Minister
Finansów

Warszawa, 17 lipca 2025 roku

Sprawa: projekt DORA: odpowiedź na interpelację nr 10564
Znak sprawy: FN5.050.1.2025
Kontakt: Kancelaria MF
tel.: +48 22 694 55 55
e-mail: kancelaria@mf.gov.pl

Pan Szymon Hołownia
Marszałek Sejmu Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w odpowiedzi na interpelację nr 10564 Pana Posła Jarosława Sachajko i Pani Poseł Anny Gembickiej dotyczącą *projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji* zawartego w druku nr 1326, który wdraża przepisy unijnego rozporządzenia 2022/2554[1] (dalej zwanego rozporządzeniem DORA) i dyrektywy 2022/2556[2] oraz rozporządzenia 2023/2631[3] (dalej zwanego rozporządzeniem EuGB), uprzejmie przesyłam odpowiedź na postawione pytania.

Ad 1.

Jednym z priorytetów Rządu podczas prac nad *projektem ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji* była zgodność projektu z przepisami ww. aktów prawa UE, w szczególności unikanie wprowadzania nadregulacji i obowiązków, które nie wynikają z prawa UE.

Jednocześnie pragnę wyjaśnić, że zgodnie z rozporządzeniem DORA, na mocy decyzji poszczególnych państw członkowskich, możliwe jest wyłączenie z zakresu stosowania rozporządzenia DORA podmiotów wskazanych w art. 2 ust. 4, tj.

[1] rozporządzenie 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 (Dz. Urz. UE L 333 z 27.12.2022, str. 1 oraz Dz. Urz. UE L 2024/90177 z 12.03.2024);

[2] dyrektywa Parlamentu Europejskiego i Rady (UE) 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 (Dz. Urz. UE L 333 z 27.12.2022, str. 153);

[3] rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2631 z dnia 22 listopada 2023 r. w sprawie europejskich zielonych obligacji oraz opcjonalnego ujawniania informacji na temat obligacji wprowadzanych do obrotu jako zrównoważone środowiskowo i obligacji powiązanych ze zrównoważonym rozwojem (Dz. Urz. UE L 2023/2631 z 30.11.2023 oraz Dz. Urz. UE L 2023/2869 z 20.12.2023);

tel.: +48 22 694 55 55
fax: +48 22 694 36 84
gov.pl/finanse
e-mail: kancelaria@mf.gov.pl

ul. Świętokrzyska 12
00-916 Warszawa

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 oraz banki państwowe, tj. BGK. Z uwagi na zakres działalności ww. podmiotów wskazana jest rezygnacja z zastosowania opcji narodowej, o której mowa w art. 2 ust. 4 rozporządzenia DORA. W przypadku braku decyzji o wyłączeniu, ww. podmioty, w zakresie zarządzania ryzykiem związanym z ICT, stosują przepisy art. 16 rozporządzenia DORA, stanowiące uproszczone ramy zarządzania ryzykiem związanym z ICT. Ograniczony katalog obowiązków, określony art. 16, w warunkach polskich, jest jednak nieadekwatny wobec BGK i SKOK-ów spełniających kryteria dla podmiotów kluczowych lub ważnych w rozumieniu dyrektywy NIS2[4]. Z uwagi na powyższe, projektodawca zdecydował się uwzględnić uwagę UKNF i w przypadku największych SKOK-ów wskazać na konieczność stosowania art. 5–15 rozporządzenia DORA. Regulacja ta nie będzie dotyczyła mniejszych podmiotów (niespełniających kryteriów podmiotów kluczowych lub ważnych w rozumieniu dyrektywy NIS2), które stosować będą art. 16 określający uproszczone ramy zarządzania ryzkiem.

Wskazane rozwiązanie zostało wprowadzone ze względu na konieczność ograniczenia ryzyka dla systemu finansowego związanego z cyberzagrożeniami, ujednolicenia obowiązków dla dużych podmiotów finansowych, a także zapewnienia równoważności wymogów w zakresie zarządzania ryzkiem związanym z ICT z wymogami dyrektywy NIS2 (zgodnie z art. 4 dyrektywy NIS2).

Ad 2.

W odniesieniu do uprawnień w zakresie nadzoru nad spełnianiem wymagań rozporządzenia DORA, należy podkreślić, że kompetencje nadane Komisji Nadzoru Finansowego (dalej zwane KNF) nie wykraczają poza zakres uprawnień określony rozporządzeniem DORA, w szczególności art. 50 – 56 tego rozporządzenia. Z uwagi na ogólny charakter katalogu kompetencji, o którym mowa w art. 50 rozporządzenia DORA, katalog kompetencji wymagał doprecyzowania, jednak KNF nie zostały nadane uprawnienia, które nie byłyby przewidziane rozporządzeniem DORA. W szczególności w odniesieniu do osób trzecich np. zewnętrznych dostawców usług ICT, art. 50 ust. 2 lit. b (ii) dopuszcza przesłuchanie wszelkich innych osób fizycznych i prawnych (osób trzecich), które wyrażają na to zgodę, w celu zebrania informacji dotyczących przedmiotu dochodzenia. Projektowany art. 18zc ust. 4 pkt 3 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, który dokonuje wdrożenia przedmiotowej kompetencji, również warunkuje pozyskanie informacji od osób trzecich ich zgodą.

W kwestii przechowywania danych, projektowana regulacja również nie wykracza poza dyspozycję art. 56 dotyczącego ochrony danych, który stanowi, że dane osobowe są zatrzymywane do czasu wywiązania się z mających zastosowanie obowiązków nadzorczych i w każdym przypadku przez maksymalnie 15 lat, z wyjątkiem sytuacji, gdy toczy się postępowanie sądowe wymagające dalszego zatrzymania takich danych. Projektowany art. 4a ust. 3a ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, który dokonuje wdrożenia art. 56

[4] dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).

wskazuje, że dane osobowe, o których mowa w art. 56 ust. 1 rozporządzenia 2022/2554, Komisja przetwarza przez okres 15 lat w celu sprawowania nadzoru w zakresie, o którym mowa w art. 1 ust. 2 pkt 16 (nadzoru nad spełnianiem wymagań wprowadzonych rozporządzeniem DORA), chyba że toczy się postępowanie sądowe wymagające dalszego przetwarzania tych danych.

Ad 3.

W zakresie sytuacji mikroprzedsiębiorców oraz małych i średnich przedsiębiorców należy wskazać, że przepisy rozporządzenia DORA uwzględniają zakres i skalę działalności podmiotów finansowych, wskazując w art. 4, że stosowanie tego rozporządzenia powinno uwzględniać zasadę proporcjonalności, stanowioną tym przepisem. Poszczególne przepisy rozporządzenia DORA również różnicują obowiązki podmiotów finansowych, zgodnie z zasadą wyrażoną w art. 4.

W przypadku małych podmiotów finansowych, w szczególności podmiotów spełniających kryteria definicji mikroprzedsiębiorstwa, określone w art. 3 pkt 60 rozporządzenia DORA, tj. podmiotów finansowych innych niż systemy obrotu, kontrahenci centralni, repozytoria transakcji lub centralne depozyty papierów wartościowych, zatrudniających mniej niż 10 osób i których roczny obrót lub bilans roczny nie przekracza 2 mln EUR, część obowiązków przewidzianych rozporządzeniem DORA nie znajdzie zastosowania. Zgodnie z zasadą proporcjonalności wyrażoną w art. 4 rozporządzenia DORA, szereg przepisów tego rozporządzania wyłącza w stosunku do mikroprzedsiębiorców określone obowiązki. Przykładowo dotyczy to obowiązków stanowionych następującymi przepisami rozporządzenia DORA:

- art. 5 ust. 3 wskazuje, że mikroprzedsiębiorstwa nie są zobowiązane do ustanowienia funkcji w celu monitorowania ustaleń zawartych z zewnętrznym dostawcą usług ICT w sprawie korzystania z usług ICT lub wyznaczenia członka kadry kierowniczej wyższego szczebla jako odpowiedzialnego za nadzorowanie związanej z tym ekspozycji na ryzyko i odpowiedniej dokumentacji;

- art. 24 ust. 1 wskazuje na wyłączenie mikroprzedsiębiorców z obowiązku ustanowienia i utrzymywania prawidłowego i kompleksowego programu testowania operacyjnej odporności cyfrowej;

- art. 24 ust. 4 stanowi, że mikroprzedsiębiorcy nie mają obowiązku zapewnienia przeprowadzania testów w zakresie operacyjnej odporności przez niezależne strony wewnętrzne i zewnętrzne.

- art. 24 ust. 6 wyłącza mikroprzedsiębiorców z obowiązku przeprowadzania odpowiednich testów wszystkich systemów i aplikacji ICT przynajmniej raz w roku;

- art. 28 ust. 2 wyłącza podmioty, o których mowa w art. 16 oraz mikroprzedsiębiorców z obowiązku przyjęcia strategii dotyczącej ryzyka ze strony zewnętrznych dostawców usług ICT i regularnego jej przeglądu.

Ww. przepisy wskazują na liczne ograniczenia obowiązków w przypadku, gdy podmiot finansowy spełnia kryteria definicji mikroprzedsiębiorstwa, co powinno zostać uwzględnione w praktyce nadzoru nad stosowaniem rozporządzenia DORA przez te podmioty.

W myśl *projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji*, mającym na celu wdrożenie rozporządzenia DORA do polskiego systemu prawnego, organem nadzoru w zakresie stosowania rozporządzenia DORA będzie KNF. Zgodnie z informacjami przekazanymi przez KNF, KNF będzie

realizować kompetencje właściwego organu w obszarze kontroli zgodnie z obowiązującymi przepisami prawa, zaś stosowanie przez podmioty finansowe zasady proporcjonalności, o której mowa w art. 4 rozporządzenia DORA, będzie przez KNF analizowane w ramach sprawowanego nadzoru, w tym w ramach prowadzonych kontroli.

Ad 4.

Rozporządzenie DORA jest aktem prawnym UE obowiązującym bezpośrednio więc już w tej chwili powinno być stosowane przez podmioty finansowe. Rozporządzenie DORA zostało opublikowane w dniu 27 grudnia 2022 r. i powinno być stosowane przez podmioty finansowe od dnia 17 stycznia 2025 r. Wydaje się zatem, że podmioty finansowe miały wystarczającą ilość czasu na wdrożenie rozwiązań przewidzianych niniejszym rozporządzeniem. *Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji* ma na celu zapewnienie stosowania rozporządzenia w wymiarze funkcji nadzoru państwa, tj. przede wszystkim dokonuje wyznaczenia organu nadzoru i nadaje mu przewidziane rozporządzeniem DORA kompetencje. Zakres obowiązków nakładanych na podmioty finansowe wynika z bezpośrednio obowiązujących przepisów rozporządzenia.

Projektodawca uwzględnia jednak konieczność dostosowania się BGK i SKOK-ów spełniających kryteria dla podmiotów kluczowych lub ważnych w rozumieniu dyrektywy NIS2 i przewiduje na to odpowiednie vacatio legis. Zgodnie z projektowanym art. 17 *projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji* przepis art. 3c pkt 1 ustawy zmienianej w art. 4a oraz przepis art. 2a ust. 2 ustawy zmienianej w art. 9, mają zastosowanie po upływie roku od dnia wejścia w życie niniejszej ustawy.

Dodatkowo, należy wskazać, że obowiązki wynikające z rozporządzenia DORA uwzględniają wielkość i zakres działalności podmiotów finansowych, kierując się zasadą proporcjonalności. Warto podkreślić, że obowiązki z zakresu cyberbezpieczeństwa chronią nie tylko konsumentów korzystających z usług podmiotów finansowych, ale także samych przedsiębiorców. W przypadku braku odpowiedniej ochrony sieci systemów i sieci informatycznych, utrata danych w wyniku ataku z zewnątrz albo przerwa w prowadzeniu działalności, skutkuje niejednokrotnie bardzo dużymi kosztami po stronie przedsiębiorców, zarówno w wymiarze pieniężnym, jak i wizerunkowym. Z uwagi na powyższe spełnienie obowiązków w tym zakresie powinno być traktowane jak inwestycja w bezpieczeństwo, a nie koszt po stronie przedsiębiorcy.

Wg „Raportu rocznego CSRIT KNF" za rok 2024 r., rok 2024 pokazał bezprecedensowy wzrost ataków phishingowych. Jednymi z najczęściej występujących oszustw były fałszywe inwestycje. Dodatkowo w roku 2024 w sektorze finansowym zaobserwowano wiele kampanii złośliwego oprogramowania należącego do różnorodnych rodzin malware. Zwiększyło się również wykorzystywanie oprogramowania typu stealer. Po analizie ww. Raportu CSIRT KNF można wskazać, że zwiększyła się liczba ataków każdego rodzaju, a przestępcy wykorzystują coraz bardziej wyrafinowane metody utrudniające identyfikację zagrożenia. W świetle powyższego, zapewnienie cyberbezpieczeństwa świadczenia usług finansowych wydaje się kluczowe.

Ad 5.

Zgodnie z r*ozporządzeniem Parlamentu Europejskiego i Rady (UE) 2023/2631 z dnia 22 listopada 2023 r. w sprawie europejskich zielonych obligacji oraz opcjonalnego ujawniania informacji na temat obligacji wprowadzanych do obrotu jako zrównoważone środowiskowo i obligacji powiązanych ze zrównoważonym rozwojem* (dalej rozporządzanie EuGB), aby obligacja mogła zostać oznaczona jako *europejska zielona obligacja/EuGB*, emisja musi spełniać szereg formalnych i merytorycznych warunków. Pierwszym z nich jest tzw. zgodność z unijną taksonomią zrównoważonego rozwoju. Zapisy rozporządzenia EuGB wskazują, że przychody z obligacji, w przypadku których stosowane jest oznakowanie *europejskiej zielonej obligacji/EuGB*, należy alokować wyłącznie na projekty uznane za zrównoważone środowiskowo – co najmniej 85% wpływów z emisji powinno zostać przeznaczone na cele i działalność gospodarczą zgodną z unijną taksonomią. Pozostałe – maksymalnie 15% – może być skierowane na działania, które spełniają zasadę „nieczynienia poważnych szkód" – nawet jeśli nie są jeszcze w pełni objęte taksonomią.

Kolejnym istotnym warunkiem standardu *europejskiej zielonej obligacji/EuGB* jest obowiązek przygotowania przez emitenta szczegółowego dokumentu przedemisyjnego, tzw. arkusza informacyjnego europejskiej zielonej obligacji. Dokument ten stanowi podstawowe źródło informacji dla potencjalnych inwestorów i zewnętrznych kontrolerów. W arkuszu tym emitent określa m.in. cel emisji i sposób wykorzystania wpływów, zgodność z unijną taksonomią, a także opis procedur monitorowania i raportowania emisji.

Niezwykle istotnym mechanizmem przeciwdziałania greenwashingowi jaki został przewidziany rozporządzeniem EuGB jest również instytucja kontrolera zewnętrznego, który przeprowadza niezależną weryfikację dokumentacji emisyjnej. W ramach weryfikacji, zewnętrzny kontroler dokonuje oceny arkusza informacyjnego europejskiej zielonej obligacji przygotowanego przez emitenta. Kolejno, na podstawie tej analizy, wydaje opinię, w której stwierdza, czy planowana emisja jest zgodna ze standardem *europejskiej zielonej obligacji/EuGB*. Poza powyższym, kontroler może realizować czynności sprawdzające po emisji, w ich zakresie możliwa jest m.in. weryfikacja raportu alokacyjnego, tj. ocena, czy wpływy pozyskane z emisji zostały rozdysponowane zgodnie z deklaracjami, a także opcjonalnie – ocena raportu wpływu środowiskowego, jeśli emitent zdecyduje się na taką usługę.

Zgodnie z rozporządzeniem EuGB, zewnętrzni kontrolerzy muszą spełniać szereg wymogów, których celem jest zapewnienie wiarygodności i niezależności procesu weryfikacji. Przede wszystkim są oni zobowiązani do obowiązkowej rejestracji w wykazie prowadzonym przez Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA). Urząd ten pełni również funkcję organu nadzoru, monitorując na bieżąco jakość, rzetelność i niezależność ich pracy. Ponadto, kontroler zewnętrzny jest zobowiązany do zachowania pełnej niezależności i bezstronności –nie może być powiązany kapitałowo ani organizacyjnie z emitentem, a także musi wykazać, że wdrożył skuteczne mechanizmy zapobiegające konfliktowi interesów. Ważnym aspektem jest również zachowanie transparentności stosowanej metodologii – kontroler zewnętrzny ma obowiązek publicznego ujawnienia przyjętej metody oceny oraz przedstawienia uzasadnienia swoich wniosków. Wreszcie, od kontrolera zewnętrznego oczekuje się odpowiedniego poziomu doświadczenia i kompetencji – musi on posiadać zarówno ekspertyzę techniczną i środowiskową, jak i odpowiednie zaplecze organizacyjne, niezbędne do przeprowadzenia profesjonalnej i rzetelnej analizy.

W związku z przekazanymi pytaniami z zakresu europejskich zielonych obligacji wyjaśnienia również wymaga, że rozporządzenie EuGB nie przewiduje dla rządów państw członkowskich szczególnej roli kontrolnej w zakresie weryfikacji faktycznego wpływu środowiskowego projektów finansowanych tymi obligacjami. Rozporządzenie to zobowiązało jedynie państwa członkowskie do wskazania organu nadzoru nad spełnianiem przez emitentów europejskich zielonych obligacji obowiązków wynikających z rozporządzenia w sprawie europejskich zielonych obligacji, którym w przypadku Polski jest Komisja Nadzoru Finansowego, oraz nadania temu organowi odpowiednich kompetencji kontrolnych i nadzorczych, w tym prawo do nakładania sankcji administracyjnych za nieprzestrzeganie przepisów rozporządzenia. Realizacja tych zobowiązań została przewidziana w projekcie ustawy zawartej w druku nr 1326.

Ad 6.

Art. 50 ust. 2 rozporządzenia DORA wskazuje, że właściwy organ jest uprawniony do dostępu do wszelkich dokumentów lub danych przechowywanych w jakiejkolwiek formie, które właściwy organ uważa za istotne z punktu widzenia wykonywania swoich obowiązków oraz otrzymywania lub sporządzania ich kopii. Projektowany art. 18zc ust. 4 pkt 6 ustawy 21 lipca 2006 r. o nadzorze nad rynkiem finansowym jest zatem zgodny z art. 50 ust. 2 rozporządzenia DORA.

Warto zaznaczyć, że w zakresie kompetencji KNF dotyczących kontroli/weryfikacji systemów informatycznych podmiotów finansowych, nie wydaje się możliwe ustalenie czy systemy informatyczne są zabezpieczone i spełniają wymagania określone rozporządzeniem DORA lub aktami delegowanymi wydanymi na jego podstawie, bez zabezpieczenia wglądu do systemów informatycznych. Brak kompetencji w tym zakresie stanowiłby jedynie kontrolę o charakterze iluzorycznym. Rozporządzenie DORA wprowadza szereg obowiązków dotyczących odpowiedniego zabezpieczenia sieci i systemów informatycznych. Np. art. 7 wprowadza wymagania, które muszą spełniać systemy, protokoły i narzędzia ICT. Art. 9 reguluje m.in. wymagania dotyczące funkcjonowania systemów i narzędzi ICT w zakresie ochrony i zapobiegania naruszeniom bezpieczeństwa danych np. wskazując w ust. 4 lit. d obowiązek wdrożenia polityk i protokołów dotyczących silnych mechanizmów uwierzytelniania, opartych na odpowiednich standardach i specjalnych systemach kontroli oraz środkach ochrony kluczy kryptograficznych, dzięki którym dane szyfruje się na podstawie wyników zatwierdzonych procesów klasyfikacji danych i oceny ryzyka związanego z ICT.

Z uwagi na powyższe, projektowane przepisy umożliwiają ocenę czy systemy informatyczne są zgodne z dokumentacją przedstawioną przez podmioty finansowe. Bez zabezpieczenia takiego uprawnienia organ nadzoru nie ma możliwości weryfikacji czy system informatyczny rzeczywiście spełnia wymagania określone rozporządzeniem DORA.

W tym zakresie, analogiczna jest opinia KNF, zgodnie z którą wskazana kompetencja pozostaje niezbędna do wykonywania obowiązków organu nadzoru wynikających z rozporządzenia DORA. Obszar operacyjnej odporności cyfrowej oparty jest na technologiach informacyjno-komunikacyjnych, a dane, które mogą stanowić podstawę oceny przez organ nadzoru realizacji obowiązków podmiotów finansowych w omawianym obszarze, będą w dużej mierze przetwarzane w systemach informatycznych w postaci cyfrowej.

W ramach rozporządzenia DORA, KNF będzie odpowiedzialna za zapewnienie przestrzegania wielu obowiązków, dla których kontroli kluczowe będą dane zawarte w systemach informatycznych, w tym dokumenty wewnętrzne

potwierdzające spełnianie obowiązków w zakresie zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi. Przykładem w tym zakresie mogą być obowiązki dotyczące zarządzania incydentami związanymi z ICT, ich klasyfikacją i zgłaszaniem. Dane zawarte w systemach informatycznych (jak np. logi systemowe) będą niezbędne dla ustalenia, czy podmiot finansowy prawidłowo zarządza incydentami związanymi z ICT, jak choćby weryfikacji, czy podmiot finansowy w sposób skuteczny wprowadził wskaźniki wczesnego ostrzegania i reaguje na nie w sposób sprawny i pozwalający ograniczyć ryzyko wystąpienia incydentów związanych z ICT, bądź czy podmiot finansowy terminowo zgłasza właściwemu organowi poważne incydenty związane z ICT.

Ad 7.

W przypadku kontroli i decyzji administracyjnych nakładających kary pieniężne lub zobowiązujących do określonego zachowania albo zaprzestania określonego zachowania obowiązują wszelkie zabezpieczenia proceduralne, określone w polskim systemie prawnym czyli przede wszystkim możliwość złożenia pisemnych zastrzeżeń do protokołu kontroli (projektowany art. 18zc ust. 5), czy możliwość odwołania od decyzji administracyjnej. Ponadto, zgodnie z projektowanymi przepisami dotyczącymi kontroli, o której mowa w projektowanym art. 18zc ust. 1, w zakresie nieuregulowanym w niniejszym rozdziale stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.

Z wyrazami szacunku

Z upoważnienia Ministra Finansów

$Imię_i_Nazwisko_podpisującego
$Stanowisko/Funkcja_podpisującego