



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, 10 maja 2023 r.

Znak sprawy: KW-ZSS.1712.1.2023.TTR

**Pan
Grzegorz Kaczorowski
Dyrektor
Biura Rozwoju Gospodarczego
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 Biurze Rozwoju Gospodarczego Urzędu m.st. Warszawy (dalej BRG) 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 22 marca 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 oddaleniu w całości złożonych zastrzeżeń do Projektu wystąpienia pokontrolnego, przekazuję Panu niniejsze Wystąpienie pokontrolne.

Kontrolą objęto realizację przez BRG w latach 2021 – 2022 Procedury nadawania uprawnień dostępu do archiwalnego informatycznego systemu Ewidencja Działalności Gospodarczej (dalej: Procedura EDG) 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.

W okresie objętym kontrolą, obowiązywały trzy, zatwierdzone przez Dyrektora BRG, wersje Procedury EDG, tj.: z lutego 2020 r., z maja 2021 r. (wersja 1.0) oraz z 29 grudnia 2022 r. (wersja 2.0). Wersja Procedury EDG z lutego 2020 r. różniła się od dwóch pozostałych: wzorami wniosków o nadanie uprawnień oraz załącznikami do tych wniosków, a także oświadczeniami składanymi przez osoby wnioskujące o nadanie uprawnień podległym im pracownikom. W przypadku Procedury EDG z lutego 2020 r. niezbędne było dołączenie kopii upoważnienia do przetwarzania danych osobowych pracownika, a w kolejnych wersjach Procedury EDG wnioskujący, tj. Burmistrz Dzielnicy lub Dyrektor Biura, został zobowiązany do złożenia oświadczenia, iż pracownik takie upoważnienie posiada.

Pomimo znaczących różnic w kolejnych wersjach Procedury EDG, to do 19 stycznia 2023 r., tj. przez ponad półtora roku od zatwierdzenia Procedury EDG w wersji 1.0, na PortUM¹ dostępna była tylko jej nieaktualna wersja z lutego 2020 r. W roku 2021 Dyrektor BRG rozpatrzył 4 wnioski, przy czym pierwszy z nich wpłynął 2 czerwca 2021 r., a w roku 2022 – 11 wniosków. Chociaż w trakcie kontroli wyjaśniono, że Procedura EDG w wersji 1.0 była udostępniana przez BRG pracownikom dzielnic, to wszystkie 4 wnioski z roku 2021, w tym wniosek dotyczący pracownika BRG, i 2 wnioski z roku 2022 były niezgodne z wnioskiem stanowiącym załącznik do obowiązującej wówczas Procedury EDG w wersji 1.0. Wnioski te były bowiem zgodne z załącznikiem do Procedury EDG z lutego 2020 r. Powyższa sytuacja świadczy o braku przestrzegania standardów kontroli zarządczej dla sektora finansów publicznych, w tym w szczególności standardu D.16, zobowiązującego do zapewnienia osobom zarządzającym i pracownikom, w odpowiedniej formie i czasie, właściwej oraz rzetelnej informacji potrzebnej do realizacji zadań.²

W trakcie kontroli ustalono także, iż dopiero 16 grudnia 2021 r., tj. niemal dwa lata od wejścia w życie Polityki bezpieczeństwa, w BRG wyznaczono Administratora Systemów Informatycznych (dalej: ASI), który odpowiada za sprawność, konserwację, wdrożenie i stosowanie zasad bezpieczeństwa danych w zakresie technicznych zabezpieczeń systemów informatycznych.³ Jednocześnie ustalono, iż do momentu powołania ASI, jego czynności były realizowane, przez 3 pracowników wskazanych przez Dyrektora BGR, jedynie w zakresie administrowania EDG.

¹ Intranet Urzędu m.st. Warszawy – portum.um.warszawa.pl zakładka Baza Wiedzy => Ochrona Danych Osobowych => Przepisy, procedury i wytyczne. Obecnie w PortUM dostępna jest Procedura EDG w wersji 2.0.

² 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.)

³ W piśmie powołującym ASI wskazano, iż swoje obowiązki rozpoczyna pełnić 27 grudnia 2021 r.

Zgodnie z § 10 ust. 3 i 4 Polityki bezpieczeństwa ASI zobowiązany jest do dokonania raz w roku okresowego przeglądu i aktualizacji uprawnień użytkowników do dostępu do systemu EDG, a o wynikach takiego przeglądu powinien poinformować Dyrektora BRG. Jednocześnie w Procedurach EDG w wersji 1.0 i 2.0 nałożono obowiązek okresowej (nie rzadziej niż raz na kwartał) weryfikacji nadanych uprawnień oraz corocznej kompleksowej, udokumentowanej weryfikacji nadanych uprawnień. Ponadto Dyrektor BRG wyznaczając ASI zobowiązał go do dokonywania nie rzadziej niż raz w roku, w terminie do 30 września, okresowego przeglądu i aktualizacji uprawnień dostępu użytkowników do EDG oraz informowania Dyrektora BRG w terminie do 20 października o wyniku takiego przeglądu.

Ustalono, iż chociaż pismami z 31 grudnia 2021 r. i 28 października 2022 r. ASI poinformował Dyrektora BRG o dokonaniu okresowego przeglądu i aktualizacji uprawnień użytkowników systemu EDG w roku 2021 i 2022, to nie przedstawił efektów tych przeglądów. W trakcie kontroli ASI oświadczył, iż w wyniku przeglądu uprawnień w roku 2021 cofnięto uprawnienia 2, a w roku 2022 10 użytkownikom EDG. Jednocześnie w trakcie kontroli nie potwierdzono realizacji w roku 2021 i 2022 okresowej (nie rzadziej niż raz na kwartał) weryfikacji nadanych uprawnień, tj. zadań wskazanych w Procedurze EDG w wersji 1.0.

Zgodnie z Procedurą EDG w BRG powinna być prowadzona bieżąca ewidencja nadanych uprawnień do systemu EGD (rejestr użytkowników EDG). Kolejne wersje Procedury EDG miały odmienne wymagania dotyczące zakresu informacji jakie powinny być zawarte w takim rejestrze. Procedura EDG w wersji z lutego 2020 r. nie określała zakresu informacji zawartych w ewidencji nadanych uprawnień do EDG. Zgodnie z Procedurą EDG w wersji 1.0 ewidencja miała zawierać co najmniej datę nadania uprawnienia, datę cofnięcia uprawnienia i dane identyfikujące osobę, której nadano uprawnienie. Natomiast w przypadku Procedury EDG w wersji 2.0 w ewidencji należy wykazywać co najmniej datę wniosku i dane identyfikujące osobę, której uprawnienia dotyczą.

Zgodnie z prowadzoną w BRG ewidencją nadanych uprawnień do systemu EGD, w trakcie kontroli⁴ w systemie EDG aktywne konta posiadało 72 użytkowników. Ustalono, iż w rejestrze tym, wbrew wymaganiom Procedury w wersji 2.0, dla żadnego użytkownika nie wskazano daty wniosku. Jednocześnie należy wskazać, iż 5 wniosków z roku 2022 nie posiada daty sporządzenia oraz daty wpłynięcia do BRG. Należy jednak podkreślić, iż data wniosku nie jest informacją przydatną w zarządzaniu dostępem do systemu EDG. Informacją taką jest natomiast, nieodnotowywany w rejestrze, termin obowiązywania upoważnienia do przetwarzania danych osobowych (daty do której uprawnienia do dostępu mogą być udzielone). Należy zaznaczyć, iż z powodu braku możliwości technicznych systemu EDG, nie ma możliwości udzielania uprawnień czasowych, tj. nadając uprawnienia nie można określić daty ich automatycznego wyłączenia przez system. Obowiązek zablokowania konta użytkownika w takim przypadku spoczywa na osobach administrujących tym systemem, w tym na ASI. Kolejną istotną z punktu widzenia zarządzania kontami użytkowników daną jest data nadania uprawnień⁵, tj. data od której użytkownik posiadał dostęp do systemu EDG.

⁴ stan na dzień 13 lutego 2023 r.

⁵ Uprawnienia takie nadawane są po wyrażeniu pisemnej zgody przez Dyrektora BRG.

Tymczasem w rejestrze nadanych uprawnień jedynie dla 23 użytkowników ujawniono datę nadania uprawnień/wyrażenia zgody.

Jednocześnie, wbrew obowiązowi wynikającemu z punktów V.7-9 Instrukcji zarządzania systemami informatycznymi w Urzędzie m.st. Warszawy⁶, rejestr nadanych uprawnień nie zawiera informacji o użytkownikach, którym zablokowano dostęp do EDG. Informacja taka dostępna jest w systemie EDG.

Kontroli poddano realizację wszystkich 15 wniosków o nadanie uprawnień dostępu do EDG, które wpłynęły do BRG w latach 2021 – 2022. Wszystkie wnioski zostały rozpatrzone pozytywnie – udzielono zgody na nadanie uprawnień dostępu do EDG. Jednak w żadnym z tych przypadków, nie można ustalić daty wyrażenia przez Dyrektora BRG zgody na dostęp do EDG. Bowiem wbrew obowiązowi wynikającemu z § 58 Instrukcji kancelaryjnej⁷ na wnioskach brak jest daty ich akceptacji przez Dyrektora BRG. Ponadto powyższa sytuacja świadczy o naruszeniu wymagań normy ISO 9001:2015,⁸ w szczególności wymagań wskazanych w punktach 7.5.2 i 8.5.2, zobowiązujących do zapewnienia odpowiedniej (jednoznacznej) identyfikacji udokumentowanych informacji (udzielonych zgód) oraz zapewnienia zdolności do prześledzenia historii podejmowanych działań związanych z nadawaniem uprawnień.

W trakcie kontroli ustalono, iż w latach 2021 – 2022 do BRG nie wpłynęły wnioski o odebranie uprawnień osób posiadających dostęp do EDG. Tym niemniej, pozytywnie należy ocenić fakt, iż Procedura w wersji 2.0, zgodnie z rekomendacjami Biura Organizacji Urzędu m.st. Warszawy⁹, została rozszerzona o proces cofania uprawnień na wniosek (np. w przypadku zmiany zakresu wykonywanych zadań przez pracownika).

Powyższe ustalenia kontroli dają podstawę do pozytywnej z zastrzeżeniami oceny działalności BRG w zakresie objętym niniejszą kontrolą.¹⁰

⁶ Vide § 21 Polityki bezpieczeństwa, wprowadzona 1 stycznia 2021 r.

⁷ Załącznik do Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. z 2011 r. Nr 14, poz. 67 z późn. zm.)

⁸ Vide Zarządzenie Nr 1600/2016 Prezydenta Miasta Stołecznego Warszawy z dnia 28 października 2016 r. w sprawie trybu i zasad zarządzania jakością, projektami i zmianą w Urzędzie m.st. Warszawy (z późn. zm.)

⁹ Pismem z dnia 29 lipca 2022 r. znak OU-WODO-BI.142.78.2022.MRO Zastępca Dyrektora Biura Organizacji Urzędu wystąpił do Dyrektorów Biur o dokonanie zmian w procedurach nadawania uprawnień dostępu do systemów informatycznych m.in. w zakresie uregulowania kwestii cofania uprawnień do tych systemów.

¹⁰ Do oceny działań BRG w obszarze objętym kontrolą zastosowano skalę: ocena pozytywna, ocena pozytywna z zastrzeżeniami, ocena negatywna.

Przedstawiając powyższe ustalenia i oceny zalecam:

1. Udostępnianie na PortUM aktualnej wersji Procedury EDG.
2. Dokonywanie przeglądów i aktualizacji uprawnień dostępu do systemu EDG w terminach wskazanych w Polityce bezpieczeństwa, a także w terminach wynikających z wewnętrznych regulacji BRG w tym zakresie (Procedura EGD, pismo powołujące ASI etc.).
3. Zapewnienie rzetelnego informowania Dyrektora BRG o wynikach przeprowadzonych przeglądów i aktualizacji uprawnień dostępu do systemu EDG.
4. Uzupełnienie ewidencji nadanych uprawnień do systemu EDG w zakresie informacji wskazanych w Procedurze EDG (data wniosku) a także o dane istotne w procesie zarządzania dostępem do systemu EDG (w szczególności data nadania uprawnień – założenia konta w systemie EDG, data ważności upoważnienia do przetwarzania danych osobowych) oraz jej bieżącą aktualizację.
5. Wskazywanie na wnioskach o dostęp do systemu EDG dat ich akceptacji albo odmowy.

Na podstawie § 22 ust. 10 Regulaminu organizacyjnego oraz § 41 ust. 1 Zarządzenia oczekuję od Pana Dyrektora, 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 Dyrektora do przekazania kopii ww. informacji Dyrektorowi Biura Kontroli.

PREZYDENT
MIASTA STOŁECZNEGO WARSZAWY



Rafał Trzaskowski

