



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.1712.70.2023.TTR

**Pan
Ludwik Rakowski
Burmistrz Dzielnicy Wilanów
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 Wilanów m.st. Warszawy (dalej UD Wilanów) w okresie od 22 sierpnia 2023 r. do 25 września 2023 r. dotyczącej procedury nadawania uprawnień dostępu do systemów informatycznych w latach 2021 – 2022, której wyniki zostały przedstawione w protokole kontroli podpisanym 26 września 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 Wilanów w latach 2021 – 2022 uprawnień dostępu do systemów informatycznych, w których przetwarzane są dane osobowe i których właścicielem biznesowym był UD Wilanów (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 Wilanów nadawane są uprawnienia dostępowe do korzystania do 22 SI. Dostęp do nich możliwy jest jedynie dla zalogowanych użytkowników domeny Urzędu m.st. Warszawy.³ Pracownicy Wydziału Informatyki dla Dzielnicy Wilanów (dalej: WIN)⁴ nadają, przedłużają i odbierają pracownikom UD Wilanów uprawnienia dostępu do 20 SI⁵ oraz pracownikom Centrum Obsługi Podatnika Urzędu m.st. Warszawy (dalej: COP) w zakresie dostępu do systemów z Pakietu Info-System.

W UD Wilanów 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 jest uzyskiwana zgoda Burmistrza lub Zastępców Burmistrza na ich przyznanie.⁶ Zgodnie z przyjętą w UD Wilanów praktyką, uprawnienia dostępu do SI nadawano (przedłużano lub odbierano) na podstawie informacji o upoważnieniach do przetwarzania danych osobowych pracowników UD Wilanów przekazywanych przez Wydział Ochrony Danych Osobowych Biura Organizacji Urzędu m.st. Warszawa (dalej: WODO), informacji o zmianach kadrowych w UD

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 Dostęp do WinDOM, Sygnity oraz monitoringu wizyjnego wymaga dodatkowego logowania.

⁴ Vide: § 17 pkt 2 i 4 Zarządzenia Nr 1488/2017 Prezydenta Miasta Stołecznego Warszawy z 1 września 2017 r. w sprawie nadania wewnętrznego regulaminu organizacyjnego Urzędu Dzielnicy Wilanów Miasta Stołecznego Warszawy w Urzędzie Miasta Stołecznego Warszawy (z późn. zm.).

⁵ Sprawy związane z dostępem do monitoringu wizyjnego i kontroli dostępu realizuje Wydział Administracyjno-Gospodarczy dla Dzielnicy Wilanów.

⁶ Administrujący, tj. Burmistrz Dzielnicy Wilanów oraz Zastępcy Burmistrza posiadają upoważnienia (znak: GP-OR.0052.5411.2018, GP-OR.0052.5433.2018 i GP-OR.0052.5432.2018 z 20 grudnia 2018 r.) do wykonywania w imieniu Administratora (Prezydent m.st. Warszawy) czynności w zakresie bezpieczeństwa i ochrony danych osobowych, w tym do udostępniania danych osobowych. Powyższe upoważnienia nie upoważniają do udzielania dalszych upoważnień.

Wilanów przekazywanych przez Wydział Organizacyjny dla Dzielnicy Wilanów (dalej: WO) albo wniosku bezpośredniego przełożonego pracownika, którego postępowanie dotyczyło.

W okresie objętym kontrolą funkcję Administratorów Systemów Informatycznych (dalej: ASI⁷) pełniło 4 pracowników WIN. Jednak żaden z nich nie został wyznaczony w sposób zgodny z trybem określonym w Instrukcji zarządzania SI.⁸ W przypadku 3 z 4 pracowników WIN, którzy zgodnie z wyjaśnieniami Zastępcy Burmistrza, pełnili w UD Wilanów funkcję ASI (w tym były Naczelnik WIN⁹), informacja o powierzeniu obowiązków ASI została jedynie umieszczona w zakresach obowiązków tych pracowników. Natomiast w przypadku czwartego pracownika WIN brak jest jakichkolwiek dowodów potwierdzających powierzenie mu obowiązków ASI, nawet ujęcia ich w zakresie obowiązków.

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 Wilanów lub jego Zastępcy. Ponadto zgodnie Instrukcją zarządzania SI, informacja o obowiązku realizacji wskazanych powyżej zadań powinna znaleźć się w dokumencie wyznaczającym ASI. Ustalenia kontroli wskazują, iż w UD Wilanów nie dokonywano okresowych przeglądów i aktualizacji uprawnień.

Ponadto w trakcie kontroli ustalono, 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) zarówno przełożeni pracowników UD Wilanów, jak również pracowników COP, wbrew obowiązkowi wynikającemu z pkt V.10 Instrukcji zarządzania SI, nie informowali WIN o takim fakcie. W przypadkach pracowników UD Wilanów ich konta dostępu do SI były blokowane (odbierano im uprawnienia dostępu do SI) po otrzymaniu przez WIN stosownych informacji z WODO lub WO¹⁰. Natomiast w przypadku pracowników COP konto pozostawało aktywne tak długo, jak długo było ważne upoważnienie do przetwarzania danych osobowych stanowiące dla WIN podstawę do nadania uprawnień dostępu do SI¹¹. Ustalono, iż w okresie objętym kontrolą 10 użytkowników z COP posiadało aktywne konta w systemach Pakietu Info-System, pomimo, iż uległy zmianie okoliczności, które miały wpływ na zasadność nadanych uprawnień. Zgodnie

⁷ 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.

⁸ W rozdziale XIV Instrukcji zarządzania SI określono tryb wyznaczania ASI. Załącznik nr 1 stanowi wzór dokumentu wyznaczającego ASI, określa minimalny zakres obowiązków i odpowiedzialności ASI.

⁹ Naczelnik WIN posiadał upoważnienie do przetwarzania danych osobowych w Urzędzie m.st. Warszawy, w zakresie działania WIN z uprawnieniami ASI.

¹⁰ Zgodnie z § 10 ust. 2 Polityki bezpieczeństwa – Administrujący dokonuje bieżącej aktualizacji uprawnień dostępowych przy zmianach w składzie personelu, a także zmianach ról osób lub zmianach podmiotów przetwarzających.

¹¹ Upoważnienia do przetwarzania danych osobowych mogą być terminowe albo bezterminowe (wydane na czas zatrudnienia w danej komórce organizacyjnej).

z wyjaśnieniami Naczelnika Wydziału Kontroli Podatkowej COP okolicznością taką był fakt rozwiązania przez pracowników COP umowy o pracę (w efekcie czego blokowane były konta tych pracowników w domenie Urzędu m.st. Warszawy, co uniemożliwia im dostęp do SI). Należy zaznaczyć, iż realizacja obowiązku dokonywania raz w roku okresowego przeglądu i aktualizacji uprawnień użytkowników do dostępu do SI, ma na celu m.in. zapobieżenie pozostawianiu aktywnych kont w przypadku użytkowników, którzy nie powinni mieć już dostępu do SI. Zgodnie z zasadą minimalizacji przetwarzania danych osobowych w Urzędzie m.st. Warszawy¹², w przypadku zmiany zakresu obowiązków pracownika, w efekcie czego do realizacji nowych obowiązków nie jest już konieczny dostęp do danych osobowych, pracownikowi należy odebrać taki dostęp.

Wskazane powyżej nieprawidłowości dotyczące pominięcia w procesie nadawania uprawnień dostępu do SI osób uprawnionych do podejmowania decyzji o przyznaniu takich uprawnień, związane ze sposobem wyznaczenia ASI oraz określenia i powierzenia im zadań, a także brak dokonywania raz w roku okresowego przeglądu i aktualizacji uprawnień użytkowników do dostępu do SI mogą świadczyć o naruszeniu standardów: A.4, C.14 i C.15 kontroli zarządczej dla sektora finansów publicznych, które zobowiązują do precyzyjnego określenia zakresu uprawnień delegowanych poszczególnym osobom zarządzającym lub pracownikom, do zadbania, aby dostęp do zasobów jednostki miały wyłącznie upoważnione osoby oraz nakazują przestrzeganie określonych mechanizmów służących zapewnieniu bezpieczeństwa danych i systemów informatycznych.¹³

Zgodnie z pkt V.8 Instrukcji zarządzania SI właściciel biznesowy zobowiązany jest do prowadzenia bieżącej ewidencji nadanych uprawnień do SI (dalej: Ewidencja). W UD Wilanów Ewidencja prowadzona była osobno dla każdego SI. W przypadku 17 SI wchodzących w skład Pakietu Info-System Ewidencja prowadzona była w jednym z systemów tego Pakietu. Ewidencja ta została udostępniona w postaci 3 plików PDF (2 dla pracowników UD Wilanów i 1 dla pracowników COP¹⁴ – łącznie w latach 2021 – 2022 ewidencja zawierała 413 kont użytkowników). W przypadku pozostałych 3 SI¹⁵ Ewidencja była prowadzona w arkuszach kalkulacyjnych MS Excel (łącznie w latach 2021 – 2022 Ewidencja zawierała 33 aktywne konta użytkowników i 9 kont nieaktywnych). W Ewidencjach uprawnień nie dokonano jednoznacznego określenia użytkownika (zawarto informacje o imionach i nazwiskach bez przypisania wewnętrznej komórki organizacyjnej). Nie określono także, w sposób zgodny z Instrukcją zarządzania SI¹⁶ zakresu dostępu do SI. Zastępca Burmistrza wyjaśnił, iż w Ewidencjach wskazano zakresy uprawnień zgodne z nazwami funkcjonującymi w danym systemie, oraz że w przypadku uprawnień z Pakietu Info-System zakres typów uprawnień jest bardzo

¹² § 7 pkt 4 Polityki bezpieczeństwa – przetwarzanie odbywa się w konkretnych i aktualnych celach.

¹³ 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.).

¹⁴ W Ewidencji uprawnień na końcu oznaczenia nazwy konta użytkownika dodano „(COP)”.

¹⁵ OPTIEST, SYGNITY i WinDOM

¹⁶ 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).

rozbudowany i nie odzwierciedla zakresu typu uprawnień zawartych w Instrukcji zarządzania SI. Na podstawie Ewidencji systemów OPTIEST, SYGNITY i WinDOM ustano, iż w latach 2021 – 2022 nadano lub odebrano uprawnienia dostępu 5 użytkownikom.¹⁷ W Ewidencji Pakietu Info-System nie odnotowywano dat nadania, przedłużenia i ewentualnego odebrania uprawnień. Nie podstawie udostępnionych plików nie można więc ustalić, ilu użytkownikom w latach 2021 – 2022 nadano, przedłużono lub odebrano uprawnienia dostępu do systemów z Pakietu Info-System oraz czy konto użytkownika jest aktywne czy nieaktywne.¹⁸ Ponadto prowadzony w UD Wilanów wewnętrzny helpdesk, nie zawiera wszystkich wniosków w sprawie nadania, przedłużenia lub odebrania uprawnień dostępu do SI.

Szczegółową kontrolą objęto wszystkie sprawy 5 użytkowników z lat 2021 – 2022 dotyczące uprawnień dostępu do systemów OPTIEST i SYGNITY oraz sprawy dotyczące uprawnień dostępu do systemów z Pakietu Info-System wybranych 37 użytkowników, w tym: 19 pracowników UD Wilanów oraz 18 pracowników COP¹⁹. Informacja o 21 wnioskach przełożonych, wiadomościach WODO lub WO stanowiących podstawę nadania, przedłużenia lub anulowania przez pracowników WIN upoważnień dostępu do SI, znajdowała się w helpdesk'u prowadzonym przez WIN. Natomiast w przypadku kolejnych 31 wniosków i wiadomości stanowiących podstawę nadania, przedłużenia lub anulowania przez pracowników WIN upoważnień dostępu do SI, stosowna informacja nie została zamieszczona w helpdesk'u. Spośród tych 31 wniosków i wiadomości, 23 znajdowały się w zasobach WIN i zostało udostępnionych w trakcie kontroli. Natomiast w pozostałych 8 przypadkach brak było takich wniosków i wiadomości. Zgodnie z wyjaśnieniami złożonymi w trakcie kontroli, sprawy te zostały zrealizowane bezpośrednio przez poprzedniego Naczelnika WIN albo wnioski złożono drogą telefoniczną. Zgodnie z wyjaśnieniami uzyskanymi w trakcie kontroli, braki w ewidencji wniosków wynikają ze sposobu prowadzenia helpdesk'u, gdyż informacje o wiadomościach i wnioskach uzyskanych przez WIN były „ręcznie” przenoszone do helpdesk'u.

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,
- powołanie ASI w sposób niezgodny z Instrukcją zarządzania SI,
- brak dokonywania okresowych przeglądów i aktualizacji uprawnień użytkowników do dostępu do SI,

¹⁷ 2 użytkownikom nadano uprawnienia dostępu do systemu OPTIEST, 1 użytkownikowi nadano uprawnienia dostępu do systemu SYGNITY, 2 użytkownikom odebrano uprawnienia dostępu do systemu OPTIEST. Nie prowadzono takich spraw w przypadku systemu WinDOM.

¹⁸ Przedrostek „old_” w nazwie użytkownika, mający świadczyć o wyłączeniu danego konta dodawany jest ręcznie przez pracowników WIN. W celu ustalenia czy konto użytkownika jest aktywne czy nieaktywne konieczne jest skorzystanie z systemu admin.

¹⁹ 10 użytkowników którym w latach 2021 – 2022 nadano uprawnienia dostępu, przy czym w przypadku 7 z nich, w okresie tym uległy zmianie okoliczności, które miały wpływ na zasadność nadanych uprawnień oraz 8 użytkowników, którym uprawnienia nadano przed rokiem 2021, a w latach 2021 – 2022 uległy zmianie okoliczności, które miały wpływ na zasadność nadanych uprawnień.

- brak w Ewidencjach informacji jednoznacznie określających użytkownika oraz niezgodne z Instrukcją zarządzania SI określenia zakresów dostępu;
 - nierzetelne prowadzenie ewidencji wniosków (hepdesk),
- dają podstawę do pozytywnej z zastrzeżeniami oceny działalności UD Wilanów w zakresie objętym niniejszą kontrolą.²⁰

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.
5. Uzupełnienie Ewidencji w sposób umożliwiający jednoznaczne określenie użytkownika oraz określenie, zgodnie z Instrukcją zarządzania SI, zakresu dostępu.
6. Rzetelne prowadzenie ewidencji wniosków.

Na podstawie § 22 ust. 10 Regulaminu organizacyjnego oraz § 41 ust. 1 Zarządzenia oczekuję od Pana Burmistrza, 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 niewykorzystaniu uwag bądź o innym sposobie usunięcia stwierdzonych nieprawidłowości lub uchybień.

Na podstawie § 41 ust. 1 Zarządzenia zobowiązuje Pana Burmistrza do przekazania kopii ww. informacji Dyrektorowi Biura Kontroli.

PREZYDENT
MIASTA STOŁECZNEGO WARSZAWY

Rafał Trzaskowski

²⁰ Do oceny działań UD Wilanów w obszarze objętym kontrolą zastosowano skalę: ocena pozytywna, ocena pozytywna z zastrzeżeniami, ocena negatywna.