Prezydent Miasta Stołecznego Warszawy
pl. Bankowy 3/5, 00-950 Warszawa, tel. 22 443 10 01, faks 22 443 10 02
sekretariatprezydenta@um.warszawa.pl, um.warszawa.pl

Warszawa, 16 maja 2023 r.

Znak sprawy: KW-ZSS.1712.2.2023.TTR

Pani
Ewa Kolankiewicz
Dyrektorka
Centrum Komunikacji Społecznej
Urzędu m.st. Warszawy

Wystąpienie pokontrolne

Na podstawie § 22 ust. 10 Regulaminu organizacyjnego Urzędu m.st. Warszawy, stanowiącego załącznik do zarządzenia Nr 312/2007 Prezydenta Miasta Stołecznego Warszawy z dnia 4 kwietnia 2007 r. w sprawie nadania regulaminu organizacyjnego Urzędu m.st. Warszawy (z późn. zm.), w związku kontrolą przeprowadzoną przez Biuro Kontroli Urzędu m.st. Warszawy w Centrum Komunikacji Społecznej Urzędu m.st. Warszawy (dalej CKS) w okresie od 11 stycznia 2023 r. do 22 lutego 2023 r. dotyczącej procedury nadawania uprawnień dostępu do systemów informatycznych w latach 2021 – 2022, której wyniki zostały przedstawione w protokole kontroli podpisanym 27 lutego 2023 r., stosownie do § 39 ust. 1 i 2 zarządzenia Nr 1837/2019 Prezydenta Miasta Stołecznego Warszawy z dnia 12 grudnia 2019 r. w sprawie zasad i trybu postępowania kontrolnego (dalej: Zarządzenie), po częściowym uwzględnieniu złożonych zastrzeżeń do Projektu wystąpienia pokontrolnego, przekazuję Pani niniejsze Wystąpienie pokontrolne.

Kontrolą objęto realizację przez CKS w latach 2021 – 2022 Procedury nadawania uprawnień dostępu do Elektronicznego Systemu Obsługi Głosowania – elektronicznego systemu do obsługi budżetu obywatelskiego w m.st. Warszawie (dalej: Procedura ESOG)[1] oraz wybranych zadań wynikających z zarządzenia nr 1879/2019 Prezydenta Miasta Stołecznego Warszawy z dnia 23 grudnia 2019 r. w sprawie polityki bezpieczeństwa i ochrony danych osobowych w Urzędzie m.st. Warszawy (z późn. zm.) – dalej: Polityka bezpieczeństwa.

Zgodnie z Procedurą ESOG z wnioskiem o nadanie dostępu do systemu ESOG dla podległych pracowników mogli wystąpić: Burmistrz Dzielnicy/Dyrektor Biura/Dyrektor Jednostki Organizacyjnej/ Osoba Prawna lub koordynator ds. budżetu obywatelskiego za zgodą burmistrza lub dyrektora (dalej: Wnioskodawca). Do wniosku należało dołączyć skan aktualnego upoważnienia do przetwarzania danych osobowych oraz w przypadku jednostek i osób prawnych skan umowy powierzenia przetwarzania danych osobowych.

W kontrolowanym okresie do CKS wpłynęło 295 wniosków o nadanie uprawnień dostępu do systemu ESOG dla 659 osób.[2] Kontroli poddano realizację 14 wniosków dla 27 użytkowników.[3]

W trakcie kontroli ustalono, iż przed nadaniem uprawnień dostępu do systemu ESOG nie weryfikowano treści dostarczanych upoważnień do przetwarzania danych osobowych, w szczególności w zakresie możliwości realizacji zadań związanych z budżetem obywatelskim.

Pismem z 2 kwietnia 2021 r. p.o. Dyrektora Zakładu Gospodarowania Nieruchomościami w Dzielnicy Bielany m.st. Warszawy (dalej: ZGN) wystąpił do Dyrektorki CKS o wyrażenie zgody na dostęp do systemu ESOG dla 11 pracowników ZGN. Do wniosku dołączono kopię umowy powierzenia przetwarzania danych osobowych (dalej: Porozumienie)[4] oraz kopie upoważnień do przetwarzania danych osobowych pracowników ZGN wskazanych we wniosku. Zgodnie z § 2 ust. 2 Porozumienia, powierzone dane osobowe miały być przetwarzane przez ZGN wyłącznie w celu realizacji procesu budżetu partycypacyjnego (obecnie budżet obywatelski)[5]. Ponadto zgodnie z § 3 ust. 3 Porozumienia, w celu jego realizacji, pracownicy ZGN powinni posiadać stosowne upoważnienia do przetwarzania danych osobowych. Zgodnie z przekazanymi przez ZGN upoważnieniami, pracownicy objęci wnioskiem mogli przetwarzać dane osobowe zawarte w konkretnych zbiorach, tj.: najemcy, windykacja, kontrahenci, wspólnoty mieszkaniowe i zarządcy nieruchomości, kontakt. Wątpliwości co do zgodności treści posiadanych przez pracowników ZGN upoważnień z zapisami Porozumienia, budzi fakt, iż w upoważnieniach tych nie wskazano, iż uprawniają one pracowników ZGN do

---

[1] Procedura ESOG została zatwierdzona przez Dyrektorkę CKS i obowiązuje od maja 2020 r.
[2] W roku 2021 wpłynęło 159 wniosków o nadanie uprawnień dostępu do systemu ESOG dla 373 osób, w roku 2022 wpłynęło 136 wniosków dla 286 osób.
[3] 7 wniosków dla 19 użytkowników z roku 2021 oraz 7 wniosków dla 8 użytkowników z roku 2022.
[4] Porozumienie z 8 maja 2019 r. w sprawie powierzenia ZGN przetwarzania danych osobowych osób mieszkańców m.st. Warszawy uczestniczących w procesie przeprowadzania budżetu partycypacyjnego w m.st. Warszawie
[5] art. 1 pkt 1 lit. b, art. 2 pkt 1 lit. b i art. 3 pkt 1 lit. b ustawy z dnia 11 stycznia 2018 r. o zmianie niektórych ustaw w celu zwiększenia udziału obywateli w procesie wybierania, funkcjonowania i kontrolowania niektórych organów publicznych (Dz. U. z 2018 r. poz. 130)

przetwarzania danych osobowych w procesie realizacji budżetu obywatelskiego. Pomimo tych wątpliwości, nie dokonano weryfikacji przedmiotowych upoważnień i udzielono dostępu do systemu ESOG wszystkim 11 pracownikom ZGN. Zgodnie ze złożonymi wyjaśnieniami, w CKS uznano, że wystarczający w tym zakresie był wskazany w punkcie IV.2 Procedury ESOG obowiązek weryfikacji przez Wnioskodawcę aktualności upoważnień do przetwarzania danych osobowych.

Tymczasem obowiązek weryfikacji zakresu upoważnień do przetwarzania danych osobowych, w przypadku wątpliwości dotyczących np. zgodności ich treści z zapisami porozumień powierzenia przetwarzania danych osobowych lub Procedurą ESOG wynika z Polityki bezpieczeństwa. Zgodnie bowiem z § 14, § 20 i § 23 Polityki bezpieczeństwa, dostęp do systemów informatycznych Urzędu m.st. Warszawy, w których przetwarzane są dane osobowe, mogą mieć wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, przy czym przetwarzanie danych osobowych może odbywać się zgodnie z zakresem upoważnienia, a za nadawanie uprawnień dostępu do tych systemów informatycznych, odpowiadają właściwe biura Urzędu m.st. Warszawy administrujące tymi systemami.

W Procedurze ESOG nie opisano w sposób precyzyjny sposobu cofania (odbierania) uprawnień dostępu do systemu ESOG. Zgodnie z Procedurą ESOG Dyrektor CKS może w dowolnym momencie zmienić zakres uprawnień lub cofnąć zgodę na dostęp użytkownika do systemu ESOG – z własnej inicjatywy lub na wniosek przełożonego pracownika. Z wyjaśnień uzyskanych w trakcie kontroli wynika, iż z wnioskiem o cofnięcie uprawnień mogą występować osoby wskazane w Procedurze ESOG jako Wnioskodawcy. Ponadto podstawą cofnięcia uprawnień dostępu do systemu ESOG może stanowić informacja z Wydziału Ochrony Danych Osobowych Biura Organizacji Urzędu m.st. Warszawy o odebraniu upoważnienia do przetwarzania danych osobowych w związku z np. rozwiązaniem umowy z pracownikiem.

Kontroli poddano realizację wniosków o cofnięcie uprawnień 11 użytkownikom, nie stwierdzając w tym zakresie nieprawidłowości. Natomiast podczas kontroli 14 wniosków o nadanie uprawień dostępu do systemu ESOG stwierdzono, że 2 z nich dotyczyły zmiany koordynatorów systemu ESOG[6], wobec czego były one także wnioskami o cofnięcie uprawnień. Ustalono, iż w 1 przypadku[7], wbrew § 10 ust. 2 oraz § 20 ust. 2 lit c Polityki bezpieczeństwa, nie dokonano stosownego cofnięcia uprawnień.

Zarówno brak zweryfikowania dostarczonych zakresów upoważnień do przetwarzania danych osobowych dla przyszłych użytkowników systemu ESOG, jak również brak cofnięcia koordynatorowi uprawnień dostępu do tego systemu, świadczą o braku przestrzegania standardów kontroli

---

[6] Wniosek w sprawie zmiany koordynatora systemu ESOG w Biurze Zarządzania Ruchem Drogowym Urzędu m.st. Warszawy z 21 stycznia 2022 r. oraz wniosek dotyczący zmiany koordynatora systemu ESOG w Biurze Polityki Zdrowotnej Urzędu m.st. Warszawy z 30 sierpnia 2022 r.

[7] Wniosek o zmianę koordynatora systemu ESOG w Biurze Polityki Zdrowotnej Urzędu m.st. Warszawy.

zarządczej dla sektora finansów publicznych, w tym w szczególności standardu C.13, zobowiązującego do dbania aby dostęp do zasobów jednostki miały wyłącznie upoważnione osoby.[8]

W trakcie kontroli ustalono, iż dopiero 26 stycznia 2022 r., tj. przeszło dwa lata od wejścia w życie Polityki bezpieczeństwa, powołano w CKS Administratora Systemów Informatycznych (dalej: ASI), który odpowiada za sprawność, konserwację, wdrożenie i stosowanie zasad bezpieczeństwa danych w zakresie technicznych zabezpieczeń systemów informatycznych. Z wyjaśnień złożonych w trakcie kontroli wynika, iż wyboru takiego dokonano dopiero na skutek pisemnej interwencji Biura Cyfryzacji Miasta z 9 grudnia 2021 r. Bowiem pismem tym przypomniano, o wynikającej z § 83 ust. 1 Polityki bezpieczeństwa konieczności wyznaczenia pracownika CKS do pełnienia funkcji ASI. Ustalono, iż do momentu powołania ASI, jego czynności były realizowane przez pracowników CKS jedynie w zakresie wynikającym z Procedury ESOG.

Ustalono także, iż wbrew § 10 ust. 3 Polityki bezpieczeństwa w roku 2021 nie dokonano okresowego przeglądu i aktualizacji uprawnień użytkowników do dostępu do systemu ESOG. Przeglądu takiego dokonano 4 stycznia 2022 roku. Jednocześnie zgodnie z § 10 ust. 4 Polityki bezpieczeństwa należało poinformować Dyrektorkę CKS o wynikach takiego przeglądu. Tymczasem przedstawiane Dyrektorce podsumowania weryfikacji użytkowników systemu ESOG zawierały jedynie informacje o podjętych działaniach związanych z przeglądami, a nie o efektach tych przeglądów. W trakcie kontroli oświadczono, iż: „Za 2021 rok w wyniku weryfikacji cofnięto dostępy dla 40 osób, zaś w 2022 roku w wyniku weryfikacji cofnięto 10 uprawnień".

Ponadto wbrew postanowieniom punktu V.2 Procedury ESOG, w prowadzonym w CKS rejestrze osób, które posiadają dostęp do systemu ESOG, nie dla wszystkich użytkowników znajdowała się informacja o okresie obowiązywania dostępu. Z wyjaśnień złożonych w trakcie kontroli wynika, iż niekompletność danych w rejestrze, wynika z faktu, że CKS w listopadzie 2022 r. utracił elektroniczny rejestr, który był prowadzony na koncie jednego z pracowników, zawierający wszystkie wymagane dane. Wobec niepowodzenia próby odzyskania rejestru, podjęto wówczas działania mające na celu jego odtworzenie na podstawie wszystkich zgłoszeń.

Opisany powyżej sposób prowadzenia rejestru, w tym brak jego bieżącej archiwizacji, świadczy o braku przestrzegania standardu C.15 kontroli zarządczej dla sektora finansów publicznych, który nakazuje wprowadzenie mechanizmów zapewniających bezpieczeństwo danych i systemów informatycznych.

Stwierdzono także, iż choć sprawy związane z realizacją Procedury ESOG prowadziło bezpośrednio 3 pracowników CKS, to tylko w jednym przypadku zadania te zostały ujęte w zakresie obowiązków pracownika.

---

[8] Wynikające z komunikatu Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych oraz zarządzenie Nr 1613/2011 Prezydenta Miasta Stołecznego Warszawy z dnia 11 października 2011 r. w sprawie zasad funkcjonowania kontroli zarządczej w m.st. Warszawie (z późn. zm.)

Sytuacja ta świadczy o braku przestrzegania standardu A.4 kontroli zarządczej dla sektora finansów publicznych, który nakazuje precyzyjne określenie zakresu uprawnień delegowanych poszczególnym pracownikom.

Wskazane powyżej nieprawidłowości i uchybienia stwierdzone w badanych obszarach, tj.:

- brak weryfikowania dostarczanych zakresów upoważnień do przetwarzania danych osobowych, w szczególności w zakresie możliwości realizacji zadań związanych z budżetem obywatelskim;
- w 1 przypadku brak cofnięcia uprawnień dostępu do systemu ESOG pomimo stosownego wniosku;
- powołanie ASI przeszło dwa lata od wejścia w życie Polityki bezpieczeństwa;
- nie dokonanie w roku 2021 okresowego przeglądu i aktualizacji uprawnień użytkowników do dostępu do systemu ESOG;
- brak informowania Dyrektorki CKS o wynikach (efektach) okresowych przeglądów i aktualizacji uprawnień użytkowników do dostępu do systemu ESOG;
- brak stosownych zapisów w zakresach obowiązków 3 pracowników realizujących zadania związane z Procedurą ESOG;

dają podstawę do pozytywnej z zastrzeżeniami oceny działalności CKS w zakresie objętym niniejszą kontrolą.[9]

Przedstawiając powyższe ustalenia i oceny zalecam:

1. Przed wyrażeniem zgody na dostęp do systemu ESOG weryfikowanie zakresów upoważnień do przetwarzania danych osobowych, w szczególności w przypadkach wątpliwości co do zgodności ich treści z zapisami porozumień/umów powierzenia przetwarzania danych osobowych.

2. Dokonywanie przeglądów i aktualizacji uprawnień dostępu do systemu ESOG w terminach wskazanych w Polityce bezpieczeństwa.

3. Zapewnienie rzetelnego informowania Dyrektora CKS o wynikach przeprowadzonych przeglądów i aktualizacji uprawnień dostępu do systemu ESOG.

4. Realizowanie wniosków o dostęp do systemu ESOG zgodnie z ich treścią, w szczególności w przypadku wniosków dotyczących zmiany koordynatorów systemu ESOG.

5. Uzupełnienie opisów stanowisk pracowników realizujących zadania związane z Procedurą ESOG o zapisy związane z tymi zadaniami.

Na podstawie § 22 ust. 10 Regulaminu organizacyjnego oraz § 41 ust. 1 Zarządzenia oczekuję od Pani Dyrektor, w terminie nie dłuższym niż 30 dni od daty doręczenia niniejszego Wystąpienia pokontrolnego, informacji o sposobie realizacji zaleceń pokontrolnych i wykorzystaniu uwag zawartych w Wystąpieniu pokontrolnym lub przyczynach braku realizacji zaleceń pokontrolnych lub

[9] Do oceny działań CKS w obszarze objętym kontrolą zastosowano skalę: ocena pozytywna, ocena pozytywna z zastrzeżeniami, ocena negatywna.

niewykorzystaniu uwag bądź o innym sposobie usunięcia stwierdzonych nieprawidłowości lub uchybień.

Na podstawie § 41 ust. 1 Zarządzenia zobowiązuję Panią Dyrektor do przekazania kopii ww. informacji Dyrektorowi Biura Kontroli.

PREZYDENT
MIASTA STOŁECZNEGO WARSZAWY
Rafał Trzaskowski