



NAJWYŻSZA IZBA KONTROLI

Delegatura w Łodzi

LLO.410.018.02.2019

Hanna Zdanowska
Prezydent Miasta Łodzi
Urząd Miasta Łodzi
Ul. Piotrkowska 104, 90-926 Łódź

WYSTĄPIENIE POKONTROLNE

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

23.12.2018 r.
Ewa Wysocka
Przewodnicząca
13.12.18

NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi
ul. Kilińskiego 210, 90-980 Łódź
T +48 42 239 32 00, F +48 42 239 32 90
llo@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Łodzi, ul. Piotrkowska 104, 90-926 Łódź (dalej: Urząd).
Kierownik jednostki kontrolowanej	Hanna Zdanowska, Prezydent Miasta Łodzi od 5 grudnia 2010 r.
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, jeśli mają 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 Delegatura w Łodzi
Kontroler	Katarzyna Marciniak, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LLO/182/2019 z dnia 16 września 2019 r. (Dowód: akta kontroli str. 1-4)

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

II. Ocena ogólna² kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie prawidłowo przygotowano się do wdrożenia 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. Ochrona danych osobowych prowadzona była zgodnie z RODO i uregulowaniami wewnętrznymi.

W Urzędzie opracowano system przetwarzania i zabezpieczania danych osobowych zgodny z wymogami RODO. Pracownicy Urzędu zostali przeszkoleni w związku z wejściem w życie nowych przepisów prawa i zapoznani ze zaktualizowanymi procedurami w zakresie bezpieczeństwa informacji. Realizując obowiązki określone w RODO, Prezydent Miasta Łodzi powołał Inspektora Ochrony Danych (IOD) i umożliwił mu realizację zadań w sposób niezależny. Osoba pełniąca tę funkcję posiadała odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. W kontrolowanym okresie IOD wywiązywał się z nałożonych na niego obowiązków. W Urzędzie rzetelnie prowadzono wymagane na podstawie RODO rejestry, tj. *Rejestr czynności przetwarzania danych osobowych*, *Rejestr kategorii czynności przetwarzania danych* i *Rejestr incydentów i naruszeń ochrony danych osobowych*.

Wdrożone w Urzędzie środki bezpieczeństwa, służące utrzymaniu poufności, integralności i odporności systemów i usług przetwarzania, były zgodne z regulacjami wewnętrznymi. Wszystkie komputery zostały zabezpieczone przed szkodliwym oprogramowaniem oraz dostępem z zewnątrz. W Urzędzie sporządzano i weryfikowano prawidłowość kopii zapasowych. Celem zapewnienia ciągłości pracy, kopie zapasowe przechowywano poza miejscem ich wytwarzania.

W kontrolowanym okresie doszło jednak do naruszeń ochrony danych osobowych. Stosowne zawiadomienie w tym zakresie, w przypadku wystąpienia przesłanek, przekazano do Prezesa Urzędu Ochrony Danych Osobowych z zachowaniem obowiązujących terminów.

Pracodawca, jako Administrator, prawidłowo informował kandydatów do pracy, pracowników, zleceniobiorców i petentów o przetwarzaniu ich danych osobowych. W Urzędzie przetwarzano dane osobowe wyłącznie na podstawie stosownego upoważnienia.

W ramach działań nadzorczych nad podległymi jednostkami pracownicy Urzędu prowadzili w tych jednostkach kontrole dotyczące m.in. zabezpieczeń teleinformatycznych i fizycznych oraz ochrony osób i mienia.

III. Opis ustalonego stanu faktycznego oraz oceny częściowej⁴ kontrolowanej działalności

OBSZAR

Opis stanu faktycznego

1. Organizacja ochrony danych osobowych w jednostce

1.1. Przygotowanie dokumentacji wymaganej przepisami RODO

W związku z wejściem w życie przepisów RODO, w ramach działań związanych z wdrożeniem systemu zarządzania bezpieczeństwem informacji, w Urzędzie dokonano szacowania ryzyka utraty bezpieczeństwa informacji, o której mowa

² Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

³ Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1. Tekst rozporządzenia dostępny pod adresem: <https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1527242776060&uri=CELEX:32016R0679>.

⁴ Oceny częściowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena częściowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

w art. 32 RODO. Szacowanie to zostało przeprowadzone przez Wydział Informatyki. Wyniki szacowania zawarto w dokumencie pn.: *Ocena ryzyk naruszenia praw lub wolności osób, których dane dotyczą, dla systemu teleinformatycznego Urzędu Miasta Łodzi, z uwzględnieniem środków obniżających ryzyko*. Dokument ten nie zawierał zaleceń i wniosków.

(dowód: akta kontroli str. 38-42)

W dniu 10 kwietnia 2018 r. Prezydent Miasta Łodzi wydał zarządzenie w sprawie wdrożenia - od dnia 25 maja 2018 r. - polityki ochrony danych osobowych w Urzędzie Miasta Łodzi (dalej *Polityka ochrony danych osobowych*). Dokumentacja ta zawierała: *Politykę bezpieczeństwa w systemach informatycznych Urzędu Miasta Łodzi* (dalej *Polityka bezpieczeństwa w systemach informatycznych*), *Instrukcję w sprawie zasad postępowania przy przetwarzaniu danych osobowych* (dalej *Instrukcja postępowania przy przetwarzaniu danych*) i *Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* (dalej *Instrukcja zarządzania systemem informatycznym*).

Stosownie do postanowień art. 30 ust. 1 i 2 RODO, w Urzędzie utworzono także *Rejestr czynności przetwarzania danych osobowych* oraz *Rejestr kategorii czynności przetwarzania*. Ponadto utworzono *Rejestr incydentów i naruszeń ochrony danych osobowych*, uwzględniający dane określone w art. 33 ust. 5 RODO.

(dowód: akta kontroli str. 5-37)

Pracownicy Urzędu zostali zapoznani z *dokumentacją w sprawie wdrożenia polityki ochrony danych osobowych* w zakresie niezbędnym do realizacji zadań służbowych.

(dowód: akta kontroli str. 5-37)

1.2. Wyznaczenie i działanie Inspektora Ochrony Danych

Zgodnie z art. 37 ust. 1 lit. a RODO, zarządzeniem z dnia 24 maja 2018 r. Prezydent Miasta Łodzi powołał IOD. IOD posiadał niezbędne kwalifikacje, wynikające z art. 37 ust. 5 RODO. Zarządzeniem z 24 maja 2018 r. ustalono także podstawowe zadania i obowiązki IOD.

Zastępcę IOD Prezydent Miasta Łodzi wyznaczył 16 lipca 2018 r.

(dowód: akta kontroli str. 57-59, 74-101)

W okresie objętym kontrolą IOD i jego zastępcą byli etatowymi pracownikami Urzędu. IOD zatrudniony był na stanowisku Dyrektora Biura Bezpieczeństwa Informacji i Ochrony Danych Osobowych, a Zastępca IOD na stanowisku p.o. Zastępcy Dyrektora Biura Bezpieczeństwa Informacji i Ochrony Danych Osobowych. Zgodnie z opisem stanowiska pracy, zadania wykonywane przez Dyrektora Biura Bezpieczeństwa Informacji i Ochrony Danych Osobowych nie obejmowały określania sposobu i celów przetwarzania danych i nie powodowały konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

(dowód: akta kontroli str. 60-94)

Zgodnie z art. 38 ust. 3 RODO, IOD podlegał najwyższemu kierownictwu Administratora danych osobowych, tj. Prezydentowi Miasta Łodzi.

(dowód: akta kontroli str. 57)

Aktualny kontakt do IOD i Zastępcy IOD podany był w ogólnodostępnych informacjach – m.in. na stronie internetowej Urzędu oraz na tablicach informacyjnych.

(dowód: akta kontroli str. 119-162, 1217-1219)

O wyznaczeniu IOD i jego zastępcy poinformowano Prezesa Urzędu Ochrony Danych Osobowych (UODO). W odniesieniu do IOD zawiadomienie przesłano 4 czerwca 2018 r., tj. z zachowaniem czternastodniowego terminu, ustalonego w art. 10 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych⁵. Dla Zastępcy IOD zawiadomienie przesłano 6 czerwca 2019 r., tj. 33 dni po wejściu

⁵ Dz. U. z 2019 r. poz. 1781.

w życie zmiany ustawy o ochronie danych osobowych, wprowadzającej taki obowiązek.

(dowód: akta kontroli str. 60-73)

W okresie objętym kontrolą nie było zmian na stanowiskach IOD i jego zastępcy.

(dowód: akta kontroli str. 57-59)

IOD realizował zadania określone w art. 39 RODO. Polegały one m.in. na:

- monitorowaniu zmian i przestrzegania przepisów dotyczących ochrony danych osobowych, polityk administratora i decyzji Prezesa UODO,
- udzielaniu komórkom organizacyjnym Urzędu odpowiedzi na pytania dotyczące ochrony danych,
- opracowaniu zakresów tematycznych i przeprowadzeniu szkoleń z zakresu ochrony danych osobowych, dostosowywanych do potrzeb pracowników Urzędu,
- prowadzeniu kontroli w komórkach organizacyjnych Urzędu.

(dowód: akta kontroli str. 57-58, 1232-1234)

1.3. Inne działania jednostki związane z wdrażaniem RODO

Zgodnie z art. 13 ust. 1 i 2 RODO oraz *Zarządzeniem w sprawie wdrożenia polityki ochrony danych osobowych* Administrator danych osobowych informował osoby wchodzące do Urzędu o przetwarzaniu ich danych osobowych. Stosowne powiadomienia w tym zakresie zawarte były m.in. w ogólnodostępnych pomieszczeniach, na stronie internetowej Urzędu, na wzorach dokumentów.

(dowód: akta kontroli str. 119-162, 1217-1219)

W Urzędzie nie prowadzono audytów i kontroli zewnętrznych dotyczących przygotowania do RODO.

(dowód: akta kontroli str. 1249)

W Urzędzie przeprowadzono szereg szkoleń z zakresu ochrony danych osobowych. Na przełomie 2018/2019 roku odbyło się szkolenie e-learningowe, w którym udział wzięli wszyscy obecni pracownicy Urzędu. Szkolenia dla nowych pracowników prowadzone były na bieżąco. Ponadto przeprowadzono osobne szkolenia m.in. dla grupy kierowniczej, grupy obsługującej media, radnych Rady Miejskiej w Łodzi, Zarządów Rad Osiedli oraz na indywidualne wnioski kierowników komórek organizacyjnych. Poruszana na szkoleniach problematyka dostosowana była do potrzeb uczestników szkoleń.

(dowód: akta kontroli str. 163-286, 1232-1233)

W związku z wdrażaniem RODO w Urzędzie poniesiono wydatki w kwocie 240,9 tys. zł. Środki te wykorzystano m.in. na:

- wynagrodzenia pracowników Biura Bezpieczeństwa Informacji i Ochrony Danych Osobowych, realizujących zadania w zakresie ochrony danych osobowych (101,2 tys. zł),
- szkolenia z zakresu RODO (80,1 tys. zł),
- zakup niszczarek i zamków (40,6 tys. zł),
- zabezpieczenie drzwi i okien (3,2 tys. zł).

Ponadto, jak wyjaśniła p.o. Dyrektora Wydziału Informatyki, w Urzędzie dokonywano zakupów sprzętu i oprogramowania, zwiększających poziom bezpieczeństwa systemów i infrastruktury teleinformatycznej. Jednak zakupów tych nie można powiązać wyłącznie z wdrażaniem RODO.

(dowód: akta kontroli str. 287-296, 1258)

Na Miasto Łódź nie zostały nałożone żadne kary pieniężne, inne sankcje lub obowiązki, zasadne w przypadku niewłaściwego stosowania przepisów RODO.

(dowód: akta kontroli str. 1249)

1.4. Nadzór nad podległymi jednostkami w obszarze stosowania RODO

We wszystkich 367 miejskich jednostkach organizacyjnych⁶ Miasta Łódź przyjęto, że administratorami danych osobowych będą kierownicy tych jednostek. Po wejściu w życie RODO jednostki te samodzielnie wdrożyły system ochrony danych osobowych i wyznaczyły inspektorów ochrony danych. Na podstawie przeglądu losowo wybranej próby 23 jednostek stwierdzono, że na ich stronach internetowych zostały zamieszczone klauzule informacyjne RODO.

(dowód: akta kontroli str. 296-336)

W ramach działań nadzorczych w okresie objętym kontrolą przeprowadzono w podległych jednostkach 18 kontroli dotyczących m.in. zabezpieczeń teleinformatycznych i fizycznych oraz ochrony osób i mienia.

Urząd także udzielał jednostkom merytorycznego i prawnego wsparcia.

(dowód: akta kontroli str. 337-481)

W kontrolowanym okresie do Urzędu nie wpłynęły skargi na podległe jednostki w zakresie przetwarzania danych osobowych.

(dowód: akta kontroli str. 1249)

Stwierdzone
nieprawidłowości

W działalności Urzędu w zakresie organizacji ochrony danych osobowych nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

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

OBSZAR

2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych

Opis stanu
faktycznego

2.1. Prowadzenie rejestrów wymaganych przepisami RODO

Prowadzony w Urzędzie *Rejestr czynności przetwarzania danych osobowych* zawierał wszystkie wymagane informacje, wymienione w art. 30 ust. 1 RODO. Rejestr ustalał kategorie danych wyłącznie w zakresie niezbędnym dla celów przetwarzania. Dla każdej wyszczególnionej w rejestrze czynności określono podstawę prawną przetwarzania danych oraz wskazano systemy przetwarzające. Rejestr ten był na bieżąco aktualizowany.

(dowód: akta kontroli str. 43-56, 484-702 1247-1249)

Prowadzony w Urzędzie *Rejestr kategorii czynności przetwarzania* zawierał wszystkie wymagane informacje, wymienione w art. 30 ust. 2 RODO. Rejestr ten był na bieżąco aktualizowany.

(dowód: akta kontroli str. 51-56, 703-784, 1247-1249)

2.2. Upoważnienia do przetwarzania danych

Zgodnie z wytycznymi określonymi w § 10 pkt 4 *Instrukcji postępowania przy przetwarzaniu danych osobowych*, w Urzędzie prowadzono *Ewidencję osób upoważnionych do przetwarzania danych osobowych*. W ewidencji tej ujęto aktualnych pracowników Urzędu oraz stażystów i praktykantów.

Kontrola zgodności zakresu upoważnień do przetwarzania danych osobowych wydanych wybranym pracownikom⁷, stażystom i praktykantom, z danymi przetwarzanymi przez nich w ramach wykonywanych obowiązków, nie wykazała rozbieżności.

(dowód: akta kontroli str. 785-910)

W wyniku badania 10 celowo dobranych umów zleceń, związanych z przetwarzaniem danych osobowych, ustalono, że we wszystkich przypadkach Administrator udzielił zleceniobiorcy upoważnienia do przetwarzania danych osobowych, stosownie do zakresu zleconego zadania.

⁶ Stan na 22 listopada 2019 r.

⁷ Do kontroli wybrano w sposób celowy wszystkich pracowników Wydziału Zdrowia i Spraw Społecznych i Wydziału Księgowości.

(dowód: akta kontroli str. 911-965, 1109-1189)

Po 25 maja 2018 r. w Urzędzie rozwiązano stosunek pracy z 424 osobami. Kontrola dostępu do systemów informatycznych dla 10 osób⁸, z którymi rozwiązano stosunek pracy, wykazała, że we wszystkich zbadanych przypadkach zablokowano dostęp do systemów najpóźniej z ostatnim dniem okresu zatrudnienia, tj. zgodnie z § 11 pkt 1 i 2 *Instrukcji zarządzania systemem informatycznym*.

(dowód: akta kontroli str. 975-996)

W *Instrukcji postępowania przy przetwarzaniu danych osobowych* ustalono zasady współpracy z podmiotami zewnętrznymi i zasady powierzania danych osobowych. Wskazano m.in., iż Miasto Łódź może powierzyć przetwarzanie danych osobowych wyłącznie podmiotowi zewnętrznemu, który przestrzega zasad ochrony danych osobowych, wynikających z przepisów prawa oraz daje rękojmię należytej ochrony powierzonych danych i wyłącznie w drodze umowy lub na podstawie przepisów prawa. Zawarta z podmiotem zewnętrznym umowa powierzenia czyni ten podmiot podmiotem przetwarzającym. Każdy podmiot przetwarzający zostaje wpisany do rejestru podmiotów przetwarzających, prowadzonego przez IOD.

(dowód: akta kontroli str. 5-37)

Analiza pięciu losowo wybranych umów powierzenia⁹ zawartych z podmiotami zewnętrznymi wykazała, że:

- w każdym przypadku Administrator zawarł z podmiotem przetwarzającym umowę powierzenia przetwarzania danych osobowych, zawierającą wszystkie elementy wymagane na podstawie art. 28 ust. 3 RODO oraz *Polityki ochrony danych osobowych*,
- w każdej z umów zawarto zapis, iż Administrator jest uprawniony do kontroli sposobu wykonania umowy przez przetwarzającego. W żadnym przypadku takiej kontroli nie przeprowadzono.

(dowód: akta kontroli str. 484-736)

IOD wyjaśnił m.in., że firmy, z którymi zawarto ww. umowy, od wielu lat utrzymują systemy i realizują zadania utrzymania bez występowania incydentów naruszenia ochrony danych. Zatem można stwierdzić, że zabezpieczenia stosowane przez firmy są adekwatne do ryzyka związanego z przetwarzaniem danych osobowych. IOD wskazała także, że *zdalny dostęp do systemu osób upoważnionych jest monitorowany na poziomie nawiązywania i zakończenia połączenia. Dodatkowo w systemach stosuje się mechanizmy kontroli dostępu do danych*.

(dowód: akta kontroli str. 1259-1260)

W kontrolowanym okresie Miasto Łódź wykonywało zadania podmiotu przetwarzającego. Zgodnie z art. 28 ust. 3 RODO przetwarzanie odbywało się na podstawie umów¹⁰ powierzenia przetwarzania danych osobowych, a także na podstawie przepisów ustaw¹¹. Analiza postanowień pięciu obowiązujących umów

⁸ Do kontroli wybrano w sposób celowy zwolnionych pracowników z Wydziału Zdrowia i Spraw Społecznych oraz Wydziału Księgowości.

⁹ Umowy: z 25 maja 2018 r. dotycząca usług utrzymania, rozwoju oprogramowania aplikacyjnego i asysty technicznej systemu, z 7 maja 2019 r. dotycząca nadzoru autorskiego dla systemu informatycznego wraz z dostarczeniem nowych wersji oprogramowania, z 1 lipca 2019 r. na dostosowanie do potrzeb zamawiającego systemu Łódzkiego Centrum Kontakt z Mieszkańcami oraz prace o charakterze utrzymaniowym, z 8 lipca 2019 r. dotycząca wykonania, wdrożenia i uruchomienia systemu, z 31 lipca 2019 r. na dostarczenie nowych wersji oprogramowania komputerowego Zintegrowanego Systemu Informatycznego oraz świadczenie usług asysty technicznej.

¹⁰ Umowa z dnia 14 sierpnia 2018 r. o wzajemnym przetwarzaniu danych osobowych z Krajowym Biurem Wyborczym, umowy dotyczące projektu realizowanego w ramach Programu Operacyjnego Infrastruktura i Środowisko na lata 2014-2020, umowy dotyczące wdrożenia rozwiązań wspierających zarządzanie finansami w Urzędzie i miejskich jednostkach organizacyjnych.

¹¹ Ustawy: z 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy (Dz. U. z 2019 r. poz. 1291 ze zm.), z 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz. U. z 2019 r. poz. 1390 ze zm.), z 20 czerwca 1997 r. - Prawo o ruchu drogowym (Dz. U. z 2018 r. poz. 1990 ze zm.), z 13 października 1995 r. - Prawo łowieckie (Dz. U. z 2018 r. poz. 2033 ze zm.).

powierzenia (z 23) wykazała, że w Urzędzie wywiązano się z obowiązków nałożonych na podmiot przetwarzający.

(dowód: akta kontroli str. 703-784)

Prowadzenie monitoringu wizyjnego w Urzędzie uregulowane zostało w *Instrukcji zarządzania systemem monitoringu wizyjnego w Urzędzie Miasta Łodzi*.

Stosownie do postanowień zawartych w art. 22² ustawy z dnia 26 czerwca 1974 r. - kodeks pracy¹², monitoring nie obejmował pomieszczeń wskazanych w tym przepisie. Kamery były prawidłowo oznakowane, zaś przy wejściach do Urzędu rozmieszczono klauzule informacyjne dotyczące monitoringu. Nagrania z monitoringu były prawidłowo zabezpieczone i przechowywane przez okres wskazany w § 7 pkt 4 ww. instrukcji – maksymalnie przez 30 dni.

(dowód: akta kontroli str. 966-973)

2.3. Ochrona systemów informatycznych

Standardy zabezpieczeń serwerowni i węzłów sieci teleinformatycznej w Urzędzie zostały wskazane w *Instrukcji zarządzania systemem informatycznym* (§ 25).

(dowód: akta kontroli str. 5-36)

W serwerowniach zapewniono podtrzymanie zasilania oraz sprzyjające warunki środowiskowe pracy serwerów i urządzeń sieciowych. Zastosowane rozwiązania były zgodne z regulacjami wewnętrznymi.

(dowód: akta kontroli str. 1222-1223)

Zasady tworzenia i przechowywania kopii zapasowych danych określono w *Instrukcji zarządzania systemem informatycznym*. W Urzędzie ostatnie kopie wykonano i przechowywano zgodnie z tymi procedurami. Kopie znajdowały się w innych miejscach niż bazy danych, co minimalizowało ryzyko ich utraty.

(dowód: akta kontroli str. 5-36, 974)

Komputery Urzędu były zabezpieczone programem antywirusowym, zgodnie z *Instrukcją zarządzania systemem informatycznym* (§ 20 - § 22). Ponadto w Urzędzie stosowano zabezpieczenia na styku sieci lokalnej z siecią Internet.

(dowód: akta kontroli str. 5-36)

W systemach informatycznych Urzędu w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem wprowadzono zabezpieczenia polegające na konieczności logowania się do systemu (identyfikator i hasło). Wymogi dotyczące złożoności haseł zostały określone w *Instrukcji zarządzania systemem informatycznym*. W dokumencie tym wskazano m.in. wymagania dla haseł użytkowników (§ 15 pkt 2). Tego rodzaju wymagania zostały centralnie wprowadzone w ustawieniach systemu umożliwiającego uruchomienie komputerów Urzędu.

(dowód: akta kontroli str. 5-36)

W wyniku kontroli 10 losowo wybranych stanowisk komputerowych pod kątem stosowanych przez użytkowników haseł dostępu oraz procedury zawieszania pracy ustalono, że:

- celem uruchomienia komputerów wszyscy pracownicy wprowadzali hasła spełniające wymogi w zakresie liczby znaków,
- ośmiu pracowników logowało się do kolejnych systemów, wykorzystywanych na danych stanowiskach pracy. Pracownicy ci wprowadzili hasła spełniające wymogi w zakresie liczby znaków. We wszystkich systemach wprowadzono ustawienia wymuszające wprowadzenie haseł zgodnych z wymogami określonymi w *Instrukcji zarządzania systemem informatycznym*,
- wszyscy pracownicy potrafili uruchomić wygaszacz ekranu z opcją ochrony hasłem, stosowanie do § 16 pkt 4 ww. instrukcji.

(dowód: akta kontroli str. 1220-1221)

¹² Dz.U. z 2019 r. poz. 1040 ze zm.

Stwierdzone
nieprawidłowości

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

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działania Prezydenta Miasta Łodzi w zakresie wykorzystywania wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych.

OBSZAR

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

Opis stanu
faktycznego

3.1. Postępowanie w przypadku naruszenia ochrony danych osobowych

W okresie objętym kontrolą w Urzędzie zidentyfikowano piętnaście przypadków naruszenia ochrony danych osobowych. W przypadku czternastu naruszeń, po przeprowadzeniu oceny skutków naruszenia, stwierdzono brak przesłanek do przekazania informacji do Prezesa UODO. Jeden przypadek, dotyczący zaginięcia w niewyjaśnionych okolicznościach koperty zawierającej nieodebrany dowód osobisty oraz wniosek o jego wydanie, został zgłoszony do Prezesa UODO, z zachowaniem terminu określonego w art. 33 ust. 1 RODO. O naruszeniu zawiadomiono osobę, której dane dotyczyły. Zawiadomienie spełniało wymogi określone w art. 34 ust. 2 RODO.

(dowód: akta kontroli str. 1015-1091)

3.2. Postępowanie z danymi osobowymi

W kontrolowanym okresie do Urzędu wpłynęło 13 wniosków dotyczących: prawa dostępu (4), ograniczenia (1), usunięcia (7) i sprostowania (1) danych osobowych. Osiem wniosków zostało rozpatrzonych pozytywnie, jeden był w trakcie rozpatrywania. Trzy wnioski o usunięcie danych osobowych zostały rozpatrzone negatywnie, m.in. z uwagi na brak technicznych możliwości realizacji żądania. Jeden wniosek, dotyczący dostępu do danych, pozostawiono bez rozpatrzenia, ze względu na brak uzupełnienia wniosku przez wnioskodawcę.

(dowód: akta kontroli str. 1092)

W ogólnodostępnych miejscach w budynku Urzędu nie znajdowały się informacje, które mogą naruszać ochronę danych osobowych osób fizycznych.

(dowód: akta kontroli str. 1217-1219)

Administrator uregulował zasady niszczenia dokumentów papierowych, a także usuwania informacji znajdujących się na sprzętach i nośnikach zewnętrznych.

W *Instrukcji zarządzania systemem informatycznym* wskazano m.in., że nośniki danych oraz wydruki z danymi osobowymi, które są przeznaczone do zniszczenia, powinny być niezwłocznie zniszczone w sposób uniemożliwiający ich odczytanie, tj. w niszcarkach (§ 19 pkt 2-3).

W *Instrukcji zarządzania systemem informatycznym* przewidziano także wymontowanie dysków w przypadku napraw zewnętrznych sprzętu (§ 19 pkt 4-8). W kontrolowanym okresie nie było napraw zewnętrznych sprzętu.

W okresie objętym kontrolą w Urzędzie przeprowadzono jedną likwidację nośników danych (113 dysków HDD). Analiza protokołu likwidacji wykazała, iż likwidacji dokonano komisyjnie, zgodnie z obowiązującymi w tym zakresie uregulowaniami.

(dowód: akta kontroli str. 5-36, 1093-1101)

3.3. Ochrona danych osobowych pracowników

Po wejściu w życie RODO pracodawca, jako Administrator danych osobowych, powiadomił wszystkich pracowników Urzędu o przetwarzaniu ich danych osobowych. Informacje w tym zakresie, zawierające elementy wymagane na podstawie art. 13 ust. 1 i 2 RODO, zostały udostępnione dla wszystkich pracowników w Intranecie, w zakładce *Dla pracownika*. Pracownicy pisemnie potwierdzili zapoznanie się z klauzulą.

(dowód: akta kontroli str. 1102-1108)

Obowiązku informacyjnego z art. 13 RODO dopełniono także w przypadku zawierania umów cywilnoprawnych¹³. Ustaleń dokonano na podstawie badania losowo wybranych dziesięciu umów cywilnoprawnych.

(dowód: akta kontroli str. 911-965)

Obowiązek informacyjny z art. 13 RODO spełniono również przy rekrutacji pracowników.

W zarządzeniu Prezydenta Miasta Łodzi w sprawie procedury naboru kandydatów na wolne stanowiska urzędnicze wskazano m.in., że dokumenty złożone w związku z naborem przez kandydata wybranego w naborze są dołączane do jego akt osobowych. Dokumenty pozostałych kandydatów przechowuje się 3 miesiące.

IOD wyjaśnił m.in., że przyjęcie trzymiesięcznego okresu przechowywania informacji o kandydatach znajduje swoje uzasadnienie w art. 15 ust. 3 ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych¹⁴, który stanowi, że jeżeli w ciągu 3 miesięcy od dnia nawiązania stosunku pracy z osobą wyłonioną w drodze naboru istnieje konieczność ponownego obsadzenia tego samego stanowiska, możliwe jest zatrudnienie na tym samym stanowisku innej osoby spośród kandydatów /.../.

(dowód: akta kontroli str. 1215-1216, 1249-1250, 1266-1267)

Stwierdzone
nieprawidłowości

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

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie zarządzania danymi osobowymi przetwarzanymi, w tym gromadzonymi, w jednostce.

IV. Uwagi i wnioski

W związku z niestwierdzeniem nieprawidłowości Najwyższa Izba Kontroli nie formułuje uwag ani wniosków.

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 Delegatury NIK w Łodzi. 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.

Łódź, dnia 27 grudnia 2019 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi

Kontroler
Katarzyna Marciniak
starszy inspektor kontroli państwowej

Dyrektor
Przemysław Szewczyk


podpis


podpis

¹³ Z wyjątkiem pracowników, którzy posiadali już te informacje – zastosowano art. 13 ust. 4 RODO.

¹⁴ Dz.U. 2019 r. poz. 1282.