrektywy 2022/2555 właściwemu CSIRT MON, CSIRT NASK albo CSIRT GOV. Projektowane rozwiązania zapewniają też możliwość przekazania przez zespół sektorowy właściwemu CSIRT MON, CSIRT NASK albo CSIRT GOV ww. powiadomień i sprawozdań pochodzących od innych niż kluczowe lub ważne podmioty finansowe.

Zgodnie z projektowanym art. 11a ustawy o krajowym systemie cyberbezpieczeństwa zgłoszenie poważnego incydentu związanego z ICT oraz wstępne powiadomienia i sprawozdania, są przekazywane w terminach i z wykorzystaniem wzorów, określonych we wspólnych regulacyjnych standardach technicznych i wspólnych wykonawczych standardach technicznych, o których mowa w art. 20 rozporządzenia 2022/2554, w postaci elektronicznej,   
a w przypadku braku możliwości przekazania ich w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji, co zapewnia wdrożenie art. 20 rozporządzenia 2022/2554.

**● zgłaszanie znaczących zagrożeń związanych z ICT**

Projektowany art. 13a ustawy o krajowym systemie cyberbezpieczeństwa stanowi wdrożenie art. 19 ust. 2 akapit pierwszy rozporządzenia 2022/2554, zgodnie z którym podmiot finansowy może przekazać właściwemu organowi w rozumieniu rozporządzenia 2022/2554 powiadomienie o znaczącym cyberzagrożeniu. Powiadomienie o znaczącym cyberzagrożeniu przekazane właściwemu organowi w rozumieniu rozporządzenia 2022/2554 uznaje się za przekazane również sektorowemu zespołowi cyberbezpieczeństwa ustanowionemu w urzędzie zapewniającym obsługę tego właściwego organu.

Sektorowy zespół cyberbezpieczeństwa niezwłocznie przekazuje powiadomienie o znaczącym cyberzagrożeniu, pochodzące od podmiotu finansowego będącego podmiotem kluczowym, o którym mowa w art. 3 ust. 1 dyrektywy 2022/2555, lub podmiotem ważnym, o którym mowa w art. 3 ust. 2 dyrektywy 2022/2555, właściwemu CSIRT MON, CSIRT NASK albo CSIRT GOV. Przekazanie powiadomienia o znaczącym zagrożeniu pochodzącego od podmiotu niebędącego podmiotem kluczowym lub podmiotem ważnym jest fakultatywne.

Powiadomienie, o którym mowa w art. 19 ust. 2 rozporządzenia 2022/2554, jest przekazywane w terminach i z wykorzystaniem wzorów, określonych we wspólnych regulacyjnych standardach technicznych i wspólnych wykonawczych standardach technicznych, o których mowa w art. 20 rozporządzenia 2022/2554, w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji.

Projektowane rozwiązania wdrażające kluczowe dla zapewnienia cyberbezpieczeństwa regulacje, dotyczące zgłaszania organom właściwym informacji o poważnych incydentach lub znaczących cybrezagrożeniach mają na celu:

- lepszą koordynację przepływu informacji między podmiotami finansowymi, organem właściwym a CSIRT poziomu krajowego (a także organem właściwym w rozumieniu dyrektywy 2022/2555 i sektorowym zespołem cyberbezpieczeństwa, gdyż te role również realizowane są w KNF/UKNF),

- zapewnienie spójności przyjętego rozwiązania z założeniami wdrożenia dyrektywy 2022/2555, zgodnie z którymi to CSIRT sektorowe mają być pierwszymi odbiorcami zgłoszeń incydentów i przekazywać je do CSIRT poziomu krajowego,

- uniknięcie obciążenia dla podmiotów finansowych wynikającego z podwójnego raportowania.

Przekazywanie powiadomień w postaci elektronicznej przyspiesza obieg informacji, pozwala na automatyzacje procesu dalszego przetwarzania danych, cała komunikacja w zakresie obowiązków wynikających rozporządzenia 2022/2554 będzie realizowana w postaci elektronicznej.

Art. 10 pkt 4 wprowadza zmianę polegająca na dodaniu art. 16a ustawy o krajowym systemie cyberbezpieczeństwa, zgodnie z którym przepisów art. 8, art. 10–13 i art. 15 tej ustawy nie stosuje się do podmiotów kluczowych, o których mowa w art. 3 ust. 1 dyrektywy 2022/2555, lub podmiotów ważnych, o których mowa w art. 3 ust. 2 dyrektywy 2022/2555, z sektora „Bankowość i infrastruktura rynków finansowych”, o którym mowa w załączniku nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa.

Zgodnie z załącznikiem 1 do zmienianej ustawy, podmiotami kluczowymi lub ważnymi z sektora „Bankowość i infrastruktura rynków finansowych” są:

- instytucja kredytowa, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe,

- bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe,

- oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe,

- oddział instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe,

- spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych,

- podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

- podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

- podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.

Podmioty te zostały wyłączone z obowiązku stosowania przepisów art. 8, 10, 11, 12, 13 i 15 ustawy o krajowym systemie cyberbezpieczeństwa w celu uniknięcia dublowania obowiązków nakładanych na te podmioty. Art. 8 ustawy o krajowym systemie cyberbezpieczeństwa nakłada na operatora usługi kluczowej obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zgodnego z wymogami tego przepisu. Art. 10 ustawy o krajowym systemie cyberbezpieczeństwa dotyczy obowiązków operatora usługi kluczowej w zakresie dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Art. 11 ustawy o krajowym systemie cyberbezpieczeństwa stanowi regulację dotycząca obowiązków związanych ze zgłaszaniem i obsługą incydentów. Art. 12 ustawy o krajowym systemie cyberbezpieczeństwa określa zakres informacji objętych zgłoszeniem poważnego incydentu i uprawnienia właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz sektorowy zespół cyberbezpieczeństwa związane z tym zgłoszeniem. Art. 13 ustawy o krajowym systemie cyberbezpieczeństwa stanowi regulację dotyczącą innych informacji, które mogą być przekazywane przez operatora usługi kluczowej. Art. 15 ustawy o krajowym systemie cyberbezpieczeństwa reguluje obowiązki operatora usługi kluczowej związane z audytem bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

W związku z ww. zmianami pozostają zmiany określone w art. 10 pkt 7 wprowadzające w dodawanym art.76a ustawy o krajowym systemie cyberbezpieczeństwa wyłączenie z obowiązku stosowania przepisów rozdziału 14 „Przepisy o karach pieniężnych” w przypadku podmiotów kluczowych lub podmiotów ważnych z sektora „Bankowość i infrastruktura rynków finansowych”, o którym mowa w załączniku nr 1 do ustawy. Niniejszy projekt ustawy wprowadza system kar pieniężnych za naruszenie obowiązków stanowionych rozporządzeniem 2022/2554 do ustawy o nadzorze nad rynkiem finansowym.

Zmiany wprowadzane art. 10 pkt 5 w zakresie art. 65 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa mają na celu zapewnienie współdziałania zespołów CSIRT MON, CSIRT GOV i CSIRT NASK oraz właściwych organów w rozumieniu rozporządzenia 2022/2554 w zakresie działalności podmiotów finansowych będących podmiotami kluczowymi lub podmiotami ważnymi, poprzez rozszerzenie katalogu zadań Kolegium działającego przy Radzie Ministrów jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa.

Ponadto, zgodnie z art. 10 pkt 6 wprowadzającym zmianę w art. 66 ust. 1 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa, Przewodniczący KNF będzie mógł uczestniczyć w posiedzeniach ww. Kolegium. Projektowane w tym zakresie rozwiązania mają na celu zapewnienie lepszej koordynacji i współdziałania organów właściwych w systemie cyberbezpieczeństwa.

**III. Przepisy przejściowe, dostosowujące i końcowe**

Art. 11 projektu ustawy stanowi przepis przejściowy dotyczący postępowań wszczętych na podstawie rozdziału 14 ustawy zmienianej w art. 10 i niezakończonych przed dniem wejścia w życie niniejszej ustawy, do których stosuje się przepisy dotychczasowe.

Art. 12 projektu ustawy stanowi regulację przejściową dotyczącą czasowego utrzymania w mocy przepisów wykonawczych wydanych na podstawie art. 87 ustawy z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji, do czasu wydania nowych przepisów wykonawczych na podstawie zmienianego w art. 9 pkt 3 projektu ustawy upoważnienia ustawowego art. 87, nie dłużej niż 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 13 stanowi przepis dostosowujący, wskazujący, że informacje, o których mowa w art. 18zc ustawy zmienianej w art. 9 podmioty finansowe, o których mowa w art. 18za ust. 1 tej ustawy, po raz pierwszy przekazują za rok 2025.

Brak jest konieczności wprowadzania dalszych przepisów przejściowych, szczególnie w zakresie kontroli podmiotów finansowych, prowadzonych na podstawie ustawy o nadzorze nad rynkiem finansowym. Mimo pewnych powiązań przedmiotowych i podmiotowych, obecnie realizowane przez KNF kontrole, nie są kontrolami w rozumieniu rozporządzenia 2022/2554.

Zgodnie z art. 14 ustawa wchodzi w życie z dniem 17 stycznia 2025 r., tj. zgodnie z terminem, od którego stosuje się przepisy rozporządzenia 2022/2554, wyznaczonym w art. 64 tego rozporządzenia.

IV. Informacje dodatkowe

Projekt ustawy jest zgodny z prawem UE.

Projektowane zmiany nie powinny mieć znaczącego wpływu na działalność MŚP, w szczególności na mikro i małych przedsiębiorców. Zgodnie z zasadą proporcjonalności wyrażoną w art. 4 rozporządzenia 2022/2554 podmioty finansowe stosują przepisy tego rozporządzenia, biorąc pod uwagę swoją wielkość i ogólny profil ryzyka oraz charakter, skalę i stopień złożoności swoich usług, działań i operacji. Z uwagi na powyższe, skutki projektowanej regulacji będą dotyczyć głównie dużych podmiotów finansowych.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i nie podlega notyfikacji Komisji Europejskiej.

Projekt ustawy nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia, o którym mowa w § 27 ust. 4 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M. P. z 2022 r. poz. 348).

Stosownie do art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt ustawy podlega udostępnieniu w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji.