



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, 30 listopada 2023 r.

Znak sprawy: KW-ZSS.1712.29.2023.TTR

**Pan
Maciej Iwanicki
Burmistrz Dzielnicy Rembertów
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 Urzędzie Dzielnicy Rembertów m.st. Warszawy (dalej UD Rembertów) w okresie od 22 maja 2023 r. do 29 czerwca 2023 r. dotyczącej procedury nadawania uprawnień dostępu do systemów informatycznych w latach 2021 – 2022, której wyniki zostały przedstawione w protokole kontroli podpisanym 6 lipca 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), przekazuję Panu niniejsze Wystąpienie pokontrolne.

Kontrolą objęto nadawanie, przedłużanie i odbieranie przez UD Rembertów w latach 2021 – 2022 uprawnień dostępu do systemów informatycznych, w których przetwarzane są dane osobowe i których właścicielem biznesowym był UD Rembertów (dalej: SI)¹ oraz realizację 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 i Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie m.st. Warszawy² – dalej: Instrukcja Zarządzania SI.

W UD Rembertów uprawnienia dostępowe do korzystania do 27 SI nadawane są przez pracowników Wydziału Informatyki dla Dzielnicy Rembertów (dalej: WIN)³. Dostęp do nich możliwy jest jedynie dla pracowników UD Rembertów po wcześniejszym zalogowaniu do domeny Urzędu m.st. Warszawy.⁴

W UD Rembertów nie opracowano i nie wdrożono procedur określających sposób postępowania przy nadawaniu, przedłużaniu lub odbieraniu uprawnień dostępu do SI.

W trakcie kontroli ustalono, iż wbrew postanowieniom pkt V.2 Instrukcji zarządzania SI, przed nadaniem uprawnień dostępu do SI nie była uzyskiwana zgoda Burmistrza na ich przyznanie.⁵ Zgodnie z przyjętą w UD Rembertów praktyką, uprawnienia dostępu do SI nadawano (przedłużano lub odbierano) na podstawie informacji o upoważnieniach do przetwarzania danych osobowych pracowników UD Rembertów przekazywanych przez Wydział Ochrony Danych Osobowych Biura Organizacji Urzędu m.st. Warszawa (dalej: WODO), informacji o zmianach kadrowych w UD Rembertów przekazywanych przez Zespół Kadr dla Dzielnicy Rembertów (dalej: ZK) albo wniosku bezpośredniego przełożonego pracownika, którego postępowanie dotyczyło.

¹ Właściciel biznesowy - komórka lub jednostka uprawniona do kierowania warstwą biznesową SI, w tym zwłaszcza: określania uzasadnienia biznesowego powstania i utrzymania systemu – określania wymagań biznesowych dla systemu – określania i potwierdzania zmian jakich system wymaga. W UD Wilanów nie dokonywano zmiany zakresu nadanych uprawnień dostępu do SI.

² Zgodnie z § 21 Polityki bezpieczeństwa dyrektor biura właściwego do spraw bezpieczeństwa teleinformatycznego w porozumieniu z dyrektorem biura właściwego do spraw cyfryzacji oraz dyrektorem biura właściwego do spraw ochrony danych osobowych, określa Instrukcję zarządzania SI. Instrukcja zarządzania SI została wprowadzona 4 stycznia 2021 r. Od 23 listopada 2021 r. do dnia zakończenia kontroli obowiązywała Instrukcja zarządzania SI w wersji 1.1.

³ Vide: § 19 pkt 2 i 4 Zarządzenia Nr 1201/2022 Prezydenta Miasta Stołecznego Warszawy z 20 lipca 2020 r. w sprawie nadania wewnętrznego regulaminu organizacyjnego Urzędu Dzielnicy Rembertów Miasta Stołecznego Warszawy w Urzędzie Miasta Stołecznego Warszawy i § 17 pkt 1 lit. e i pkt 2 lit. l Zarządzenia Nr 1158/2016 Prezydenta Miasta Stołecznego Warszawy z dnia 29 lipca 2016 r. w sprawie nadania wewnętrznego regulaminu organizacyjnego Urzędu Dzielnicy Rembertów Miasta Stołecznego Warszawy w Urzędzie Miasta Stołecznego Warszawy (z późn. zm.). W UD Rembertów nie dokonywano zmian zakresu nadanych uprawnień dostępu do SI.

⁴ Dostęp do systemu Dodatki Mieszkaniowe i systemu monitoringu wymaga dodatkowego logowania.

⁵ Administrujący, tj. Burmistrz Dzielnicy Rembertów posiada upoważnienie (znak: GP-OR.0052.727.2022, do wykonywania w imieniu Administratora (Prezydent m.st. Warszawy) czynności w zakresie bezpieczeństwa i ochrony danych osobowych, w tym do udostępniania danych osobowych. Powyższe upoważnienie nie upoważnia do udzielania dalszych upoważnień. Poprzednia Pani Burmistrz również posiadała w tym zakresie stosowne upoważnienie (znak: GP-OR.0052.6322.2018).

W okresie objętym kontrolą funkcję Administratorów Systemów Informatycznych, dalej: ASI⁶ pełniło 3 pracowników WIN, którzy zostali wyznaczeni przez Burmistrza Dzielnicy Rembertów przed wejściem w życie Instrukcji zarządzania SI.

Zgodnie z § 10 ust. 3 i 4 Polityki bezpieczeństwa, do obowiązków ASI należy dokonywanie raz w roku okresowego przeglądu i aktualizacji uprawnień użytkowników do dostępu do SI, a o wynikach takiego przeglądu powinien zostać poinformowany Burmistrz Dzielnicy Rembertów. Ponadto zgodnie Instrukcją zarządzania SI, informacja o obowiązkach realizacji wskazanych powyżej zadań powinna znaleźć się w dokumencie wyznaczającym ASI.⁷ Ustalenia kontroli wskazują, iż w UD Rembertów nie dokonywano okresowych przeglądów i aktualizacji uprawnień.

Wskazane powyżej nieprawidłowości dotyczące pominięcia w procesie nadawania uprawnień dostępu do SI osób uprawnionych do podejmowania decyzji o przyznaniu takich uprawnień, a także brak dokonywania raz w roku okresowego przeglądu i aktualizacji uprawnień użytkowników do dostępu do SI mogą świadczyć o naruszeniu standardów C.14 i C.15 kontroli zarządczej dla sektora finansów publicznych, które zobowiązują do zadbania, aby dostęp do zasobów jednostki miały wyłącznie upoważnione osoby oraz nakazują przestrzeganie określonych mechanizmów służących zapewnieniu bezpieczeństwa danych i systemów informatycznych.⁸

Zgodnie z pkt V.8 Instrukcji zarządzania SI właściciel biznesowy zobowiązany jest do prowadzenia bieżącej ewidencji nadanych uprawnień do systemu (dalej: Ewidencja). Udostępniona w trakcie kontroli Ewidencja (arkusz kalkulacyjny MS Excel) nie zawierała informacji o 10 zmianach dotyczących kont użytkowników, tj. nadaniu lub odebraniu możliwości korzystania przez użytkowników z SI, wynikających z wiadomości otrzymanych z WODO. Zgodnie z wyjaśnieniami uzyskanymi w trakcie kontroli braki powstały w trakcie generowania Ewidencji z systemu AD (Active Directory). Ponadto w Ewidencji nie określono jaki zakres dostępu do SI posiadał każdy użytkownik.⁹

Zgodnie z Ewidencją, w latach 2021-2022 dostęp do SI (w których przetwarzane były dane osobowe i których właścicielem biznesowym był UD Rembertów, w tym system służący do zarządzania systemem wydruku) nadano 11 użytkownikom, a 7 odebrano takie uprawnienia. W wyniku kontroli wszystkich powyższych spraw ustalono, iż WIN w 15 przypadkach nadania lub odebrania uprawnień

⁶ ASI – pracownik Urzędu m.st. Warszawy odpowiedzialny za sprawność, konserwację, wdrożenie i stosowanie zasad bezpieczeństwa danych w zakresie technicznych zabezpieczeń systemów informatycznych. Zgodnie z § 83 ust. 1 Polityki bezpieczeństwa – Administrujący, zarządzający systemem informatycznym, w którym przetwarzane są dane osobowe, wyznacza ASI.

⁷ Udostępnione dokumenty potwierdzające wyznaczenie ASI nie zawierają takich zapisów.

⁸ Komunikat 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.).

⁹ Zgodnie z Instrukcją zarządzania SI (rozdział V pkt. 5) zakres dostępu do SI może być: podstawowy (wprowadzanie do SI danych, ich modyfikacji lub usuwanie) albo rozszerzony (administracyjny/uprzywilejowany – przeznaczony dla ASI).

dysponuje wiadomościami WODO lub wnioskami bezpośrednich przełożonych, a w 3 kolejnych przypadkach bezpośredni przełożeni potwierdzili, iż występowali z takimi wnioskami do WIN.

W trakcie kontroli ustalono także, iż w przypadkach, w których uległy zmianie okoliczności, mające wpływ na zasadność nadanych użytkownikowi uprawnień dostępu do SI (np. w przypadku odejścia pracownika z pracy lub zamiana zakresu obowiązków pracownika wynikająca z przejścia do innej wewnętrznej komórki organizacyjnej) przełożeni pracowników UD Rembertów, wbrew obowiązkowi wynikającemu z pkt V.10 Instrukcji zarządzania SI, nie informowali WIN o takim fakcie. W związku z powyższym, zmiany uprawnień dostępu do SI dokonywano z opóźnieniem, które maksymalnie wyniosło 2 miesiące.¹⁰

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

- brak uzyskiwania przed nadaniem uprawnień dostępu do SI stosownej zgody osób uprawnionych do podejmowania decyzji o przyznaniu takich uprawnień,
- brak zapisów w dokumentach powołujących ASI zapisów wskazanych w Instrukcji zarządzania SI,
- brak dokonywania okresowych przeglądów i aktualizacji uprawnień użytkowników do dostępu do SI;
- brak w Ewidencji informacji o zakresach nadanych uprawnień oraz o 10 zmianach dotyczących kont użytkowników,
- nieinformowanie ASI o zmianie okoliczności, mających wpływ na zasadność nadanych uprawnień dostępu do SI,

dają podstawę do pozytywnej z zastrzeżeniami oceny działalności UD Rembertów w zakresie objętym niniejszą kontrolą.¹¹

Przedstawiając powyższe ustalenia i oceny zalecam:

1. Opracowanie i wdrożenie procedury nadawania, przedłużania i odbierania uprawnień dostępu do SI.
2. Powołanie ASI w sposób zgodny z Instrukcją zarządzania SI.
3. Dokonywanie przeglądów i aktualizacji uprawnień dostępu do SI w terminach wskazanych w Polityce bezpieczeństwa.
4. Nadzorować ASI w zakresie realizacji obowiązku rzetelnego informowania o wynikach przeprowadzonych przeglądów i aktualizacji uprawnień dostępu do SI.

¹⁰ W przypadku odejścia z pracy w UD Rembertów jednego z pracowników Wydziału Infrastruktury. W trzech przypadkach zmiany wewnętrznej komórki organizacyjnej UD Rembertów, opóźnienia te wynosiły od 2 do 10 dni.

¹¹ Do oceny działań UD Rembertów w obszarze objętym kontrolą zastosowano skalę: ocena pozytywna, ocena pozytywna z zastrzeżeniami, ocena negatywna.

5. Uzupelnienie Ewidencji poprzez okrešlenie, zgodnie z Instrukcj zarzdzania SI, zakresów dostępu.

Na podstawie § 22 ust. 10 Regulaminu organizacyjnego oraz § 41 ust. 1 Zarzdzenia oczekuję od Pana Burmistrza, w terminie nie dłuŹszym niŹ 30 dni od daty doręczenia niniejszego Wystpienia pokontrolnego, informacji o sposobie realizacji zaleceń pokontrolnych i wykorzystaniu uwag zawartych w Wystpieniu pokontrolnym lub przyczynach braku realizacji zaleceń pokontrolnych lub niewykorzystaniu uwag bdŹ o innym sposobie usunięcia stwierdzonych nieprawidłowości lub uchybień.

Na podstawie § 41 ust. 1 Zarzdzenia zobowizuję Pana Burmistrza do przekazania kopii ww. informacji Dyrektorowi Biura Kontroli.

PREZYDENT
MIASTA STOŁECZNEGO WARSZAWY

Rafał Trzaskowski

