| | |
|---|---|
| **Nazwa projektu**<br>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<br><br>**Ministerstwo wiodące i ministerstwa współpracujące**<br>Ministerstwo Cyfryzacji<br><br>**Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu**<br>Paweł Olszewski, Sekretarz Stanu<br><br>**Kontakt do opiekuna merytorycznego projektu**<br>Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa<br>lukasz.Wojewoda@cyfra.gov.pl<br><br>Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa<br>marcin.Wysocki@cyfra.gov.pl<br><br>e-mail: Sekretariat.DC@cyfra.gov.pl | **Data sporządzenia**<br>10.03.2025 r.<br><br>**Źródło:** art. 14lc ust. 4 ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2025 r. poz. 198)<br><br>**Nr w Wykazie prac legislacyjnych Ministra Cyfryzacji: 27** |

# OCENA SKUTKÓW REGULACJI

## 1. Jaki problem jest rozwiązywany?

Polska cyberprzestrzeń jest jedną z najczęściej atakowanych przez hakerów na całym świecie. W 2020 r. 13% polskich firm stało się celem cyberataku ransomware, czyli wymuszenia okupu za umożliwienie dostępu do danych zablokowanych za pomocą złośliwego oprogramowania. Sytuacja w cyberprzestrzeni z każdym rokiem staje się coraz bardziej niebezpieczna. Zespół CSIRT NASK, jeden z trzech zespołów poziomu krajowego zajmujących się incydentami cyberbezpieczeństwa, z roku na rok odnotowuje coraz więcej incydentów. W 2021 r. było to prawie 30 tys. incydentów, a w 2022 r. prawie 40 tys. incydentów. W 2023 r. było to już ponad 80 tys. incydentów – co oznacza wzrost o ponad 100% w stosunku do ubiegłego roku. W ciągu pierwszych 5 miesięcy 2024 r. odnotowano już około 47,6 tys. incydentów i jeśli ten trend się utrzyma to w tym roku może zostać przekroczona liczba 100 tys. zgłoszonych incydentów. W związku z tym konieczne jest podjęcie działań służących zwiększeniu cyberbezpieczeństwa w obszarach kluczowych z punktu widzenia funkcjonowania państwa i społeczeństwa.
Przyjęta do sfinansowania w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), w ramach komponentu C – Transformacja Cyfrowa, inwestycja C3.1.1. „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo" zakłada wydatkowanie środków na wsparcie podmiotów krajowego systemu cyberbezpieczeństwa w zakresie zwiększania cyberbezpieczeństwa i służy osiągnięciu ww. celu.

KPO jest finansowany w ramach przyjętego przez państwa członkowskie Unii Europejskiej Instrumentu na rzecz Odbudowy i Zwiększania Odporności (Recovery and Resilience Facility – RRF). Jednym z kluczowych wyzwań w tym zakresie jest zwiększenie poziomu cyberbezpieczeństwa w podmiotach kluczowych z punktu widzenia gospodarki. Jednym z takich sektorów, objętych krajowym systemem cyberbezpieczeństwa, jest sektor zaopatrywania w wodę. Szeroko w tym sektorze wykorzystywane są technologie operacyjne (OT) do sterowania i monitorowania świadczonych usług. Wystąpienie incydentu w tym obszarze łatwo mogłoby prowadzić do przerwania ciągłości świadczonych usług. Ponadto, jest to obszar w którym nie jest łatwo uzyskać środki na inwestycje z rynku prywatnego. Dlatego ten obszar wymaga działania ze strony państwa. Podmioty, dla których jest dedykowana pomoc, stanowią również podmioty krajowego systemu cyberbezpieczeństwa, zgodnie z art. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222).

Podstawą do wydania przedmiotowego rozporządzenia jest art. 14lc ust. 4 ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju. Podmiotem uprawnionym do wydania programów pomocowych umożliwiających takie wsparcie jest właściwy minister pełniący funkcję instytucji odpowiedzialnej za realizację inwestycji – w zakresie, w jakim pomoc, o której mowa powyżej, ma być udzielana w ramach inwestycji.

## 2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projektowane rozporządzenie ma umożliwić udzielanie pomocy *de minimis* przedsiębiorstwom wodociągowo-kanalizacyjnym na inwestycje z zakresu cyberbezpieczeństwa. Wsparcie będzie udzielane na przedsięwzięcie, którego celem jest zapewnienie cyberbezpieczeństwa wewnątrz danego podmiotu poprzez inwestycje w:
1) środki organizacyjne służące zapewnianiu cyberbezpieczeństwa;
2) środki techniczne służące zapewnianiu cyberbezpieczeństwa;
3) rozwój kompetencji personelu w zakresie cyberbezpieczeństwa.

Projektowane wsparcie pozwoli na zwiększenie cyberbezpieczeństwa w tych podmiotach poprzez inwestycje w sprzęt oraz kompetencje pracowników. Dzięki temu ten sektor gospodarki stanie się bardziej odporny na cyberzagrożenia. Należy podkreślić, że zagwarantuje to zapewnienie ciągłości działania tych przedsiębiorstw co pozytywnie wpłynie również na wszystkie inne podmioty korzystające z usług tych podmiotów.

Osiągnięcie celów inwestycji C3.1.1. „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo" w wyniku podjęcia działań innych niż legislacyjne nie jest możliwe.

## 3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Regulacja dotyczy programu pomocowego opartego o KPO, które jest dokumentem dotyczącym jedynie Rzeczpospolitej Polskiej, w związku z czym odstąpiono od analizy porównawczej z innymi państwami.

## 4. Podmioty, na które oddziałuje projekt

| Grupa | Wielkość | Źródło danych | Oddziaływanie |
|---|---|---|---|
| Przedsiębiorstwa z sekcji E.36.00.Z wg PKD – Pobór, uzdatnianie i dostarczanie wody | Liczebność populacji, która może ubiegać się o wsparcie w ramach inwestycji C3.1.1. „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo", w ramach komponentu C – Transformacja Cyfrowa.<br>Przedsiębiorstwa realizujące zadania polegające na zbiorowym zaopatrzeniu w wodę – 1965<br><br>Całkowita liczba wspartych przedsiębiorców do końca II kwartału 2026 z ramach Sekcji E.36.00.Z wg PKD, wyniesie minimum 430, zgodnie z założeniami KPO.<br><br>Stan na 31.11.2024 r. | „Miesięczna informacja GUS o podmiotach gospodarki narodowej w rejestrze REGON listopad 2024" (https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/miesieczna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-listopad-2024,4,91.html)<br><br>Informacje nt. liczby przedsiębiorstw objętych wsparciem będzie pochodzić ze sprawozdawczości KPO | Ułatwienie dostępu do pomocy publicznej z inwestycji C3.1.1. „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo", w ramach komponentu C – Transformacja Cyfrowa.<br><br>Bezpośrednie – otrzymana pomoc przyczyni się do wsparcia w zakresie cyberbezpieczeństwa min. 430 przedsiębiorstw z sekcji E.36.00.Z wg PKD.<br><br>Pośrednie – korzyści dla przedsiębiorstw, także spoza wymienionych sekcji PKD jako kooperantów, poddostawców, wykonawców robót i usług oraz odbiorców pozytywnych efektów zewnętrznych. |
| Minister właściwy do spraw informatyzacji | 1 | Informacja ogólnodostępna | Minister właściwy do spraw informatyzacji uzyska narzędzie, dzięki któremu będzie mógł udzielać wsparcia w zakresie cyberbezpieczeństwa w Polsce. |
| Centrum Projektów Polska Cyfrowa | 1 | Informacja Ogólnodostępna | Centrum Projektów Polska Cyfrowa, jako jednostka podległa Ministrowi Cyfryzacji, będzie organizować nabór i przeprowadzać konkurs |

| | | | |
|---|---|---|---|
| | | | na udzielenie pomocy *de minimis*. |

**5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji**

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.

Projekt został skierowany do opiniowania i konsultacji publicznych na okres 10 dni.

W ramach konsultacji publicznych projekt otrzymali:

1) Amerykańska Izba Handlowa w Polsce;
2) Centrum Łukasiewicz;
3) European AI Forum;
4) FAIR MARKET INSTITUTE;
5) Federacja Konsumentów;
6) Fundacja Bezpieczna Cyberprzestrzeń;
7) Fundacja Open Allies;
8) Fundacja OPOR;
9) Fundacja Pułaskiego;
10) Fundacja Rozwoju Obrotu Bezgotówkowego;
11) Green Rev Institute;
12) Instytut Kolejnictwa;
13) Internet Society Poland;
14) ISAC-GIG;
15) ISAC-Kolej;
16) ISAC-Lotniczy;
17) Izba Gospodarcza Wodociągi Polskie;
18) Izba Gospodarki Elektronicznej;
19) Izba POLMED;
20) Krajowa Izba Gospodarcza;
21) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
22) Krajowa Izba Gospodarki Cyfrowej;
23) Krajowa Izba Komunikacji Ethernetowej;
24) Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa;
25) Międzynarodowe Centrum Bezpieczeństwa Chemicznego (ICCSS);
26) Morskie Centrum Cyberbezpieczeństwa;
27) Naczelna Organizacja Techniczna;
28) Naczelna Rada Zrzeszeń Handlu i Usług;
29) Polska Izba Gospodarki Odpadami;
30) Polska Izba Informatyki i Telekomunikacji;
31) Polska Izba Kolei;
32) Polska Izba Komunikacji Elektronicznej;
33) Polska Izba Przemysłu Chemicznego;
34) Polska Organizacja Handlu i Dystrybucji;
35) Polska Rada Biznesu;
36) Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland;
37) Polski Związek Przemysłu Motoryzacyjnego;
38) Polskie Centrum Badań i Certyfikacji S.A.;
39) Polskie Stowarzyszenie Fotowoltaiki;
40) Polskie Stowarzyszenie Magazynowania Energii;

41) Polskie Stowarzyszenie Marketingu SMB;
42) Polskie Stowarzyszenie Menedżerów Logistyki i Zakupów;
43) Polskie Towarzystwo Informatyczne;
44) Polsko-Chińska Główna Izba Gospodarcza;
45) Porozumienie Zielonogórskie;
46) Sektorowa Rada ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
47) Skandynawska Izba Gospodarcza;
48) Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA;
49) Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji;
50) Stowarzyszenie Inżynierów Telekomunikacji;
51) Stowarzyszenie ISACA;
52) Stowarzyszenie ISSA Polska;
53) Stowarzyszenie Polska Izba Rozwoju Elektromobilności;
54) Sudecka Izba Przemysłowo-Handlowa;
55) Związek Banków Polskich;
56) Związek Cyfrowa Polska;
57) Związek Firm Biotechnologicznych;
58) Związek Telewizji Kablowych w Polsce Izba Gospodarcza.

W ramach opiniowania projekt otrzymali:
1) Centrum Projektów Polska Cyfrowa;
2) Komisja Nadzoru Finansowego;
3) Prezes Urzędu Komunikacji Elektronicznej;
4) Prezesa Urzędu Ochrony Konkurencji i Konsumentów;
5) Prezes Urzędu Zamówień Publicznych;
6) Prezes Urzędu Ochrony Danych Osobowych;
7) Prezes Głównego Urzędu Statystycznego;
8) Prezes Prokuratorii Generalnej Rzeczypospolitej Polskiej;
9) Rzecznik Małych i Średnich Przedsiębiorców;
10) Polskie Centrum Akredytacji;
11) Polski Komitet Normalizacyjny;
12) Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy;
13) Instytut Łączności – Państwowy Instytut Badawczy.

Projekt został przekazany do zaopiniowaniu przez Komisję Wspólną Rządu i Samorządu Terytorialnego.

Projekt nie wymaga zaopiniowania przez Radę Działalności Pożytku Publicznego, o której mowa w ustawie z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz. U. z 2024 r. poz. 1491, 1761 i 1940), gdyż nie dotyczy funkcjonowania organizacji pozarządowych oraz działalności pożytku publicznego oraz wolontariatu.
Projekt nie wymaga zaopiniowania przez Radę Dialogu Społecznego, o której mowa w ustawie z dnia 24 lipca 2015 r. o Radzie Dialogu Społecznego i innych instytucjach dialogu społecznego (Dz. U. z 2018 r. poz. 2232, z późn. zm.), gdyż nie dotyczy warunków rozwoju społeczno-gospodarczego oraz zwiększenia konkurencyjności polskiej gospodarki i spójności społecznej.
Projekt nie wymaga zaopiniowania przez Radę do Spraw Cyfryzacji, o której mowa w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717).
Projekt nie wymaga zaopiniowania przez związki zawodowe w trybie art. 19 ust. 1 ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2022 r. poz. 854 oraz z 2025 r. poz. 39), gdyż zakres rozporządzenia nie dotyczy zadań związków zawodowych.
Projekt nie wymaga zaopiniowania przez organizacje pracodawców w trybie art. 16 ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców (Dz. U. z 2022 r. poz. 97 oraz z 2025 r. poz. 39), gdyż zakres rozporządzenia nie dotyczy zadań organizacji pracodawców.
Wyniki konsultacji publicznych i opiniowania zostaną omówione po ich zakończeniu w raporcie z konsultacji.

## 6. Wpływ na sektor finansów publicznych

| (ceny stałe z …… r.) | Skutki w okresie 10 lat od wejścia w życie zmian [mln zł] | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | *Łącznie (0-10)* |
| **Dochody ogółem** | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | |
| JST | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | |
| **Wydatki ogółem** | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | |
| JST | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | |
| **Saldo ogółem** | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | |
| JST | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | |

| | |
|---|---|
| Źródła finansowania | Źródłem finansowania pomocy *de minimis* udzielanej na podstawie niniejszego rozporządzenia będą środki pochodzące z części dotacyjnej europejskiego Instrumentu na rzecz Odbudowy i Zwiększania Odporności. Indykatywny budżet wsparcia dla min. 430 przedsiębiorstw z sekcji E.36.00.Z wg PKD, realizujących zadania polegające na zbiorowym zaopatrzeniu w wodę, to ok. 69,8 mln EUR, co wg kursu EUR/PLN 4,4819 na dzień wydania decyzji ws. finansowania inwestycji, daje kwotę ok. 313 mln PLN. Nie jest przewidziane finansowanie pomocy de minimis ze środków budżetu państwa ani budżetów jednostek samorządu terytorialnego. |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | Kwota pomocy *de minimis* udzielanej na podstawie niniejszego rozporządzenia wchodzi w skład alokacji przewidzianej dla inwestycji C3.1.1. „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo", której łączna wartość wynosi 477 913 286,00 EUR, co wg kursu EUR/PLN 4,4819 na dzień wydania decyzji ws. finansowania inwestycji, daje łączną kwotę w wysokości 2 141 959 557,00 PLN.<br>Projektowane rozporządzenie zapewni realizację drugiego naboru wniosków o granty, dedykowanego dla przedsiębiorstw realizujących zadania polegające na zbiorowym zaopatrzeniu w wodę, w ramach projektu pn. „Udzielenie 500 podmiotom wsparcia na rzecz modernizacji i rozbudowania infrastruktur cyberbezpieczeństwa przy wykorzystaniu technologii informacyjnej i technologii operacyjnej", wchodzącego w skład wskaźnika C23G KPO, zgodnie zapisami załącznika 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, z dnia 1.7.2024 r. (CID). Jest to projekt, w ramach którego przedsiębiorstwa realizujące zadania polegające na zbiorowym zaopatrzeniu w wodę będą mogły otrzymać wsparcie finansowe na cyberbezpieczeństwo. |

## 7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

| | | Skutki | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Czas w latach od wejścia w życie zmian | | 0 | 1 | 2 | 3 | 5 | 10 | *Łącznie (0-10)* |
| W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.) | duże przedsiębiorstwa | | | | | | | |
| | sektor mikro-, małych i średnich przedsiębiorstw | | | | | | | |
| | rodzina, obywatele oraz gospodarstwa domowe | | | | | | | |
| W ujęciu niepieniężnym | duże przedsiębiorstwa | Dodatkowe wsparcie finansowe przyczyni się do wzmocnienia cyberodporności systemów informacyjnych (IT i OT), wykorzystywanych w przedsiębiorstwach wodociągowo-kanalizacyjnych z sekcji E.36.00.Z wg PKD, realizujących zadania | | | | | | |

| | | |
|---|---|---|
| | | polegające na zbiorowym zaopatrzeniu w wodę, w tym do zwiększenia bezpieczeństwa, ciągłości i wydajności ich działania. |
| | sektor mikro-, małych i średnich przedsiębiorstw | Dodatkowe wsparcie finansowe przyczyni się do wzmocnienia cyberodporności systemów informacyjnych (IT i OT), wykorzystywanych w przedsiębiorstwach wododociągowo-kanalizacyjnych z sekcji E.36.00.Z wg PKD, realizujących zadania polegające na zbiorowym zaopatrzeniu w wodę, w tym do zwiększenia bezpieczeństwa, ciągłości i wydajności ich działania. |
| | rodzina, obywatele oraz gospodarstwa domowe | Wzrost cyberbezpieczeństwa w przedsiębiorstwach wodociągowo-kanalizacyjnych, realizujących zadania polegające na zbiorowym zaopatrzeniu w wodę, przełoży się na większe bezpieczeństwo świadczonych przez nie usług, a co za tym idzie na zwiększenie bezpieczeństwa dla życia i zdrowia obywateli. |
| | pracownicy MŚP ze wspieranych sektorów | Wzrost kompetencji zawodowych pracowników przedsiębiorstw wodociagowo-kanalizacyjnych, realizujących zadania polegające na zbiorowym zaopatrzeniu w wodę, w wyniku przeprowadzonych szkoleń z zakresu cyberbezpieczeństwa. |
| Niemierzalne | rozwój regionalny | Nie zakłada się koncentracji regionalnej wsparcia. Projekt będzie realizowany w skali kraju. |
| | (dodaj/usuń) | |

| | |
|---|---|
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | „Krajowy Plan Odbudowy i Zwiększenia Odporności” przyjęty uchwałą Rady Ministrów z dnia 30 kwietna 2021 r. |

**8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu**

☒ nie dotyczy

| | |
|---|---|
| Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności). | ☐ tak<br>☒ nie<br>☐ nie dotyczy |
| ☐ zmniejszenie liczby dokumentów<br>☐ zmniejszenie liczby procedur<br>☐ skrócenie czasu na załatwienie sprawy<br>☐ inne: | ☐ zwiększenie liczby dokumentów<br>☐ zwiększenie liczby procedur<br>☐ wydłużenie czasu na załatwienie sprawy<br>☐ inne: |
| Wprowadzane obciążenia są przystosowane do ich elektronizacji. | ☐ tak<br>☐ nie<br>☒ nie dotyczy |

Komentarz:

Nie dotyczy.

**9. Wpływ na rynek pracy**

Projektowane rozporządzenie będzie miało pozytywny wpływ na rynek pracy w sektorze wodociągowo-kanalizacyjnym. Ukierunkowanie wsparcia na przedsięwzięcia służące zapewnieniu cyberbezpieczeństwa przyczynią się do stabilizacji zatrudnienia we wspieranych podmiotach, zwiększenie kompetencji pracowników, a także pozwoli na utworzenie nowych stanowisk w ramach wspieranych podmiotów.

**10. Wpływ na pozostałe obszary**

| | | |
|---|---|---|
| ☐ środowisko naturalne<br>☐ sytuacja i rozwój regionalny<br>☐ sądy powszechne, administracyjne lub wojskowe | ☐ demografia<br>☐ mienie państwowe<br>☐ inne: | ☒ informatyzacja<br>☐ zdrowie |

| | |
|---|---|
| Omówienie wpływu | Dzięki wsparciu podmioty z sektora wodociągowo-kanalizacyjnego będą mogły rozbudować swoje systemy zarządzania bezpieczeństwem informacji oraz wykorzystywane systemy teleinformatyczne, osiągając wyższą dojrzałość w obszarze cyberbezpieczeństwa. |

**11.Planowane wykonanie przepisów aktu prawnego**

Projektowane rozporządzenie wejdzie w życie z dniem następującym po dniu ogłoszenia.

**12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?**

Weryfikacja osiągniętych rezultatów inwestycji będzie dokonana zgodnie z systemem sprawozdawczości KPO oraz Mechanizmem weryfikacji osiągnięcia wskaźnika dla inwestycji C3.1.1. „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo" określonym w umowie technicznej z Komisją Europejską (tzw. ustalenia operacyjne).

**13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)**

Nie dotyczy.