

prezydent@inowroclaw.pl

Od: urzad@inowroclaw.pl
Wysłano: piątek, 6 października 2023 09:40
Do: prezydent@inowroclaw.pl
Temat: FW: Oficjalny Wniosek na mocy art 63 Konstytucji RP w trybie Ustawy o dostępie do informacji Publicznej w związku z art. 241 KPA
Załączniki: Wkład merytoryczny wniosku CPPC.docx; Wkład merytoryczny wniosku CPPC.pdf; Cyberbezpieczny samorząd List Przewodni.pdf; Cyberochrona JST - Wstępna oferta współ pracy.pdf; Cyberochrona JST - Pytania i odpowiedzi.pdf; Inicjatywa wszyscy dbajmy o cyberbezpieczeństwo 2 - Zmieniamy Gminy na Lepsze .docx; Inicjatywa wszyscy dbajmy o cyberbezpieczeństwo 2 - Zmieniamy Gminy na Lepsze .docx.xades

2ej. 2926/2023
Dy 132/2023

Biuro Obsługi Interesantów
i Kontroli

Wpłynęło dnia 06.10.2023

L. Dz. 594/2023

p. J. Michalski

From: CKC RIG <CKC@rig.katowice.pl>
Sent: Friday, October 6, 2023 8:35 AM
To: adresat.urzad@samorzad.pl
Subject: Oficjalny Wniosek na mocy art 63 Konstytucji RP w trybie Ustawy o dostępie do informacji Publicznej w związku z art. 241 KPA

Adresatem niniejszej korespondencji jest - jest Organ - jednoznacznie identyfikowalny za pośrednictwem adresu e-mail pod którym odebrano niniejszą korespondencję. Rzeczony adres e-mail uzyskano z Biuletynu Informacji Publicznej Urzędu. Korespondencja kierowana jest do Kierownika Jednostki Samorządu Terytorialnego (dalej JST) - w rozumieniu art. 33 ust. 3 Ustawy z dnia 8 marca 1990 r. o samorządzie gminnym.

Szanowni Państwo,
W imieniu Centrum Kompetencji Cyberbezpieczeństwa Regionalnej Izby Gospodarczej oraz Polskiego Towarzystwa Informatycznego zwracamy się z propozycją podjęcia wspólnych działań w celu zapewnienia niezbędnego poziomu cyberbezpieczeństwa w Państwa urzędzie.

Cytując fragment listu przewodniego Prezesa Polskiego Towarzystwa Informatycznego (pełna treść w załączeniu): „(...) Zapewnienie efektywnego i kompleksowego cyberbezpieczeństwa to poważne (i wciąż rosnące) wyzwanie dla Władz Samorządowych. Ryzyko cyberataków prowadzących do utraty danych czy zablokowania pracy urzędu jest realnym problemem jaki może dotknąć każdą Jednostkę Samorządu Terytorialnego.

W 2024 r. poziom określonych prawem wymagań wzrośnie skokowo, po uruchomieniu nowej Dyrektywy UE (tzw. NIS2). (...)

Dostrzegając powyższe aspekty, Ministerstwo Cyfryzacji przygotowało program dofinansowania wydatków ponoszonych przez JST na zwiększenie cyberbezpieczeństwa. Program nosi nazwę **Cyberbezpieczny Samorząd. Wnioski JST mogą składać do dnia 13.10.2023 r. (...) „**

Możliwa do uzyskania kwota dofinansowania - może sięgać kwoty 850 tys. pln - per gmina.

Szczegółowe informacje, dot. przyznanych dla poszczególnych gmin, kwot - można znaleźć pod adresem URL: <https://www.gov.pl/attachment/ab5f4848-f10b-45d0-a30a-7bd72dd3d75c>

Według naszej oceny bazującej na ogólnodostępnych informacjach i kwerendach publicznych Gminy mają powszechny problem z wdrażaniem rozwiązań organizacyjnych i technicznych, zapewniających zdolność do monitorowania, ochrony i zarządzania incydentami cyberbezpieczeństwa, a także spełnieniem ustawowych obowiązków w tym zakresie.

Dlatego przy współpracy z zespołem ekspertów Polskiego Towarzystwa Informatycznego przygotowaliśmy zestaw materiałów, którym chcemy wesprzeć Państwo w aplikowaniu o przedmiotowe dofinansowanie.

Załączamy przykładowy wsad merytoryczny do wniosku o dofinansowanie.

Jednocześnie załączamy wzmiankowany list intencyjny oraz przydatne (według naszej oceny) materiały w zakresie kolejnych kroków możliwych i koniecznych do uzyskania przedmiotowego dofinansowania oraz realizacji działań wdrożenia systemu cyberbezpieczeństwa w JST.

Ze względu na fakt, że cyberzagrożenia mają obecnie charakter nieprzerwany i powszechny oraz z powodu uruchomienia przepisów, które już nakładają na JST określone wymagania w zakresie cyberbezpieczeństwa - wśród załączników znajduje się opracowana przez Centrum Kompetencji Cyberbezpieczeństwa RIG **proponycja realizacji usług pomostowych**. Skorzystanie z tej oferty umożliwia możliwie najszybsze uruchomienie usług zapewniających cyberbezpieczeństwo w JST oraz zgodność z wymogami ustawowymi w tym zakresie. Usługa ma za zadanie przejęcie odpowiedzialności za cyberbezpieczeństwo w JST w trybie bieżącym, w okresie oczekiwania na uzyskanie dofinansowania i wdrożenie rozwiązań docelowych. Usługa pomostowa może zostać ujęta w finansowaniu Programu Cyberbezpieczny Samorząd.

Dlatego biorąc pod uwagę powyższe, oraz uzasadniony społecznie - interes pro publico bono, wnosimy:
Osnowa Wniosku:

§1) Na mocy art. 61 Konstytucji RP, w trybie art. 6 ust. 1 pkt. 1 lit a Ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) (" Udostępnieniu podlega informacja (...) zamierzeniach działań władzy ustawodawczej oraz wykonawczej") - wnosimy o udzielenie informacji publicznej **czy Adresat (JST) - ma w planach złożenie stosownego wniosku związanego z wyżej wzmiankowanym programem „Cyberbezpieczny Samorząd” ?**

Prosimy, aby załączone materiały zadekretować zgodnie z §6 ust. 2 pkt. 2 załącznika nr 1 do Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, (...) (Dz. U. z dnia 20 stycznia 2011 r.) - jako propozycje mogące przyczynić się do poszerzenia opcji zapewniających zwiększenie zakresu możliwości - wyboru najkorzystniejszej dla Urzędu opcji.

Oprócz wyżej powołanych proceduralnych podstaw prawnych - prosimy potraktować niniejszy wniosek w kontekście art 241 Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego t.j. Dz. U. z 2023 r. poz. 775) Jesteśmy przekonani, że zarówno załączniki jak i treść wniosku koresponduje z jego brzmieniem - scilicet: "Przedmiotem wniosku mogą być w szczególności sprawy ulepszenia organizacji, wzmocnienia praworządności, usprawnienia pracy i zapobiegania nadużyciom, ochrony własności, lepszego zaspokajania potrzeb ludności."

§2) Wnosimy o zwrotne potwierdzenie otrzymania niniejszego wniosku w trybie §7 Rozporządzenia Prezesa Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania s. i wniosków. (Dz. U. z dnia 22 stycznia 2002 r. Nr 5, poz. 46) - na adres CKC@rig.katowice.pl

§3) Wnosimy o to, aby odpowiedź w przedmiocie powyższych pytań złożonych na mocy art. 63 Konstytucji RP - w związku z art. 241 KPA, została udzielona - zwrotnie na adres CKC@rig.katowice.pl

Z poważaniem


**Centrum Kompetencji Cyberbezpieczeństwa
REGIONALNA IZBA GOSPODARCZA
W KATOWICACH**

Partnerzy Merytoryczni:
Polskie Towarzystwo Informatyczne
Szulc-Efekt sp zoo KRS: 0000059459