



Zastępca Prezydenta Miasta Szczecin

Łukasz Kadłubowski

pl. Armii Krajowej 1,

70-456 Szczecin;

tel. +4891 42 45209, fax +4891 4245207

lkadlubowski@um.szczecin.pl; www.szczecin.eu

Szczecin, dnia ²⁸11.2025 r.

**Stanisław Kaup
Radny Rady Miasta
Szczecin**

w miejscu

Nasz znak: BPS-S.0003.2.2025.MŁ

Dotyczy: interpelacji nr 1638

Szanowny Panie Radny,

w odpowiedzi na interpelację nr 1638 z dnia 07 listopada 2025 roku dotyczącą zabezpieczenia systemu informatycznego głosowania na projekty Budżetu Obywatelskiego w Szczecinie, poniżej przesyłam odpowiedzi na zadane pytania:

1. Władze miasta wraz z firmą MediaPark, która realizuje zamówienie systemu do głosowania wdrożyły wielopoziomowe mechanizmy weryfikacji tożsamości oraz rozwiązania techniczne i organizacyjne zapobiegające automatycznemu głosowaniu oraz wykorzystaniu cudzych danych osobowych. System posiada wielopoziomowe zabezpieczenia, które skutecznie eliminują możliwość nadużyć.
System głosowania w Szczecinie w edycji Budżetu Obywatelskiego 2026 charakteryzuje się zaawansowanymi zabezpieczeniami, łączącymi technologie i procedury rekomendowane przez Wydział Informatyki Urzędu Miasta Szczecin oraz dostawcę systemu, firmę MediaPark.
2. System działa na bazie bezpiecznej infrastruktury, utrzymywanej w certyfikowanym centrum danych home.pl, z całodobową ochroną i monitoringiem. Cała komunikacja z systemem jest szyfrowana certyfikatem SSL, a aplikacja przeszła audyt bezpieczeństwa OWASP Top10 z maksymalnym wynikiem. Stosowane są również zaawansowane firewalle i systemy zapobiegania włamaniom IDS/IPS.

Kluczowe elementy zabezpieczeń to:

- **Bezpieczna infrastruktura**

System jest utrzymywany w certyfikowanym centrum danych home.pl na terenie Polski, z całodobową ochroną fizyczną i monitoringiem.

- **Szyfrowanie komunikacji i danych**

Cała komunikacja z systemem głosowania jest szyfrowana przy użyciu protokołu TLS 1.3. Dane przechowywane w systemie również są zabezpieczone poprzez szyfrowanie.

- **Mechanizmy weryfikacji tożsamości**

Wprowadzone zostały wielopoziomowe mechanizmy potwierdzania tożsamości użytkowników, w tym potwierdzenie głosu za pomocą jednorazowego kodu SMS i weryfikacja numeru PESEL (kontrola poprawności oraz wykrywanie duplikatów).

- **Zaawansowane mechanizmy antybotowe i przeciwdziałanie manipulacjom**

ograniczenia liczby prób, monitoring nietypowych zachowań, a także logi audytowe, które rejestrują wszystkie działania w systemie.

- **Audyt i certyfikacja bezpieczeństwa**

System przeszedł audyt bezpieczeństwa OWASP Top10 z wynikiem 10/10.

Ochrona danych osobowych zgodna z wymogami RODO

Dane mieszkańców są minimalizowane (przetwarzanie wyłącznie takich danych, które są niezbędne do zidentyfikowania, że głos oddają jedynie osoby do tego uprawnione), a dostęp do nich mają tylko uprawnione osoby, posiadające pisemne upoważnienie oraz przeszkolenie do przetwarzania danych osobowych.

W ramach tworzenia nowych zasad głosowania w SBO, od podstaw zaprojektowano ten proces z uwzględnieniem wymagań dotyczących ochrony danych osobowych, z zastosowaniem zasad *privacy by design* i *privacy by default*.

Każdy rodzaj przetwarzania danych osobowych w procesie głosowania w SBO podlega szczegółowym wewnętrznym regulacjom Urzędu Miasta Szczecin w zakresie bezpieczeństwa informacji i ochrony danych osobowych, zapisanym w Polityce Bezpieczeństwa Informacji Urzędu Miasta Szczecin. Zapisy Polityki oraz jej stosowanie są na bieżąco monitorowane, poddawane przeglądowi i aktualizowane w celu zminimalizowania ryzyka naruszenia praw i wolności osób fizycznych, których dane dotyczą.

- **Ciągłość działania i dostępność**

Zapewnione zostały wysokie standardy dostępności systemu (w tym zgodność z WCAG) oraz regularne, szyfrowane kopie zapasowe i plany ciągłości działania.

- **Monitoring, analiza i reagowanie na zagrożenia**

System rejestruje szczegółowe dane o głosach oraz aktywności użytkowników, co pozwala na szybką identyfikację i reakcję na ewentualne próby nadużyć. W razie wykrycia

nieprawidłowości możliwe jest unieważnienie błędnych głosów i przeliczenie wyników lub też powtórzenie głosowania.

3. Każdy głosujący musi potwierdzić swoją tożsamość za pomocą SMS-a, co skutecznie blokuje masowe i automatyczne oddawanie głosów przez boty. Dodatkowo przeprowadzana jest walidacja numeru PESEL, a system monitoruje podejrzane zachowania (np. nietypową liczbę głosów z jednego adresu IP). Dodatkowo osoby niezameldowane na terenie miasta zobowiązane są do złożenia oświadczenia o zamieszkiwaniu na terenie Szczecina, które jest weryfikowane przez Urząd Miasta, co stanowi dodatkowe zabezpieczenie przeciwdziałające głosom nieuprawnionym. Po zakończeniu głosowania dane głosujących zostaną zweryfikowane w oparciu o bazę ewidencji ludności, co znacznie eliminuje ryzyko oddania głosu przez osoby nieuprawnione.
4. System głosowania na projekty SBO 2026 został odpowiednio zabezpieczony przed możliwością nadużyć, takich jak automatyczne oddawanie głosów, poprzez zastosowanie następujących mechanizmów:
 - Weryfikacja głosującego odbywa się za pomocą jednorazowego kodu SMS, który potwierdza tożsamość użytkownika i uniemożliwia wielokrotne oddanie głosu przez tę samą osobę.
 - System wykonuje walidację numeru PESEL, sprawdzając poprawność składni oraz sumę kontrolną, oraz porównuje dane osobowe z ich zaszyfrowaną reprezentacją (hash z tajnym hasłem), aby wykrywać duplikaty i nadużycia.
 - System posiada wysokiej klasy zabezpieczenia techniczne, w tym szyfrowanie transmisji TLS 1.3 oraz szyfrowanie danych w spoczynku, a także nieedytowalne logi audytowe i zasady minimalnych uprawnień dla administratorów.
 - Całość infrastruktury działającej systemu jest utrzymywana w certyfikowanym centrum danych z całodobową ochroną fizyczną i monitoringiem.
 - Wszystkie działania w systemie są monitorowane i rejestrowane, co umożliwia wykrywanie i szybką reakcję na próby manipulacji systemem oraz ewentualne unieważnianie fałszywych głosów.

Dzięki tym kompleksowym zabezpieczeniom system głosowania na projekty SBO 2026 w Szczecinie zapewnia ochronę przed nadużyciami i gwarantuje uczciwość oraz rzetelność procesu wyboru projektów.

5. System przeszedł audyt bezpieczeństwa OWASP Top 10, uzyskując wynik 10/10. Specjalistyczne testy penetracyjne i audyty zewnętrzne gwarantują odporność systemu na manipulacje. Dostawca posiada międzynarodowy certyfikat ISO/IEC 27001:2023-08, potwierdzający wdrożenie i utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Certyfikacja gwarantuje, że wszystkie procesy związane z przetwarzaniem danych osobowych są realizowane zgodnie z najwyższymi standardami bezpieczeństwa.
6. Dane mieszkańców są chronione zgodnie z RODO oraz wewnętrzną Polityką Bezpieczeństwa Informacji Urzędu Miasta Szczecin, stosowana jest minimalizacja danych. Po zakończeniu głosowania i weryfikacji dane są anonimizowane, co oznacza, że nie jest możliwe ich bezpośrednie ani pośrednie powiązanie z osobami fizycznymi (identyfikacja). System stosuje mechanizmy weryfikacji tożsamości, takie jak potwierdzenie głosu jednorazowym kodem SMS oraz walidację numeru PESEL, co zabezpiecza przed wielokrotnym głosowaniem czy wykorzystaniem cudzych danych. Dostęp do danych i panelu administracyjnego jest ograniczony do wąskiej grupy uprawnionych osób, a wszystkie działania są rejestrowane i podlegają monitoringowi. System przeszedł audyt bezpieczeństwa OWASP Top 10, uzyskując wynik 10/10, co potwierdza wysoki poziom ochrony i bezpieczeństwa danych i samego procesu głosowania. Takie działania gwarantują mieszkańcom świadomość, że ich dane są bezpieczne, a oddane głosy są uczciwie liczone i chronione przed nadużyciami.
7. Przewidziano odpowiednie działania na wypadek wykrycia nieprawidłowości w systemie głosowania SBO 2026, które umożliwiają szybkie podjęcie decyzji o unieważnieniu wyników lub ich weryfikacji. System posiada wielowarstwowy monitoring oraz pełną rejestrację wszystkich operacji, co pozwala na dokładną analizę i wykrycie ewentualnych prób nadużyć. W przypadku stwierdzenia błędów lub prób manipulacji, możliwe jest unieważnienie nieprawidłowych głosów oraz przeliczenie wyników. Ponadto, system umożliwia powtórne głosowanie, jeżeli sytuacja tego wymaga, a ostateczne decyzje w tej sprawie należą do Prezydenta Miasta Szczecin. Wszystkie incydenty związane z zabezpieczeniami są na bieżąco monitorowane i zgłaszane odpowiednim służbom, w tym organom ścigania. Dzięki tym mechanizmom proces głosowania jest zabezpieczony i zapewnia przejrzystość oraz uczciwość wyników.

8. Komunikacja z mieszkańcami na temat bezpieczeństwa i przejrzystości procesu głosowania odbywać się będzie przez stronę internetową SBO, media społecznościowe, email oraz telefon kontaktowy.

9. W przypadku wystąpienia ryzyka naruszenia ochrony danych osobowych Urząd Miasta Szczecin posiada skuteczne i sprawdzone procedury reagowania i minimalizowania ryzyka naruszenia praw i wolności osób, których dane dotyczą.

W razie pytań i wątpliwości związanych z przetwarzaniem danych osobowych w procesie głosowania w SBO do dyspozycji Mieszkańców pozostaje Inspektor Ochrony Danych Urzędu Miasta Szczecin, z którym można się skontaktować pod adresem: iod@um.szczecin.pl

Mamy pełne przekonanie, że przygotowany system gwarantuje przejrzystość i bezpieczeństwo głosowania, dając mieszkańcom Szczecina pewność, że ich głos będzie traktowany poważnie i uczciwie.

2 powtórzenie
ZASTĘPCY PREZYDENTA MIASTA
Lukasz Kadiukowski

