UZASADNIENIE

Rozporządzenie Ministra Cyfryzacji w sprawie udzielania pomocy de minimis na wsparcie przedsiębiorstw wodociągowo-kanalizacyjnych w zakresie cyberbezpieczeństwa w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, dalej zwane „rozporządzeniem de minimis", ma na celu wsparcie przedsiębiorstw wodociągowo-kanalizacyjnych w zapewnianiu cyberbezpieczeństwa w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, dalej zwanego „KPO".

Plan rozwojowy – KPO zgodnie z definicją zawartą w ustawie z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2025 r. poz. 198), dalej zwane „ustawą", to dokument, o którym mowa w art. 17 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/241 z dnia 12 lutego 2021 r. ustanawiającego Instrument na rzecz Odbudowy i Zwiększania Odporności (Dz. Urz. UE L 57 z 18.02.2021, str. 17, z późn. zm.), stanowiący podstawę realizacji reform i inwestycji objętych wsparciem ze środków europejskiego Instrumentu na rzecz Odbudowy i Zwiększania Odporności (Recovery and Resilience Facility – RRF). KPO jest dokumentem programowym określającym cele związane z odbudową i tworzeniem odporności społeczno-gospodarczej Polski po kryzysie wywołanym pandemią COVID-19. Jego realizacja służy promowaniu spójności gospodarczej, społecznej i terytorialnej przez zwiększenie odporności, gotowości na wypadek sytuacji kryzysowych, zdolności dostosowawczych i potencjału wzrostu gospodarczego, łagodzeniu społecznych i gospodarczych skutków kryzysu wywołanego pandemią COVID-19, wspieraniu zielonej transformacji, przyczynianiu się do realizacji unijnych celów w zakresie klimatu oraz transformacji cyfrowej. KPO koncentruje swoje działania na sześciu europejskich filarach w ramach odpowiedzi na kryzys i budowę odporności:

1) zielona transformacja;
2) transformacja cyfrowa;
3) inteligentny i trwały wzrost sprzyjający włączeniu społecznemu;
4) spójność społeczna i terytorialna;
5) opieka zdrowotna oraz odporność gospodarcza, społeczna i instytucjonalna;
6) polityki na rzecz następnego pokolenia, takie jak edukacja i umiejętności.

Interwencje KPO uzupełnią i rozszerzą podejmowane dotychczas przez rząd i samorządy działania doraźne i antyrecesyjne na rzecz sektorów i przedsiębiorców. Dla osiągnięcia zakładanych celów KPO, Polska planuje podjęcie szeregu kluczowych reform oraz towarzyszących im inwestycji, które pozwolą nie tylko przezwyciężyć kryzys po pandemiczny,

ale także przyśpieszyć, w ciągu najbliższych kilku lat w okresie jego realizacji, transformację gospodarki polskiej i europejskiej oraz zwiększyć poziom życia Polaków. Realizacja KPO została skoncentrowana wokół następujących sześciu komponentów, stanowiących obszary koncentracji reform i inwestycji: A. Odporność i konkurencyjność gospodarki; B. Zielona energia i zmniejszenie energochłonności; C. Transformacja cyfrowa; D. Efektywność, dostępność i jakość systemu ochrony zdrowia; E. Zielona, inteligentna mobilność; F. Poprawa jakości instytucji i warunków realizacji KPO.

W KPO przewidziano realizację inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo", której celem jest w szczególności wzmocnienie cyberodporności systemów informacyjnych (IT i OT) wykorzystywanych w podmiotach wchodzących w skład krajowego systemu cyberbezpieczeństwa, zapewnienie wysoce wydajnej, energooszczędnej i skalowalnej infrastruktury obliczeniowej, zwiększenie bezpieczeństwa ciągłości jej działania oraz odporności na zakłócenia, tj. skutki zagrożeń epidemiologicznych, jak również zwiększenie wydajności i wydolności systemów bezpieczeństwa publicznego oraz zwiększenie możliwości infrastrukturalnych w zakresie bezpieczeństwa publicznego. W ramach komponentu Cyberbezpieczeństwo (program CyberPL) realizowany jest m.in. obszar interwencji pn. KSC – PL – Program podniesienia skuteczności funkcjonowania krajowego systemu cyberbezpieczeństwa, w skład którego wchodzi niniejsze przedsięwzięcie. Celem tego programu jest m.in. uzyskanie rozszerzonej świadomości sytuacyjnej oraz systemowego wsparcia operacyjnego w reagowaniu na incydenty poprzez m.in. wzmocnienie potencjału i modernizacja infrastruktury (IT i OT) podmiotów krajowego systemu cyberbezpieczeństwa oraz innych podmiotów kluczowych, szczególnie operatorów usług kluczowych poprzez m.in. modernizację sprzętu i oprogramowania, podniesienie jakości oprogramowania, urządzeń i usług. Ponadto istotnym elementem obszaru jest zapewnienie systemowego programu podnoszącego świadomość, wiedzę i kompetencje kadr w podmiotach krajowego systemu cyberbezpieczeństwa. Jako obszar szczególnie istotny zidentyfikowano w tym zakresie przedsiębiorstwa wodociągowo-kanalizacyjne. Jest to obszar, w którym szeroko wykorzystywane są technologie operacyjne (OT), a świadczone usługi służą realizacji zadań publicznych i są realizowane w większości przez jednostki organizacyjne jednostek samorządu terytorialnego lub przez samorządowe osoby prawne. Są to więc usługi szczególnie istotne dla obywateli, a równocześnie

są one szczególnie narażone na cyberataki. W związku z powyższym konieczne jest wzmocnienie tych podmiotów.

Realizacja powyższych działań przyczyni się do wzmocnienia cyberodporności systemów informacyjnych (IT i OT) wykorzystywanych w tych podmiotach, w tym do zwiększenia bezpieczeństwa, ciągłości ich działania oraz zwiększenia wydajności.

Przedsięwzięcie to przyczyni się również do podniesienia skuteczności funkcjonowania krajowego systemu cyberbezpieczeństwa, tj. m.in. uzyskania rozszerzonej świadomości sytuacyjnej oraz systemowego wsparcia operacyjnego w reagowaniu na incydenty poprzez m.in. wzmocnienie potencjału (IT i OT) przedsiębiorstw wodociągowo-kanalizacyjnych poprzez m.in. modernizację sprzętu i oprogramowania.

Technologie operacyjne (OT) obejmują szeroki zakres programowalnych systemów i urządzeń, które wchodzą w interakcję ze środowiskiem fizycznym (lub zarządzają urządzeniami, które wchodzą w interakcję ze środowiskiem fizycznym). Te systemy i urządzenia wykrywają lub powodują bezpośrednie zmiany poprzez monitorowanie i/lub kontrolę sprzętu, procesów i zdarzeń. Przykładami OT są systemy SCADA, kontrolery PLC, systemy Andon, czujniki IIoT (Industrial Internet of Things), systemy Embedded, elektroniczny Kanban (eKanban), systemy HMI (Human Machine Interface), itd. OT jest krytyczne z punktu widzenia przedsiębiorstw i ciągłości biznesowej jego procesów wytwórczych.

Na podstawie projektowanego rozporządzenia wsparcie udzielane będzie w ramach, wchodzącej w skład komponentu C Transformacja cyfrowa, inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo". W tym względzie realizowane działania w ramach inwestycji mają na celu zapewnienie cyberbezpieczeństwa przedsiębiorstw wodociągowo-kanalizacyjnych. W ramach KPO za realizację reform i inwestycji odpowiadają instytucje odpowiedzialne za realizacje reform i instytucje odpowiedzialne za realizacje inwestycji. Zgodnie z definicją zawartą w ustawie instytucją odpowiedzialną za realizację inwestycji jest minister kierujący działem administracji rządowej, któremu zgodnie z planem rozwojowym zostało powierzone to zadanie. Instytucja odpowiedzialna za realizację inwestycji może powierzyć realizację zadań związanych z realizacją inwestycji jednostce wspierającej plan rozwojowy. Instytucją odpowiedzialną za realizację przedmiotowej inwestycji jest Minister Cyfryzacji i to on jest odpowiedzialny za wydanie programu pomocowego. Podstawą do wydania rozporządzenia przez Ministra Cyfryzacji jest art. 14lc ust. 4 ustawy, w którym zawarta została delegacja do wydawania

programów pomocowych (rozporządzeń) w przypadku wsparcia stanowiącego pomoc publiczną lub pomoc de minimis udzielaną w ramach KPO przez ministra właściwego pełniącego funkcję instytucji odpowiedzialnej za realizację inwestycji.

Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:

1) Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP), w odniesieniu do 4.2.2. „Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office)" oraz 4.2.3. „Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej". Przedsięwzięcie realizuje kierunek interwencji 5.2.2. Zarządzanie infrastrukturą IT.

2) Realizacja Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, w tym, w szczególności celu szczegółowego nr 1 – rozwój krajowego systemu cyberbezpieczeństwa oraz celu szczegółowego nr 2 – Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.

Projekt rozporządzenia szczegółowo określa cel pomocy wskazując, że wsparcie otrzyma jedynie ograniczona grupa podmiotów z sektora wodociągowo-kanalizacyjnego. Konkursowy tryb naboru wniosków zapewni, że pomoc de minimis otrzymają podmioty, które najlepiej mogą wykorzystać dodatkowe środki. Zapewni to efektywne i skuteczne wykorzystanie tej pomocy. Równocześnie konkursowy model wyboru wniosków, które otrzymają dofinansowanie, zapewnia niezbędną przejrzystość tego procesu.

Żadne odrębne przepisy nie określają szczegółowego przeznaczenie, warunków lub trybu udzielania pomocy, o której mowa w projekcie rozporządzenia, w związku z czym konieczne jest określenie ich w przedmiotowym akcie prawnym.

Projekt rozporządzenia określa szczegółowe przeznaczenie, warunki i tryb udzielania pomocy de minimis, do której mają zastosowanie przepisy rozporządzenia Komisji (UE) 2023/2831 z dnia 13 grudnia 2023 r. w sprawie stosowania art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej do pomocy de minimis, a także podmioty udzielające tej pomocy.

W § 1 projektu rozporządzenia został określony zakres przedmiotowy projektowanego rozporządzenia.

W § 2 projektu rozporządzenia zdefiniowane zostały podstawowe pojęcia, którymi posługuje

się projektowane rozporządzenie, tj. definicje cyberbezpieczeństwa, przedsiębiorstwa wodociągowo-kanalizacyjnego oraz przedsięwzięcia.

Przepis § 3 wskazuje, że wsparcie będzie udzielane w formie pomocy de minimis zdefiniowanej w rozporządzenia Komisji (UE) 2023/2831 z dnia 13 grudnia 2023 r. w sprawie stosowania art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej do pomocy de minimis, co zapewnia zgodność tej pomocy z rynkiem wewnętrznym Unii Europejskiej.

Z kolei przepis § 4 precyzuje jakim przedsiębiorstwom wodociągowo-kanalizacyjnym może być udzielane wsparcie w ramach niniejszego rozporządzenia. Będzie to przedsiębiorstwo wodociągowo-kanalizacyjne, które jest:

1) operatorem usług kluczowych w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), lub
2) spółką prawa handlowego wykonującą zadania o charakterze użyteczności publicznej w rozumieniu przepisów ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679), wykorzystując technologie operacyjne w przemysłowych systemach sterowania, lub
3) jednostką sektora finansów publicznych, o której mowa w art. 9 pkt 2–4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, 1572, 1717, 1756, i 1907 oraz z 2025 r. poz. 39).

Wystąpienie incydentu w tych podmiotach oraz przerwanie świadczenia usług może mieć szczególnie negatywny wpływ na funkcjonowanie państwa i społeczeństwa.

Zgodnie z § 5 wsparcie obejmie przedsięwzięcia zwiększające poziom bezpieczeństwa informacji przez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w przedsiębiorstwach wodociągowo-kanalizacyjnych. W ramach niniejszego przedsięwzięcia planowane jest udzielenie wsparcia na inwestycje w 3 obszarach:

1) wdrożenie środków organizacyjnych służących zapewnieniu cyberbezpieczeństwa;
2) zakup lub modernizację środków technicznych służących zapewnieniu cyberbezpieczeństwa;
3) rozwój kompetencji personelu w zakresie cyberbezpieczeństwa.

Przykładowe działania jakie mogą być finansowane w ramach obszaru 1 to:

- przegląd, aktualizacja lub opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji,

- wprowadzenie środków obejmujących m.in.: politykę analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługę incydentu, ciągłość działania i zarządzanie kryzysowe, polityki i procedury stosowania kryptografii i szyfrowania, politykę kontroli dostępu, stosowanie uwierzytelniania wieloskładnikowego,
- audyt systemu zarządzania bezpieczeństwem informacji przeprowadzonego przez wykwalifikowanego audytora, stanowiącego dowód wdrożenia i stosowania ww. systemu w organizacji lub instytucji.

Przykładowe działania jakie mogą być finansowane w ramach obszaru 2 to:

- zakup i wdrożenie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, reakcję i detekcję zagrożeń cyberbezpieczeństwa,
- usługi wdrożenia i konfiguracji urządzeń i oprogramowania oraz wsparcia eksperckiego w zakresie cyberbezpieczeństwa,
- zakup i wdrożenie systemów lub usług na potrzeby operacyjnych centrów bezpieczeństwa (SOC),
- zakup lub rozwój systemów lub usług zarządzania podatnościami i skanerów podatności.

Przykładowe działania jakie mogą być finansowane w ramach obszaru 3 to:

- szkolenia z zakresu cyberbezpieczeństwa dla kadry danego podmiotu istotnej z punktu widzenia wdrożonej polityki cyberbezpieczeństwa lub systemu zarządzania bezpieczeństwem informacji, w tym w szczególności w zakresie środków wdrażanych w ramach przedsięwzięcia,
- szkolenia z zakresu cyberbezpieczeństwa dla: informatyków odpowiedzialnych za cyberbezpieczeństwo, kadry kierowniczej oraz pozostałych pracowników podmiotu, obejmujących m.in. symulowane cyberataki na użytkowników sieci i systemów informacyjnych w organizacji (np. phishing).

Norma § 6 określa, że pomoc de minimis będzie udzielana przez CPPC. Jest to podmiot zaangażowany już w działania w ramach KPO, który swoim doświadczeniem gwarantuje prawidłowy przebieg procesu udzielania pomocy.

W § 7 określono ogólnie, że kosztami kwalifikowalnymi mogą być wyłącznie koszty poniesione na realizację przedsięwzięcia, o którym mowa w § 5.

Ponadto w § 7 ust. 2 projektu rozporządzenia wskazano, że pomoc de minimis nie może przekroczyć 100% poniesionych i udokumentowanych kosztów kwalifikowanych przedsięwzięcia, o którym mowa w § 5. Pomoc de minimis będzie udzielana na pokrycie części lub całości kosztów przedsięwzięć dotyczących zapewnienia cyberbezpieczeństwa w danym podmiocie. Pomoc de minimis będzie udzielana na pokrycie części kosztów ponoszonych na realizację przedsięwzięć, w sytuacji, w której podmiot udzielający pomocy określi w naborze, jakie konkretnie koszty przedsięwzięć mogą być pokryte pomocą de minimis i nie będą to wszystkie koszty poniesione albo przewidziane do poniesienia w ramach danych przedsięwzięć.

W § 8 projekt rozporządzenia określa formę, w jakiej będzie udzielana pomoc de minimis na podstawie projektowanego rozporządzenia, którą będzie bezzwrotne wsparcie. Taka forma wynika z tego, że podmioty, które otrzymają wsparcie realizują istotne zadanie publiczne jakim jest zaopatrywanie w wodę.

Przepis § 9 projektu rozporządzenia określa wartość dopuszczalnej pomocy odsyłając, w tym zakresie, do przepisów rozporządzenia nr 2023/2831.

W § 10 projektu rozporządzenia uregulowano tryb udzielenia pomocy de minimis, w zakresie składania wniosku do CPPC.

W § 10 ust. 3 wskazano także, że wniosek może zawierać również inne informacje niezbędne do dokonania oceny wniosku, określone w regulaminie konkursu, w ramach którego będzie prowadzony nabór. Zaproponowane rozwiązanie jest konsekwencją faktu, iż program pomocowy jest przewidziany jako podstawa prawna udzielania pomocy de minimis w nieokreślonych z góry przypadkach, na szeroki katalog kosztów kwalifikowalnych i nie jest możliwe jednoznaczne wskazanie, jakiego rodzaju informacje mogą być potrzebne do ocenienia poszczególnych wniosków. Informacje te będą wskazane w regulaminie naboru wniosków o udzielenie pomocy. Należy również podkreślić, że wśród tych innych informacji nie będzie informacji mających charakter danych osobowych.

Wskazany w § 10 ust. 4 pkt 1 obowiązek załączania przez przedsiębiorstwo wodociągowo-kanalizacyjne nałożono obowiązek dołączenia do wniosku zaświadczeń albo oświadczeń o udzielonej pomocy de minimis w sektorze rolnictwa lub rybołówstwa wynika z regulacji zawartej w art. 5 rozporządzenia nr 2023/2831, tj. z obowiązku kumulacji wszystkich rodzajów pomocy de minimis udzielonych na podstawie różnych aktów prawa Unii Europejskiej (a zatem również pomocy de minimis w sektorze rolnictwa lub rybołówstwa) do limitu wskazanego

w art. 3 ust. 2 rozporządzenia nr 2023/2831. Przepis § 11 ust. 4 zakłada obowiązek załączania informacji dotyczy informacji niezbędnych do udzielenia pomocy de minimis, dotyczących w szczególności wnioskodawcy i prowadzonej przez niego działalności gospodarczej oraz wielkości i przeznaczenia pomocy publicznej otrzymanej w odniesieniu do tych samych kosztów kwalifikujących się do objęcia pomocą, na pokrycie których ma być przeznaczona pomoc de minimis.

Przepis § 11 projektu określa w jaki sposób prowadzony jest nabór wniosków oraz sposób ogłoszenia o konkursie.

Określono również procedurę usunięcia błędów formalnych wniosku, tak aby każde z wnioskujących przedsiębiorstw wodociągowo-kanalizacyjnych mogło skutecznie złożyć wniosek i nie traciło szansy na wsparcie.

Zgodnie z § 11 projektu pomoc de minimis będzie udzielana w trybie konkursowym przedsiębiorstwom wodociągowo-kanalizacyjnym, którzy złożą wnioski o udzielenie pomocy de minimis. Obsługą ww. wniosków będzie zajmowało się CPPC. Nabór wniosków będzie trwał co najmniej miesiąc, zapewniając wszystkim przedsiębiorstwom wodociągowo-kanalizacyjnym odpowiedni czas na przygotowanie dokumentacji.

Wybór wniosków w konkursie będzie odbywał się na podstawie regulaminu konkursu, który ustali CPPC. Każdy wniosek zostanie oceniony co najmniej pod kątem tego w jakim stopniu zaproponowane działania służą zapewnieniu cyberbezpieczeństwa przedsiębiorstwa wodociągowo-kanalizacyjnego, którego dotyczą, a także dopuszczalności zakwalifikowania zaproponowanych przez przedsiębiorstwa wodociągowo-kanalizacyjne kosztów kwalifikowalnych. Sprecyzowano również, że w ramach naboru przedsiębiorstwo wodociągowo-kanalizacyjne będzie mogło złożyć tylko jeden wniosek.

W § 12 projekt rozporządzenia reguluje procedurę oceny wniosków i udzielania pomocy przez CPPC. Z uwagi na fakt, iż pomoc de minimis udzielana przez ostatecznych odbiorców wsparcia na rzecz przedsiębiorstw wodociągowo-kanalizacyjnych będzie pomocą na tzw. drugim poziomie, wsparcie będzie udzielane na podstawie umowy o udzielenie pomocy, która nie jest umową o objęcie przedsięwzięcia wsparciem z KPO w rozumieniu ustawy.

Z kolei § 13 projektu wskazuje, że kryteria wyboru wniosków muszą mieć obiektywny charakter i zapewniać efektywne i skuteczne wykorzystanie pomocy de minimis. Przepis ten wyznacza jakie muszą być kryteria wyboru wniosków i gwarantuje, że będą służyły realizacji celu niniejszego projektu.

Przepis § 14 projektu rozporządzenia precyzuje, że po dokonaniu wyboru wniosków, pomoc de minimis będzie udzielana podstawie umowy o udzielenie pomocy de minimis.

Na podstawie § 15 projektu rozporządzenia zobowiązuje się przedsiębiorstwo wodociągowo-kanalizacyjne do przedłożenia, przed podpisaniem umowy, określonych informacji i zaświadczeń albo oświadczeń. Rozwiązanie to ma na celu umożliwienie podmiotowi udzielającemu pomocy dokonania weryfikacji, czy w momencie jej udzielenia nie zostanie przekroczony dopuszczalny limit pomocy i czy nie zostaną naruszone reguły kumulacji pomocy.

Przepis § 16 wskazuje, że umowa między przedsiębiorstwem wodociągowo-kanalizacyjnym a CPPC określa częstotliwość z jaką beneficjent będzie sprawozdawał z realizacji przedsięwzięcia. Pozwoli to CPPC monitorować czy pomoc de minimis wydatkowana jest w sposób efektywny i zgodny z przepisami.

W § 17 projektu rozporządzenia wskazany został termin, do którego będzie udzielana pomoc. Zgodnie z postanowieniami art. 7 ust. 3 w związku z art. 8 rozporządzenia nr 2023/2831 możliwość udzielania pomocy de minimis na podstawie obecnie obowiązujących przepisów prawa unijnego wskazuje na dzień 30 czerwca 2031 r. Jednak w związku z tym, że data końcowa kwalifikowalności wydatków w KPO została określona na dzień 30 czerwca 2026 r. Dzień 30 czerwca 2026 r. będzie więc ostatnim dniem z jakim będzie można wydatkować środki otrzymane w ramach pomocy de minimis. Data ta została również wskazana, jako zakończenie inwestycji C3.1.1. „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo", w załączniku do wniosku dotyczącego decyzji wykonawczej Rady zmieniającej decyzję wykonawczą (UE) (ST 9728/22 INIT; ST/9728/22 ADD 1) z dnia 17 czerwca 2022 r. w sprawie zatwierdzenia oceny planu odbudowy i zwiększania odporności Polski.

W § 18 projektu rozporządzenia określono termin wejścia w życie przedmiotowego aktu. Zgodnie z art. 4 ust. 1 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2019 r. poz. 1461) standardowy okres vacatio legis wynosi 14 dni, natomiast zgodnie z art. 4 ust. 2 w uzasadnionych przypadkach termin ten może zostać skrócony. Uzasadnione jest skrócenie terminu wejścia w życie przedmiotowego aktu normatywnego z uwagi na przyspieszenie udzielania przedsiębiorstwom wodociągowo-kanalizacyjnym pomocy na podstawie nowych przepisów, korzystniejszych z uwagi na zwiększenie limitu dopuszczalnej pomocy de minimis do 300 tys. EUR w okresie 3 lat dla

jednego przedsiębiorstwom wodociągowo-kanalizacyjnym (obecnie limit wynosi 200 tys. EUR). Ponadto zaproponowany termin wejścia w życie rozporządzenia nie narusza zasad demokratycznego państwa prawnego i nie stoi w sprzeczności z art. 4 ust. 2 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych. Mając na uwadze powyższe rozporządzenie wejdzie w życie z dniem następującym po dniu ogłoszenia.

Projektowane przepisy są zgodne z przepisami Unii Europejskiej.

Projekt nie podlega przedstawieniu właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt rozporządzenia nie podlega procedurze notyfikacji w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. z 2002 r. poz. 2039 oraz z 2004 r. poz. 597), ponieważ nie zawiera przepisów technicznych.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248 oraz z 2024 r. poz. 1535), projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw informatyzacji. Ponadto, zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806), projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.