NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP.410.006.03.2019

Pan
Rafał Kazimierz Trzaskowski
Prezydent Miasta Stołecznego Warszawy
pl. Bankowy 3/5
00-950 Warszawa

WYSTĄPIENIE POKONTROLNE

P/19/007 – Wdrożenie przez administrację publiczną regulacji dotyczących ochrony danych osobowych po wejściu w życie RODO

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 53 08, F +48 22 444 52 52
kap@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Stołecznego Warszawy, Plac Bankowy 3/5, 00-950 Warszawa (dalej Urząd Miasta)
Kierownik jednostki kontrolowanej	Rafał Kazimierz Trzaskowski, Prezydent Miasta Stołecznego Warszawy od 22 listopada 2018 r. (dalej: Prezydent lub Administrator). Poprzednio, w okresie objętym kontrolą, funkcję kierownika jednostki pełniła Hanna Beata Gronkiewicz-Waltz.
Zakres przedmiotowy kontroli	1. Organizacja ochrony danych osobowych w jednostce. 2. Wykorzystanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych. 3. Zarządzanie danymi osobowymi przetwarzanymi, w tym gromadzonymi, w jednostce.
Okres objęty kontrolą	Od 25 maja 2018 r. do czasu zakończenia kontroli oraz dla zdarzeń wcześniejszych jeżeli miały wpływ na kontrolowaną działalność.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontrolerzy:	1. Andrzej Brunejko, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/96/2019 z 17 października 2019 r. 2. Marcin Grochal, specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/94/2019 z 17 października 2019 r. 3. Krzysztof Aleksander Matuszek, doradca ekonomiczny, upoważnienie do kontroli nr KAP/95/2019 z 17 października 2019 r. (akta kontroli str.1-5)

[1] Dz. U. z 2019 r. poz. 489, ze zm., dalej: ustawa o NIK.

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie Miasta Stołecznego Warszawy realizowano zadania zmierzające do wdrażania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[3] (dalej RODO).

Został opracowany system przetwarzania i zabezpieczania danych osobowych zgodny z wymogami RODO. Pracownicy odbyli szkolenia z zakresu ochrony danych osobowych oraz zostali zapoznani ze zaktualizowanymi procedurami dotyczącymi bezpieczeństwa informacji. Realizując obowiązki określone w RODO, Prezydent powołał Inspektora Ochrony Danych (IOD) oraz jego zastępcę i umożliwił im realizację zadań w sposób niezależny. Osoby pełniące te funkcje posiadały odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. W okresie objętym kontrolą NIK nie stwierdziła zaniedbań w realizacji obowiązków IOD.

Zawiadomienia o naruszeniu ochrony danych osobowych sporządzono zgodnie z przepisami RODO oraz z przyjętymi uregulowaniami wewnętrznymi i w terminie przekazano je do Prezesa Urzędu Ochrony Danych Osobowych.

Kontrola w zakresie przestrzegania zasad ochrony danych osobowych przeprowadzona Urzędzie Dzielnicy Ochota[4] (dalej: Urząd Dzielnicy) wykazała, że ochrona ta, poza niewielkimi odstępstwami, prowadzona była zgodnie z wytycznymi określonymi w RODO i w uregulowaniach wewnętrznych. Stosowano techniczne, fizyczne i informatyczne środki bezpieczeństwa, służące utrzymaniu poufności, integralności i odporności systemów oraz usług przetwarzania. Pracownicy posiadali stosowne upoważnienia do przetwarzania danych osobowych. Burmistrz ww. Dzielnicy, pełniąca funkcję Administrującego, prawidłowo informowała kandydatów do pracy, pracowników posiadających służbowe konta e-mail, zleceniobiorców i petentów o przetwarzaniu ich danych osobowych. Monitoring wizyjny funkcjonował tylko w miejscach dozwolonych. Nie stwierdzono przypadków ujawnienia danych osobowych w miejscach ogólnodostępnych.

Kontrola NIK wykazała nieprawidłowości polegające na:

- niezablokowaniu dostępu do domeny[5] pracownikom Urzędu Dzielnicy, których upoważnienie do przetwarzania danych osobowych utraciło moc na skutek zakończenia stosunku pracy[6],
- niepoinformowaniu przez Burmistrza Dzielnicy Ochota, za potwierdzeniem odbioru, pracowników którzy nie posiadają służbowych kont mailowych o przetwarzaniu ich danych osobowych.

---

2 Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
3 Dz. U UE L 119 z 4 maja 2016 r., str. 1, ze zm.
4 Urząd Dzielnicy Ochota wybrano do przeprowadzenia szczegółowych badań kontrolnych.
5 Dostęp do domeny umożliwia przetwarzanie danych osobowych w systemach informatycznych.
6 W przypadku 16 z 21 byłych pracowników.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe kontrolowanej działalności

OBSZAR

1. Organizacja ochrony danych osobowych w jednostce.

1.1 Przygotowanie dokumentacji wymaganej przepisami RODO.

Opis stanu faktycznego

Organizacja i zasady funkcjonowania Urzędu Miasta zostały określone w Regulaminie Organizacyjnym wprowadzonym zarządzeniem Nr 312/2007 Prezydenta miasta stołecznego Warszawy z dnia 4 kwietnia 2007 r., w sprawie nadania regulaminu organizacyjnego Urzędu miasta stołecznego Warszawy. Ochrona danych osobowych należy do zadań Biura Organizacji Urzędu. Zgodnie z wewnętrznym Regulaminem organizacyjnym Biura Organizacji Urzędu[7] do zakresu działania Wydziału Ochrony Danych Osobowych należało m.in. opracowywanie dokumentacji dotyczącej bezpieczeństwa przetwarzania i ochrony danych osobowych oraz prowadzenie rejestrów z tym związanych, wyjaśnienie incydentów bezpieczeństwa danych osobowych w Urzędzie Miasta oraz prowadzenie szkoleń w zakresie realizacji zadań ochrony oraz bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta.

(akta kontroli str. 897-1028)

W ramach przygotowania do wejścia w życie RODO, w kwietniu 2018 r. na podstawie jednostkowych analiz przedłożonych przez urzędy dzielnic i biur m. st. Warszawy w Urzędzie Miasta została przeprowadzona analiza ryzyka związanego z przetwarzaniem danych osobowych. W sporządzonym raporcie m.in. wykazano, że nie występują ryzyka (zagrożenia) na poziomie wysokim i bardzo wysokim, w związku z tym, stosownie do § 19 ust. 5 zarządzenia Nr 828/2015 z dnia 10 czerwca 2015 r. Prezydenta m. st. Warszawy w sprawie systemu zarządzania ryzykiem w m. st. Warszawie, nie było obowiązku sporządzenia planu postępowania z ryzykiem.

(akta kontroli str. 837-888)

W Urzędzie Miasta opracowano dokumentację w zakresie ochrony danych osobowych uwzględniającą wymogi RODO, obejmującą w szczególności:

- Politykę bezpieczeństwa przetwarzania i ochrony danych osobowych w Urzędzie m. st. Warszawy[8],
- Instrukcję zgłoszenia incydentu ODO[9] wraz z metodyką oceny wagi naruszenia[10],
- Procedurę zewnętrzną powierzania przetwarzania danych osobowych[11],
- Procedurę nadawania/zmiany/anulowania upoważnień do przetwarzania danych osobowych w Urzędzie m.st. Warszawy[12].

Dokumentacja dotycząca ochrony danych osobowych (przepisy, procedury, wytyczne) dostępna była na wewnętrznym portalu informacyjnym Urzędu Miasta w zakładce „ochrona danych osobowych”[13].

(akta kontroli str. 1085-1105, 1115-1144, 1237-1238, 1360-1414)

---

7 Zarządzenie Nr 1444/2018 Prezydenta m. st. Warszawy z dnia 31 sierpnia 2018 r. w sprawie nadania wewnętrznego regulaminu organizacyjnego Biura Organizacji Urzędu.

8 Zarządzenie Nr 850/2018 r. Prezydenta Miasta Stołecznego Warszawy z dnia 24 maja 2018 r. w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania i ochrony danych osobowych w Urzędzie m. st. Warszawy (niepublikowane), zmienione zarządzeniem Nr 1879/2019 z dnia 23 grudnia 2019 r.; dalej: Polityka bezpieczeństwa.

9 Ochrona danych osobowych.

10 Obowiązująca od 23 maja 2019 r. (Nr ODO/OU/M/1).

11 Zatwierdzona przez Dyrektora Biura Organizacji Urzędu obowiązująca od 31 sierpnia 2018 r. (Nr ODO/BU/PZ/2). Wcześniej obowiązywała *Procedura zewnętrzna zawierania umów powierzenia przetwarzania danych osobowych* obowiązująca od 8 czerwca 2018 r. (Nr ODO/BU/PZ/2) i znowelizowana 10 lipca 2018 r.; dalej: Procedura powierzania.

12 Z dnia 25 maja 2018 r. (Nr ODO/BOU/PZ1); dalej: Procedura nadawania.

13 https://helpdesk.um.warszawa.pl

1.2 Wyznaczenie i działanie Inspektora Ochrony Danych.

Opis stanu faktycznego

Stosownie do przepisu art. 37 ust. 1 lit. a) RODO Prezydent, dla całego Urzędu Miasta, łącznie z urzędami dzielnic, powołał Inspektora Ochrony Danych[14], który podlega bezpośrednio Administratorowi.

W dniu 9 grudnia 2019 r. Administrator wyznaczył Zastępcę IOD[15]. O wyznaczeniu IOD i jego zastępcy terminowo poinformowano Prezesa Urzędu Ochrony Danych Osobowych.

Nadzór nad prawidłowością przetwarzania danych osobowych w urzędach dzielnic sprawowany jest przez Prezydenta, za pośrednictwem burmistrzów pełniących funkcję Administrujących[16]. Zgodnie z Polityką bezpieczeństwa[17] Administrujący wyznacza koordynatora ODO, zadaniem którego jest wspieranie Administrującego w realizacji zadań oraz współpraca z IOD i dyrektorem biura właściwego ds. ochrony danych osobowych.

Zgodnie z art. 37 ust. 7 RODO na stronach internetowych Urzędu Miasta oraz w ogólnodostępnych miejscach podane były aktualne dane kontaktowe IOD.

IOD miał niezbędne kwalifikacje, o których mowa w art. 37 ust. 5 RODO, poparte wykształceniem (m.in. aplikacja radcowska, podyplomowe studia z zakresu ochrony danych osobowych i informacji niejawnych), kursami i szkoleniami związanymi z problematyką RODO.

(akta kontroli str. 258-262, 683-697, 830-836, 889-896, 1116-1117, 1239-1244)

IOD realizował zadania określone w art. 39 RODO, tj. m.in. przeprowadził szkolenia pracowników Urzędu, kierował pisma zawierające wytyczne i wyjaśnienia dla pracowników odnośnie obowiązków związanych z ochroną danych osobowych, dokonywał przeglądu dokumentacji związanej z postępowaniami administracyjnymi prowadzonymi przez Urząd Ochrony Danych Osobowych (UODO).

(akta kontroli str. 683-697)

1.3 Inne działania jednostki związane z wdrażaniem RODO.

Opis stanu faktycznego

Oględziny w Urzędzie Dzielnicy[18] wykazały, że w ogólnodostępnych miejscach tego urzędu, zgodnie z art. 13 ust. 1 i ust. 2 RODO, znajdowały się klauzule informujące gości/petentów o przetwarzaniu ich danych osobowych. Wchodzących do ww. urzędu informowano także o monitoringu prowadzonym w Urzędzie Dzielnicy.

(akta kontroli str. 280-341)

W grudniu 2018 r., w Urzędzie Miasta i Delegaturze Biura Administracji i Spraw Obywatelskich w Urzędzie Dzielnicy Żoliborz UODO przeprowadził kontrolę, którą objęto m.in. sporządzenie i wdrożenie polityki ochrony danych, źródło, zakres, cel i rodzaj przetwarzanych danych osobowych, sposób zbierania i udostępnienia danych osobowych, prowadzenie rejestrów czynności przetwarzania danych osobowych. W wyniku kontroli UODO stwierdzono uchybienia, które zostały usunięte jeszcze w trakcie tej kontroli[19].

(akta kontroli str. 6-36, 1029-1030)

---

[14] Zarządzenie Nr 1442/2018 Prezydenta m. st. Warszawy z dnia 31 sierpnia 2018 r. w sprawie wyznaczenia Inspektora Ochrony Danych w Urzędzie m. st. Warszawy oraz określenia jego zadań.

[15] Zarządzenie nr 1829/2019 Prezydenta Miasta Stołecznego Warszawy z dnia 9 grudnia 2019 r. w sprawie wyznaczenia osoby zastępującej Inspektora Ochrony Danych w Urzędzie m. st. Warszawy w czasie jej nieobecności.

[16] Stosownie do § 6 pkt 4 Polityki bezpieczeństwa (wg zarządzenia 850/2018).

[17] Stosownie do § 6 pkt 11 i § 29 ust. 6 Polityki bezpieczeństwa (wg zarządzenia 850/2018).

[18] Oględziny w zakresie zamieszczania informacji o przetwarzaniu danych osobowych przeprowadzono w siedzibach Urzędu Dzielnicy Ochota przy ul. Grójeckiej 17a i ul. Tarczyńskiej 21.

[19] W wyniku kontroli została wydana przez Prezesa Urząd Ochrony Danych Osobowych decyzja (z 17.05.2019 r. znak ZSPU.421.10.2018 EMU) w której m.in. podano, że Prezydent m.st. Warszawy jako Administrator danych naruszył przepisy o ochronie danych osobowych polegające na opracowaniu w Urzędzie m. st. Warszawy klauzuli informacyjnej dla osób realizujących obowiązek meldunkowy, która nie zawierała wszystkich informacji określonych w art. 13 RODO oraz nieujęcia w rejestrze czynności przetwarzania danych osobowych prowadzonym w Urzędzie m.st. Warszawy informacji o wszystkich odbiorcach danych osobowych przetwarzanych w związku z prowadzeniem rejestru mieszkańców. W decyzji wskazał jednocześnie, że w trakcie postępowania zostały usunięte ww. uchybienia i związku z powyższym umorzono postępowanie administracyjne w tym zakresie.

W 2018 r. w Urzędzie Miasta został przeprowadzony audyt wewnętrzny *Ocena bezpieczeństwa informatycznego ze szczególnym uwzględnieniem ochrony danych osobowych w kontekście zmieniającego się otoczenia prawnego*, zrealizowany w formie audytu zapewniającego w trzech jednostkach organizacyjnych oraz w formie audytu metodą analityczną w 1005 jednostkach organizacyjnych. W 2019 r. w planie audytu zostało ujęte zadanie pn*. Ocena bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych*, które do czasu zakończenia kontroli NIK było w trakcie realizacji.

W wyniku ww. audytów audytor wewnętrzny wskazał m.in., że zapewnienie bezpieczeństwa informacji wymaga usprawnień. W sprawozdaniu z audytu podano, że w ocenie audytora Biuro Organizacji Urzędu dołożyło należytych starań, aby wprowadzając w życie przepisy RODO odpowiednio zadbać o bezpieczeństwo danych osobowych. Podejmowane działania organizacyjne były nastawione na realizowanie wynikających z RODO obowiązków, co w znacznym zakresie pozwalało na osiągnięcie zgodności z prawem, jednak sposób ich realizacji zdaniem audytora wymaga ciągłego doskonalenia i zwiększenia efektywności, którą można byłoby osiągnąć stosując ujednolicone i wystandaryzowane systemy informatyczne.

(akta kontroli str. 37-255, 740-766)

W Urzędzie Miasta, przed 25 maja 2018 r. prowadzone były szkolenia kadry kierowniczej (dyrektorów biur, burmistrzów dzielnic) i radnych, przeprowadzone przez firmę zewnętrzną oraz pracowników Wydziału Ochrony Danych Osobowych Biura Organizacji Urzędu m. st. Warszawy. Szkolenia dotyczyły zmian prawnych związanych z wejściem w życie RODO oraz wynikających z nich obowiązków dla Administratora, dyrektorów biur oraz burmistrzów dzielnic. W maju 2018 r. wprowadzono szkolenie e-learningowe pn. *RODO - Rozporządzenie o ochronie danych osobowych*. Do udziału w tym szkoleniu zostali zobowiązani wszyscy pracownicy, stażyści, wolontariusze oraz praktykanci. W październiku 2018 r. uruchomiono dodatkowy moduł szkolenia e-learningowego pn. *Zastosowanie RODO w Urzędzie Miasta*, które dotyczyło m.in. ochrony danych osobowych, polityki bezpieczeństwa, zgłaszania naruszeń ochrony danych osobowych (dalej: incydentów) oraz obowiązków informacyjnych.

Dyrektor Biura Organizacji Urzędu wyjaśnił, że szkolenia e-learningowe są obowiązkowe dla każdego nowozatrudnionego pracownika w terminie 30 dni od zatrudnienia. Ponadto nowozatrudnieni pracownicy odbywają cykl szkoleń w zakresie ochrony danych osobowych, tj. szkolenia adaptacyjne (szkolenie obowiązkowe), służba przygotowawcza (szkolenie obowiązkowe). Dodał również, że każdy pracownik Urzędu Miasta ma możliwość uczestniczenia w szkoleniu *Ochrona danych osobowych w praktyce stosowanej w Urzędzie m. st. Warszawy*, przygotowanym w ramach programu samokształcenia[20].

(akta kontroli str. 830-836, 1031-1032)

Na przygotowanie i realizację zadań dotyczących ochrony danych osobowych w związku z wejściem w życie przepisów RODO w latach 2018-2019 wydatkowo w Urzędzie Miasta łączną kwotę 381,0 tys. zł, z czego 279,0 tys. zł na szkolenia dla pracowników, 16,0 tys. zł na wdrożenie oprogramowania do obsługi zgłoszeń i prowadzenia repozytorium incydentów bezpieczeństwa w zakresie danych osobowych oraz 86,0 tys. zł na zakup licencji dla użytkowników obsługujących incydenty bezpieczeństwa w zakresie ochrony danych osobowych.

[20] W szkoleniu tym biorą udział pracownicy, którzy wyrazili chęć uczestnictwa. Szkolenie to obejmuje m.in. zagadnienia dotyczące regulacji prawnych, zasad i przesłanek przetwarzania danych osobowych, powierzania i udostępniania danych osobowych, naruszenia bezpieczeństwa i ochrony danych osobowych.

W kontrolowanym okresie Prezes UODO nie nakładał na Urząd Miasta kar pieniężnych w związku z niewłaściwym stosowaniem RODO.

(akta kontroli str. 683-697)

Zgodnie z danymi przekazanymi przez IOD, w okresie od maja 2018 do lipca 2019 r., do UODO wpłynęło 10 skarg na funkcjonowanie ochrony danych osobowych w m. st. Warszawa, z których na dzień 24 października 2019 r. rozpatrzono cztery. Badanie NIK rozpatrzenia trzech skarg[21] wykazało, że dwie skargi uznano za bezzasadne[22], a w przypadku jednej skargi, Prezes UODO nałożył na Prezydenta karę upomnienia w związku z nieuprawnionym przetwarzaniem danych osobowych skarżącej w zakresie jej adresu zameldowania. Na wydaną ww. decyzję Prezydent wniósł skargę do Wojewódzkiego Sądu Administracyjnego, która została odrzucona[23].

(akta kontroli str. 353-446)

1.4 Nadzór gminy nad podległymi jednostkami w obszarze stosowania RODO.

Opis stanu faktycznego

Prezydent nie prowadził nadzoru nad podległymi jednostkami w zakresie ochrony danych osobowych.

Dyrektor Biura Organizacji Urzędu wyjaśnił*, że zgodnie z przepisami prawa kierownicy jednostek organizacyjnych gminy są odrębnymi od organów gminy administratorami, samodzielnie decydującymi o celach i sposobach przetwarzania danych osobowych. RODO, ani przepisy krajowe nie dają podstaw do sprawowania nadzoru przez jednego administratora nad innymi. Natomiast zgodnie z ustawą o finansach publicznych Prezydent m. st. Warszawy sprawuje kontrolę zarządczą nad jednostkami organizacyjnymi gminy. Kontrola ta prowadzona jest m.in. pod kątem legalności*.

Analiza informacji zawartych na stronach internetowych wybranych jednostek organizacyjnych[24] wykazała, że jednostki te na swoich stronach umieściły informacje wymagane przepisami RODO w zakresie wskazania administratora danych osobowych oraz IOD.

(akta kontroli str. 830-836)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działania Prezydenta w zakresie organizacji bezpieczeństwa informacji.

[21] Jedna skarga dotyczyła działań Prezydenta Miasta, a pozostałe dwie Burmistrzów Dzielnic.

[22] Postanowienie Wojewódzkiego Sądu Administracyjnego w Warszawie (Sygn. akt II SAWa 1971/19) z dnia 17 października 2019 r. Decyzja z dnia 30 maja 2019 r. (ZSPU.440.517.2018.DH) Prezesa Urzędu Ochrony Danych Osobowych.

[23] Postanowienie Wojewódzkiego Sądu Administracyjnego z dnia 19 lipca 2019 r. (sygn. akt II SA/Wa 1445/19).

[24] Badaniem objęto 10 jednostek organizacyjnych gminy.

OBSZAR

2. Wykorzystanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych.

2.1 Prowadzenie rejestrów wymaganych przepisami RODO.

Opis stanu faktycznego

Od 27 kwietnia 2018 r. w Urzędzie Miasta prowadzone były Rejestry: czynności przetwarzania danych osobowych (dalej: Rejestr czynności) oraz kategorii czynności przetwarzania (dalej: Rejestr kategorii czynności). Stosownie do art. 5 ust. 1 pkt c) RODO w prowadzonych rejestrach nie zawierano danych zbędnych lub niewspółmiernych do danej kategorii czynności przetwarzania. Zbierane dane były adekwatne, stosowne oraz ograniczone do tego, co było niezbędne do celów, dla których były przetwarzane.

Rejestr czynności zawierał wszystkie wymagane informacje, wymienione w art. 30 ust. 1 RODO i był na bieżąco aktualizowany. Natomiast Rejestr kategorii czynności nie zawierał wszystkich danych określonych w art. 30 ust. 2 RODO. Ustalono, że brak było danych kontaktowych Administratora i IOD podmiotu powierzającego przetwarzanie danych, tj. IOD Ministerstwa Cyfryzacji i Ministerstwa Spraw Wewnętrznych i Administracji, które dostępne są na stronach internetowych[25]. Ponadto nie podano aktualnych danych Administratora oraz IOD Urzędu Miasta. Nieprawidłowość ta została usunięta w trakcie kontroli.

(akta kontroli str. 683-697, 733-766)

Zgodnie z Polityką bezpieczeństwa[26] (§ 34 ust. 1 pkt 1 i 2) Administrujący prowadzą w nadzorowanej przez nich komórce organizacyjnej lokalne Rejestry czynności i lokalne Rejestry kategorii czynności dla danych powierzonych. Stosownie do § 34 ust. 4 Polityki bezpieczeństwa[27] sposób prowadzenia lokalnych Rejestrów czynności oraz lokalnych Rejestrów kategorii czynności, a także zakres informacji w nich zawartych i sposób przekazywania informacji, powinien być określony w odrębnej procedurze opracowanej przez Dyrektora biura właściwego w sprawie ochrony danych osobowych. Do czasu zakończenia czynności kontrolnych NIK procedura ta nie została określona.

Dyrektor Biura Organizacji Urzędu wyjaśnił, że wprowadzenie procedury jest ściśle powiązane z wdrożeniem narzędzia informatycznego, w którym prowadzony będzie Rejestr czynności i Rejestr kategorii czynności, a także lokalne rejestry czynności przetwarzania. Uruchomienie Rejestru czynności planowane jest na styczeń 2020 r., a wraz z uruchomianiem docelowej formy tego rejestru opublikowana zostanie procedura regulująca sposób prowadzenia rejestrów.

(akta kontroli str. 683-697, 752-766, 1033-1064, 1115-1134, 1516-1533)

2.2 Upoważnienia do przetwarzania danych.

Opis stanu faktycznego

W Urzędzie Miasta ewidencję pracowników posiadających upoważnienie do przetwarzania danych osobowych prowadzono w Wydziale Ochrony Danych Osobowych Biura Organizacji Urzędu. Sposób postępowania w przypadku nadawania/zmiany/anulowania upoważnień do przetwarzania danych osobowych został określony w Procedurze nadawania. Zgodnie z tą procedurą, upoważnienie do przetwarzania danych osobowych nadawane jest: pracownikom, radnym Rady

[25] Na stronie https://www.gov.pl/web/cyfryzacja/dane-kontaktowe są dostępne dane IOD Ministerstwa Cyfryzacji, na stronie https://www.gov.pl/web/mswia/inspektor-ochrony-danych są dostępne dane IOD MSWiA.

[26] Na podstawie zarządzenia Nr 850/2018.

[27] Na podstawie zarządzenia Nr 850/2018. Po zmianie ww. zarządzenia obowiązek ten wynika z § 57 pkt 1 Polityki bezpieczeństwa, wprowadzonej zarządzeniem Nr 1879/2019 z dnia 23 grudnia 2019 r.

Warszawy lub dzielnicy, pracownikom jednostek organizacyjnych m.st. Warszawy[28], wolontariuszom, stażystom, praktykantom i osobom realizującym na rzecz urzędu usługi na podstawie umowy cywilnoprawnej. Obsługa upoważnień, tj. wnioskowanie, wydawanie, zmiana i anulowanie realizowane jest z wykorzystaniem narzędzia informatycznego „aplikacja WODO[29]".

Na podstawie badania ewidencji wydanych upoważnień dla pracowników dwóch Wydziałów w Urzędzie Dzielnicy[30], stwierdzono, że wszyscy pracownicy badanych dwóch komórek organizacyjnych przetwarzający dane osobowe, zostali upoważnieni do przetwarzania tych danych oraz złożyli pisemne oświadczenia zobowiązujące do zachowania w tajemnicy wszelkich informacji dotyczących bezpieczeństwa danych osobowych, sposobów ich zabezpieczania oraz zapewnienia bezpieczeństwa przetwarzania i ochrony danych osobowych.

Badanie w zakresie wydawania upoważnień 15 pracownikom Urzędu Dzielnicy (10 nowozatrudnionym i pięciu zmieniającym komórkę organizacyjną) wykazało, że upoważnienia były nadawane/aktualizowane w terminach od jednego do pięciu dni.

Badanie pięciu umów zleceń związanych z przetwarzaniem danych osobowych wykazało, że zleceniobiorcom tym wydano upoważnienia do przetwarzania danych osobowych.

(akta kontroli str. 1106-1114, 1271-1275)

Zgodnie ze *Standardem: Zarządzania kontami użytkowników domeny Urzędu m. st. Warszawy o statusie wyłączony oraz nieaktywny* oraz *Procedurą wyłączania kont zwykłych*[31], blokada konta użytkownika (pracownika) domeny Urzędu Miasta następuje odpowiednio na wniosek osoby upoważnionej lub kierownika komórki organizacyjnej.

Kontrola w zakresie blokowania kont w domenie Urzędu Miasta, przeprowadzona w odniesieniu do 21 byłych pracowników Urzędu Dzielnicy wykazała, że blokady konta 16 z nich[32] następowały od jednego do 345 dni od zakończenia stosunku pracy, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 1150-1163, 1480)

Badanie 14 wybranych umów[33] zawartych w Urzędzie Dzielnicy i Urzędzie Miasta z podmiotami zewnętrznymi wykazało, że 11 z nich wiąże się z przetwarzaniem danych osobowych. Zgodnie z art. 28 ust. 3 RODO w ww. 11 umowach określono ich przedmiot, czas trwania, charakter i cel przetwarzania danych, rodzaj danych osobowych oraz kategorie osób, których dotyczą, jak również prawa i obowiązki administratora.

(akta kontroli str. 598-682, 1415-1471)

Prezydent wykonywał zadania podmiotu przetwarzającego na podstawie obowiązujących przepisów prawa[34]. W Rejestrze kategorii czynności zostały ujęte czynności Prezydenta, jako podmiotu przetwarzającego dla: obsługi rejestru PESEL i obsługi rejestru dowodów osobistych dla których administratorem jest Minister

---

28 Zgodnie z Regulaminem Organizacyjnym Urzędu m. st. Warszawy przez jednostkę organizacyjną m. st. Warszawy rozumie się nie wchodzące w skład Urzędu m.st. Warszawy i nie posiadające osobowości prawnej jednostki budżetowe i zakłady budżetowe m. st. Warszawy.

29 Program użytkowy przeznaczony do zarządzania systemem nadawania, anulowania i rejestrowania upoważnień.

30 Badaniem objęto 24 pracowników Dzielnicy Ochota – Wydziału Obsługi Mieszkańców i Wydziału Oświaty i Wychowania.

31 Standard: *Zarządzania kontami użytkowników domeny Urzędu m. st. Warszawy o statusie wyłączony oraz nieaktywny* z 24 stycznia 2018 r. oraz Procedura wyłączania kont zwykłych zatwierdzona 29 maja 2019 r. – oba dokumenty zatwierdzone przez Dyrektora Miejskiego Centrum Sieci i Danych.

32 W przypadku pozostałych pięciu pracowników jedna osoba nie posiadała konta w domenie, dwie osoby zostały zatrudnione w innej jednostce organizacyjnej gminy, jedna osoba zawarła nową umowę o pracę z Urzędem Miasta i jednej osobie zablokowano konto przed zakończeniem stosunku pracy.

33 W Urzędzie Dzielnicy Ochota od maja 2018 r. do 31 grudnia 2019 r. zawarto 256 umów powierzenia. Do badania wybrano w Urzędzie Dzielnicy 10 umów w sposób losowy i w sposób celowy trzy umowy dotyczące ochrony budynków Urzędu Dzielnicy Ochota (z 9.05.2018 r., 26.04.2019 r., 11.12.2019 r.) Ponadto w sposób celowy wybrano umowę zawartą przez Urząd Miasta nr OU/B/X/2/2/2/366/18-19/2100050406 z 6 grudnia 2018 r. dotyczącą niszczenia dokumentacji.

34 Ustawy: z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2019 r. poz. 1387), z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2019 r. poz. 2294), z 5 stycznia 2011 r. Kodeks wyborczy (Dz. U. z 2019 r. poz. 1504).

Cyfryzacji oraz obsługi rejestru mieszkańców i obsługi rejestrów wyborców dla których administratorem jest Minister Spraw Wewnętrznych i Administracji.

(akta kontroli str. 1311-1314)

2.3 Prowadzenie monitoringu wizyjnego.

Opis stanu faktycznego

Zasady prowadzenia monitoringu wizyjnego we wszystkich siedzibach Urzędu Miasta zostały opisane w *Wytycznych w zakresie funkcjonowania monitoringu wizyjnego*[35]. Stosownie do ww. Wytycznych Administratorem danych pozyskiwanych z systemu monitoringu w Urzędzie Miasta jest Prezydent. Administrującym dla danych pozyskanych z kamer monitoringu systemu zainstalowanego na terenie obiektów urzędów dzielnic jest Burmistrz właściwej dzielnicy. Zgodnie z ww. Wytycznymi nagrania obrazu są przechowywane maksymalnie przez okres trzech miesięcy od dnia nagrania. Kontrola w zakresie umiejscowienia monitoringu wizyjnego przeprowadzona w budynkach Urzędu Dzielnicy[36] wykazała, że stosownie do art. 22^2 § 2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy[37], monitoring nie obejmował pomieszczeń sanitarnych, szatni i innych pomieszczeń socjalnych.
Monitoringiem wizyjnym objęto ciągi korytarzowe, wejścia do Urzędu Dzielnicy, wjazdy oraz miejsca parkingowe przed tym Urzędem. Ustalono, że w miejscach ogólnodostępnych, tj. na zewnątrz budynków oraz w ich obszarze, w szczególności przy wejściach, umieszczone były symbole z napisem „*obiekt całodobowo monitorowany*", a także klauzule informacyjne.

(akta kontroli str. 263-341)

2.4 Ochrona systemów informatycznych.

Opis stanu faktycznego

Przyjęte w Urzędzie Miasta rozwiązania dotyczące zabezpieczeń przetwarzania danych osobowych oraz minimalizujące ryzyko przed nieuprawnionym uzyskaniem danych osobowych, ich kradzieżą lub utratą były opisane m.in. w Polityce bezpieczeństwa. W obszarze dostępu do serwerowni Urzędu Miasta, zastosowano instalacje alarmowe, przeciwwłamaniowe oraz system przeciwpożarowy i autoryzację wejść i wyjść przy pomocy elektronicznych kart dostępu. W Urzędzie Miasta uregulowano również zasady sporządzania kopii bezpieczeństwa zbiorów danych. Kopie wykonuje się cyklicznie w sposób automatyczny. Przewidziano także zasady testowania kopii bezpieczeństwa.
W ramach systemu zabezpieczeń danych osobowych w Urzędzie Dzielnicy stosowano ochronę fizyczną i ochronę techniczną budynku, w tym m.in. system pobierania i wydawania kluczy oraz elektroniczny system kontroli wejścia i wyjścia.
Badanie stosowania przez pracowników Urzędu Dzielnicy przyjętych rozwiązań minimalizujących ryzyko przed nieuprawnionym uzyskaniem danych osobowych, ich kradzieżą lub utratą, NIK przeprowadziła na próbie 10 stanowisk komputerowych. Każdy z użytkowników stanowiska posiadał indywidualne hasło dostępu do systemu informatycznego, przy użyciu którego rozpoczynał pracę w systemie. Praca wykonywana była przy wykorzystaniu wyłącznie własnego indywidualnego konta dostępu do systemu. We wszystkich kontrolowanych stanowiskach komputerowych zainstalowane zostało oprogramowanie antywirusowe, a korzystanie z poczty elektronicznej realizowane było przy pomocy konta pocztowego przydzielonego użytkownikom systemu. Kontrola wykazała, że pracownicy prawidłowo logowali się do systemu oraz prawidłowo blokowali i odblokowywali ekrany monitorów w stanowiskach komputerowych, działając zgodnie z obowiązującą w tym zakresie procedurą. Rozwiązania minimalizujące ryzyko nieuprawnionego uzyskania danych

[35] Z dnia 16 maja 2019 r. (Nr 0DO/OU/2/4).
[36] Tj. przy ul. Grójeckiej 17a i ul. Tarczyńskiej 21.
[37] Dz.U. z 2019 r. poz. 1040, ze zm.

osobowych, ich kradzieżą lub utratą pracownicy stosowali zgodnie z obowiązującą Polityką bezpieczeństwa.

(akta kontroli str. 342-352, 1509-1533)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Zablokowanie dostępu do kont w domenie Urzędu Miasta w przypadku 16 z 21 byłych pracowników[38] Urzędu Dzielnicy zostało dokonane w terminie od jednego do 345 dni od zakończenia stosunku pracy przez tych pracowników. Ponadto ustalono, że w przypadku kont czterech byłych pracowników dokonywane były logowania w systemach informatycznych Urzędu Miasta, po zakończeniu stosunku pracy.
Kontrolerom NIK nie przekazano informacji i dokumentów dotyczących terminu zgłoszenia konieczności odłączenia od domeny pracowników, z którymi rozwiązano stosunek pracy[39].
Nieblokowanie dostępu do systemów informatycznych (domeny) zawierających dane osobowe, osobom, których upoważnienia do przetwarzania danych osobowych wygasły z dniem zakończenia stosunku pracy może powodować, że nie zostanie dochowana zasada poufności danych określona w art. 5 ust. 1 lit. f) RODO.
Dyrektor Biura Organizacji Urzędu wyjaśnił, że na podstawie informacji uzyskanych od Miejskiego Centrum Sieci i Danych, przyczyną braku blokowania dostępu, było niezakupienie odpowiednich licencji dla dzielnic (zakupiono je dopiero w listopadzie 2019 r.) umożliwiających wyłączanie użytkownika bezpośrednio przez urzędy dzielnic.
Na pytanie kontrolujących odnośnie przyczyn niezgłaszania jako incydentów stwierdzonych przypadków logowań po zakończonym stosunku pracy Dyrektor Biura Organizacji Urzędu wyjaśnił, iż ze wstępnej analizy logów wynika, że logowania nastąpiły z adresów IP Urzędu Miasta i nie można jednoznacznie stwierdzić, czy miał miejsce incydent bezpieczeństwa. Ponadto wskazał, że wygenerowanie raportu wykazującego ile razy nastąpiło logowanie na wskazanych przez kontrolerów kontach użytkowników może nastąpić po 7 stycznia 2020 r.

(akta kontroli str.1150-1236, 1315-1317, 1480, 1534-1535, 1549-1552)

OCENA CZĄSTKOWA

W Urzędzie Miasta opracowano rozwiązania organizacyjne i techniczne w zakresie ochrony danych osobowych. Pracownicy Urzędu Dzielnicy posiadali wymagane upoważnienia do przetwarzania danych osobowych. Organizacja monitoringu wizyjnego w Urzędzie Dzielnicy była prawidłowa. Należy jednak wskazać, że blokowanie byłym pracownikom[40] Urzędu Dzielnicy dostępu do systemów informatycznych Urzędu Miasta następowało od jednego do 345 dni od daty rozwiązania stosunku pracy.

---

38 Patrz przypis 31.

39 Kontrolujący pismem z 16 grudnia 2019 r. zwrócili się do Burmistrza Dzielnicy Ochota o wskazanie terminu złożenia wniosku o odłączenie od domeny pracowników, z którymi rozwiązano stosunek pracy. W piśmie z 31 grudnia 2019 r. Burmistrz Dzielnicy nie udzieliła odpowiedzi na pytanie w tym zakresie. Pismem z 30 grudnia 2019 r. kontrolujący zwrócili się do Dyrektora Biura Organizacji Urzędu o podanie, na jakiej podstawie dokonano wyłączenia kont byłych pracowników Urzędu Dzielnicy Ochota i przedłożenie dokumentów potwierdzających formę i termin złożenia zleceń. W odpowiedzi z 3 stycznia 2020 r. Dyrektor Biura Organizacji Urzędu przekazał maile, z których nie wynika kto i kiedy złożył wnioski o odłączenie od domeny kont byłych pracowników Urzędu Dzielnicy.

40 W przypadku 16 z 21 byłych pracowników.

OBSZAR

3. Zarządzanie danymi osobowymi przetwarzanymi, w tym gromadzonymi w jednostce.

3.1 Postępowanie w przypadku naruszenia ochrony danych osobowych.

Opis stanu faktycznego

W Urzędzie Miasta wdrożono narzędzie informatyczne w sieci intranetowej do celów zgłaszania przypadków naruszenia ochrony danych osobowych, które umożliwia zgłaszanie takich incydentów przez urzędników. Zgłaszanie incydentów dokonywane jest poprzez wewnętrzny intranet za pomocą Centrum Wsparcia Urzędu Miasta[41].

Wprowadzono także metodykę oceny wagi naruszenia oraz zautomatyzowano sposób wyliczania wagi naruszenia. Wdrożone rozwiązanie standaryzuje klasyfikację incydentów i ocenę wagi naruszenia w całej strukturze Urzędu Miasta.

W Urzędzie Miasta opracowywano kwartalne i roczne *Raporty incydentów bezpieczeństwa danych osobowych*. Raporty te zawierały dane dotyczące m.in. liczby zgłoszonych incydentów, miejsca ich stwierdzenia oraz najczęstszych przyczyn ich powstania.

(akta kontroli str. 447-597)

Na podstawie prowadzonego w Urzędzie Miasta Rejestru naruszeń ustalono, że do dnia 18 grudnia 2019 r. do Prezesa UODO zostały zgłoszone 134 naruszenia ochrony danych osobowych. Szczegółowe badanie postępowań w przypadku naruszeń ochrony danych osobowych przeprowadzono na podstawie naruszeń stwierdzonych w Urzędzie Dzielnicy. W urzędzie tym, w okresie objętym kontrolą, zarejestrowano łącznie sześć przypadków naruszenia ochrony danych osobowych, z czego jeden w 2018 r. i pięć w 2019 r.

W przypadku dwóch naruszeń, po przeprowadzeniu oceny skutków naruszenia, w Urzędzie Miasta stwierdzone zostało, że były one zasadne i w terminie określonym w art. 33 ust. 1 RODO powiadomiono Prezesa UODO. W zgłoszeniach podano informacje o których mowa w art. 33 ust. 3 RODO, tj. opis charakteru naruszenia, konsekwencje oraz środki zastosowane w celu zaradzenia naruszeniu. Burmistrz Dzielnicy Ochota, zgodnie z 34 ust. 1 RODO, zawiadomiła osoby o fakcie naruszenia ochrony ich danych osobowych. W pozostałych czterech przypadkach po przeprowadzeniu przez IOD analizy stwierdzono, że nie było potrzeby przesyłania zawiadomień do Prezesa UODO, jak i informowania osób których to dotyczyło.

(akta kontroli str. 1239-1256)

3.2 Postępowanie z danymi osobowymi.

Opis stanu faktycznego

Od 25 maja 2018 r. do 31 października 2019 r. do Urzędu Miasta wpłynęły 344 żądania usunięcia danych osobowych oraz 46 wniosków o sprostowanie danych osobowych. W okresie tym do Urzędu Dzielnicy nie wpłynęły żądania usunięcia danych osobowych, natomiast wpłynęły dwa wnioski o sprostowanie danych osobowych (dotyczyły zmiany adresu zamieszkania i sprostowania nazwiska dziecka). W tych dwóch przypadkach Urząd Dzielnicy, w terminie określonym w art. 12 ust. 3 RODO prawidłowo poinformował wnioskodawców o pozytywnym uwzględnieniu wniosków i o podjętych działaniach w tym zakresie.

(akta kontroli str. 1239-1244, 1490-1507)

[41] https://helpdesk.um.warszawa.pl

W wyniku przeprowadzonych oględzin[42] w ogólnodostępnych miejscach znajdujących się w budynku Urzędu Dzielnicy ustalono, że nie było tam informacji, które mogły naruszać ochronę danych osobowych osób fizycznych.

(akta kontroli str. 280-341)

Zasady niszczenia dokumentów papierowych, a także usuwania informacji znajdujących się na sprzętach i nośnikach zewnętrznych uregulowane były w Polityce bezpieczeństwa. Zgodnie z przyjętą procedurą spis dokumentów do brakowania, podlegał akceptacji przez komórkę merytoryczną, a po otrzymaniu zgody Archiwum Państwowego, dokumentacja niszczona była przez wyspecjalizowany podmiot, wybrany przez Biuro Organizacji Urzędu. Urząd Miasta zawarł w 2018 r. umowę[43] z firmą zewnętrzną, której przedmiotem był odpłatny wywóz, zniszczenie zbędnej dokumentacji niearchiwalnej i makulatury, a także wystawianie z tego tytułu certyfikatów zniszczenia dokumentacji. Firmie tej w przedmiotowym zakresie, powierzono przetwarzanie danych osobowych[44]. Ustalono, że były sporządzane dokumenty potwierdzające odbiór i niszczenie ww. dokumentacji. Z procesu niszczenia dokumentacji sporządzano: certyfikat zniszczenia dokumentów, który zawierał m.in.: nr, datę i miejsce wydania dokumentów, nr zgody na brakowanie dokumentacji, datę zniszczenia, ilość zniszczonych metrów bieżących dokumentacji, nr pojemników, w których odebrano dokumentację do zniszczenia. Certyfikat zniszczenia dokumentów przekazywano do Zamawiającego.

(akta kontroli str. 610-625)

3.3 Ochrona danych osobowych pracowników.

Opis stanu faktycznego

W związku z dyspozycją Dyrektora Biura Organizacji Urzędu przekazaną e-mailem z 23 maja 2018 r., pracownicy Urzędu Dzielnicy posiadający służbowe konto e-mail zostali zapoznani z zasadami przetwarzania ich danych osobowych oraz poinformowani o przysługujących im prawach z tym związanych. Informacja o przetwarzaniu danych osobowych pracowników została przekazana wszystkim pracownikom drogą elektroniczną.

W przypadku pracowników nie posiadających służbowego konta e-mail Burmistrzowie zostali zobowiązani przez Dyrektora Biura Organizacji Urzędu do przekazania im treści klauzul informacyjnych w formie papierowej za potwierdzeniem odbioru. Ustalono, że w Urzędzie Dzielnicy nie wykonano tego polecenia, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 1276-1310, 1318-1330, 1481-1489, 1546-1548)

W 11 umowach powierzenia objętych badaniem, pięć z nich było umowami zlecenia zawartymi z osobami fizycznymi. W przypadku tylko dwóch z nich do umów załączono klauzule informacyjne o przetwarzaniu danych osobowych zleceniobiorców.

Burmistrz Urzędu Dzielnicy wyjaśniła, że klauzule informacyjne nie wymagają podpisu, ponieważ przyjęcie do wiadomości informacji zawartej w klauzuli jest uprawnieniem osoby fizycznej. Nie ma obowiązku parafowania i oznaczania datą faktu otrzymania lub zapoznania się z treścią klauzuli.

NIK zauważa, że chociaż przepisy RODO, w szczególności art. 12, nie narzucają konkretnej formy spełnienia obowiązku informacyjnego, jednakże niestosowanie pisemnej formy przekazywania informacji określonych w art. 13 RODO może rodzić problem w przypadku ewentualnego sporu dotyczącego przekazania tych informacji,

---

42 Oględziny przeprowadzono w pomieszczeniach Urzędu Dzielnicy Ochota na u. Grójeckiej 17a i ul. Tarczyńskiej 21.

43 Umowa nr OU/B/X/2/2/2/366/18-19/2100050406 z dnia 6 grudnia 2018 r.

44 Zamawiający w trybie art. 28 RODO powierzył Wykonawcy do przetwarzania wyłącznie w celu realizacji umowy dane osobowe Zasobu Archiwum Zakładowego Urzędu (…) i inne nieuporządkowane dokumenty do przetwarzania, na zasadach i w celu określonym w Umowie – § 6, pkt 3 Umowy.

gdzie ciężar wykazania, że obowiązek informacyjny został zrealizowany spoczywa na administratorze[45].

(akta kontroli str. 1167-1169, 1315-1317, 1415-1471)

W okresie objętym kontrolą, dokumenty aplikacyjne kandydatów, którzy nie zostali przyjęci do pracy w Urzędzie Dzielnicy, zostały usunięte z systemu elektronicznej rekrutacji, a z czynności tej sporządzono protokoły zniszczenia[46].

Sposób postępowania opisany powyżej był zgodny z zarządzeniem Prezydenta *w sprawie regulaminu przeprowadzania naboru kandydatów na wolne stanowiska urzędnicze, w tym na wolne kierownicze stanowiska urzędnicze w Urzędzie m. st. Warszawy*[47]. Zgodnie z tym zarządzeniem dokumenty aplikacyjne kandydatów niewyłonionych do zatrudnienia, po upływie nie mniej niż trzech miesięcy od zakończenia naboru, mają być usuwane z systemu elektronicznej rekrutacji urzędu i zgodnie z§ 14 ust. 2 ww. zarządzenia z czynności tej sporządza się protokół zniszczenia.

Kandydaci ubiegający się o pracę byli informowania o celu i sposobie przetwarza ich danych osobowych poprzez zaznaczenie odpowiedniego oświadczenia w elektronicznym formularzu aplikacyjnym[48].

(akta kontroli str.1278-1280, 1318-1330, 1508)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Burmistrz Dzielnicy Ochota nie wykonała polecenia Dyrektora Biura Organizacji Urzędu w zakresie przekazania pracownikom, którzy nie mają kont w domenie *klauzuli informacyjnej o przetwarzaniu danych osobowych dla pracowników Urzędu m. st. Warszawy,* w formie papierowej za potwierdzeniem odbioru, co było działaniem nierzetelnym.

Burmistrz Dzielnicy Ochota wyjaśniła m.in., że (…) *wszystkie osoby które nie posiadają służbowych adresów email i kont w domenie, zapoznały się z klauzulami informacyjnymi dotyczącymi przetwarzania danych osobowych. Klauzule informacyjne dla pracowników Urzędu m. st. Warszawy zostały zalaminowane i wywieszone w sekretariacie WAG[49] i pokoju pracowników.*

(akta kontroli str. 1318, 1546-1548)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie wprowadzenie zasad zarządzania danymi osobowymi przetwarzanymi w Urzędzie. Biorąc jednak pod uwagę stwierdzoną w Urzędzie Dzielnicy Ochota, nieprawidłowość w zakresie informowania niektórych pracowników o przetwarzaniu ich danych osobowych, w ocenie NIK konieczne jest wzmożenie nadzoru Prezydenta nad przestrzeganiem przez Burmistrzów tych zasad.

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

1. Wzmocnienie nadzoru nad działaniami Burmistrza Dzielnicy Ochota w zakresie:

---

45 Patrz: E. Bielak-Jomaa (red.), D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*.

46 Kontrolą objęto protokoły zniszczenia z czterech postępowań rekrutacyjnych.

47 Nr 1896/2017 z 13 grudnia 2017 r.

48 W § 5 ust. 5 zarządzenia wskazano, że *odznaczenie w elektronicznym formularzu oświadczeń (…) o wyrażeniu zgody na przetwarzanie danych osobowych zawartych w ofercie pracy dla potrzeb danej rekrutacji jest równoznaczne ze złożeniem oświadczenia (*oświadczenia dotyczą Administratora danych osobowych, danych kontaktowych z IOD, celu przetwarzania, informacji o odbiorcach, okresu przechowywania danych, prawie żądania do dostępu do danych osobowych, prawie do ich sprostowania, sprzeciwu i złożenia skargi do organu nadzorczego).

49 Wydział Administracyjno-Gospodarczy w Urzędzie Dzielnicy.

a) blokowania dostępu pracownikom do systemów informatycznych zawierających dane osobowe, najpóźniej w dniu rozwiązania z nimi stosunku pracy,
b) wykonywania poleceń Dyrektora Biura Organizacji Urzędu Miasta dotyczących poinformowania wszystkich pracowników o przetwarzaniu ich danych osobowych.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania.

Zastrzeżenia zgłasza się do dyrektora Departamentu Administracji Publicznej Najwyższej Izby Kontroli. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, dnia stycznia 2020 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej
Dyrektor
Bogdan Skwarka

.....
podpis

Kontrolerzy:
Andrzej Brunejko
Główny specjalista kontroli państwowej

.....
podpis

Marcin Grochal
Specjalista kontroli państwowej

.....
podpis

Krzysztof Aleksander Matuszek
Doradca ekonomiczny

.....
podpis