



# Minister Rozwoju i Technologii

BM.WSKN.161.159.2023  
Warszawa, 11 grudnia 2023 r.

Pan  
Adam Szulc

Szanowny Panie,

odpowiadając na Pana petycję<sup>1</sup> przekazaną według właściwości przez Kancelarię Prezesa Rady Ministrów<sup>2</sup>, w sprawie wdrożenia w jednostkach samorządu terytorialnego przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555<sup>3</sup>, uprzejmie informuję, że postulat zawarty w petycji należy uznać za zasadny. Wszystkie podmioty objęte zakresem dyrektywy NIS2 powinny podjąć działania służące dostosowaniu się do nowych obowiązków. W tym zakresie w Ministerstwie Cyfryzacji trwają prace nad implementacją ww. dyrektywy do polskiego porządku prawnego.

Należy zauważyć, że jednostki samorządu terytorialnego (dalej - JST), są częścią krajowego systemu cyberbezpieczeństwa już od początku jego istnienia, mimo że implementowana wtedy dyrektywa NIS<sup>4</sup> tego nie wymagała. W związku z tym obowiązki w zakresie cyberbezpieczeństwa np. obsługa incydentów czy ich zgłaszanie nie są dla tych podmiotów czymś nowym.

Prowadzony jest też szereg działań mających na celu wsparcie tych jednostek w zapewnianiu cyberbezpieczeństwa swoich systemów. W 2023 r. w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym (dalej - NASK – PIB) powołano Fundusz Wsparcia Jednostek Samorządu Terytorialnego. Środki Funduszu przeznacza się, na podstawie umowy zawartej z NASK-PIB, na realizację przez JST zadań z zakresu cyberbezpieczeństwa. Podstawowym warunkiem uzyskania wsparcia z Funduszu jest wystąpienie w danej JST lub jej jednostce organizacyjnej incydentu w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa i zgłoszenie go do właściwego CSIRT<sup>5</sup>. Kolejny krok, to analiza przeprowadzana przez ekspertów CSIRT NASK. Jeśli po jej przeprowadzeniu wydane zostaną stosowne rekomendacje, zgłaszającej JST może zostać udzielone wsparcie. Można je przeznaczyć wyłącznie na ograniczenie skutków zaistniałego incydentu i wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na kolejne incydenty. Decyzja w sprawie udzielenia bądź

<sup>1</sup> wpływ do MC - 16.10.2023 r.

<sup>2</sup> pismo KPRM z 16.10.2023 r. znak: DSO.ZAN.161.1796.2023.

<sup>3</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) (tzw. dyrektywa NIS2) nr 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terenie Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

<sup>4</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) nr 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz.UE.L 2016 Nr 194, str. 1).

<sup>5</sup> Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego - <https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt>