Sekretarz Miasta Szczecin
Ryszard Sloka
pl. Armii Krajowej 1, 70-456 Szczecin
tel. + 48 91 425 280
rsloka@um.szczecin.pl • www.szczecin.eu

Szczecin 27.04. 2026 r.

Pan Dariusz Smoliński
Radny Rady Miasta Szczecin

Znak: BPM.0003.57.2026.IŁ
Dotyczy: interpelacji nr 1865

W odpowiedzi na interpelację nr 1865 informuję, że w przypadku przetwarzania danych mieszkańców Szczecina w systemach informatycznych Samodzielnego Publicznego Wojewódzkiego Szpitala Zespolonego przy ul. Arkońskiej – co, jak należy przyjąć, miało miejsce – oraz ich ewentualnego skopiowania przez osoby nieuprawnione, istnieje wysokie prawdopodobieństwo, że dane te mogą zostać wykorzystane lub wprowadzone do obrotu, w tym sprzedane. Urząd Miasta Szczecin nie posiada informacji dotyczących zakresu, rodzaju ani liczby danych osobowych, które mogły zostać pozyskane w wyniku incydentu naruszenia bezpieczeństwa systemów informatycznych wskazanego podmiotu. W związku z tym nie ma możliwości przekazywania osobom trzecim szczegółowych informacji o zdarzeniu. Zgodnie z obowiązującymi przepisami obowiązek informacyjny w tym zakresie spoczywa na administratorze danych osobowych podmiotu, w którym doszło do incydentu.
Należy podkreślić, że Samodzielny Publiczny Wojewódzki Szpital Zespolony przy ul. Arkońskiej nie jest jednostką organizacyjną Gminy Miasto Szczecin, lecz podlega Samorządowi Województwa Zachodniopomorskiego. Gmina Miasto Szczecin nie ma dostępu do baz danych tej placówki ani wiedzy o tym, którzy mieszkańcy byli jej pacjentami. Urząd Miasta Szczecin nie dysponuje również informacjami o działaniach podejmowanych przez inne podmioty w ramach ich systemów bezpieczeństwa. Zgodnie z obowiązującymi regulacjami kwestie wdrażania i utrzymania systemów cyberbezpieczeństwa pozostają w gestii każdego administratora danych.
W ramach działań prewencyjnych Urząd Miasta Szczecin regularnie organizuje szkolenia z zakresu bezpieczeństwa informacji i systemów informatycznych dla pracowników oraz szkolenia specjalistyczne dla pracowników IT miejskich instytucji. Obecnie nie funkcjonuje jednak jednolity, miejski plan reagowania na incydenty cyberbezpieczeństwa obejmujący wszystkie jednostki organizacyjne gminy. Każda z nich jest zobowiązana do wdrożenia, w ramach własnego systemu zarządzania bezpieczeństwem informacji, procedur zarządzania incydentami, planów reagowania oraz prowadzenia rejestrów incydentów.
Audytorzy wewnętrzni Wydziału Kontroli i Audytu Wewnętrznego Urzędu Miasta Szczecin prowadzą audyty w jednostkach organizacyjnych gminy oraz w urzędzie w zakresie bezpieczeństwa informacji, koncentrując się na aspektach proceduralnych, organizacyjnych i systemowych. W latach 2022–2025 przeprowadzono łącznie piętnaście takich audytów. Pracownicy WKiAW nie posiadają jednak kwalifikacji do przeprowadzania analiz technicznych infrastruktury informatycznej, takich jak ocena zabezpieczeń sieciowych czy analiza podatności systemów.
W gminie nie funkcjonuje wyspecjalizowana jednostka posiadająca kompetencje i uprawnienia do centralnego zarządzania cyberbezpieczeństwem wszystkich jednostek podległych, która mogłaby zapewnić spójne standardy w tym zakresie. Rozwiązaniem systemowym mogłoby być

utworzenie Centrum Usług Informatycznych odpowiedzialnego za kompleksową i bezpieczną informatyzację jednostek gminnych.
Jednocześnie w Urzędzie Miasta Szczecin obowiązuje instrukcja postępowania z incydentami bezpieczeństwa oraz naruszeniami ochrony danych osobowych, regulująca proces obsługi incydentów i aktualizowana w razie potrzeby.