NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.018.03.2019

Paweł Osiewała
Prezydent Miasta Sieradza
Urząd Miasta Sieradza
Plac Wojewódzki 1, 98-200 Sieradz

WYSTĄPIENIE POKONTROLNE

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

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 Sieradza, Plac Wojewódzki 1, 98-200 Sieradz (dalej: Urząd).
Kierownik jednostki kontrolowanej	Paweł Osiewała, Prezydent Miasta Sieradza od 8 grudnia 2014 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	Emilia Wyciszkiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LLO/174/2019 z dnia 2 września 2019 r.

(Dowód: 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 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 była prowadzona efektywnie i zgodnie z wymogami określonymi w RODO. W wyniku kontroli stwierdzono jednak nieprawidłowości polegające na niestosowaniu zasad ustalonych w wewnętrznych procedurach bezpieczeństwa.

Uzasadnienie oceny ogólnej

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 Sieradza 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, z wyjątkiem aktualizacji wymaganego procedurami wewnętrznymi *Rejestru podmiotów przetwarzających dane osobowe*. Rejestr ten prowadzony był nierzetelnie, bowiem ujęto w nim zaledwie 32% umów zawartych z podmiotami przetwarzającymi dane osobowe na polecenie Administratora. W trakcie kontroli rejestr został zaktualizowany. Pozostałe rejestry, tj. *Rejestr czynności przetwarzania danych osobowych*, *Rejestr kategorii czynności przetwarzania danych* i *Rejestr incydentów i naruszeń ochrony danych osobowych* prowadzone były zgodnie z wymogami RODO.

Gmina Miasto Sieradz zapewniła zaprojektowanie i wdrożenie systemu przetwarzania i zabezpieczania danych osobowych we wszystkich miejskich jednostkach organizacyjnych Gminy Miasta Sieradz. W kontrolowanym okresie w Urzędzie i miejskich jednostkach organizacyjnych nie stwierdzono przypadków naruszenia danych osobowych.

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

W Urzędzie sporządzano i weryfikowano prawidłowość kopii zapasowych. Celem zapewnienia ciągłości pracy kopie zapasowe przechowywano poza miejscem ich wytwarzania. Wszystkie komputery zostały zabezpieczone przed szkodliwym oprogramowaniem oraz dostępem z zewnątrz.

W wyniku kontroli stwierdzono nieprawidłowości polegające na niespełnianiu wymagań w zakresie złożoności haseł przez dwa systemy informatyczne, co było niezgodne z obowiązującą w Urzędzie *Instrukcją zarządzania systemem informatycznym*. Prezydent Miasta Sieradza zapowiedział dostosowanie tych systemów do wymogów określonych w procedurach wewnętrznych.

---

[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.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[4] kontrolowanej działalności

OBSZAR

1. Organizacja ochrony danych osobowych w jednostce

Opis stanu faktycznego

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. Szacowanie to zostało przeprowadzone na zlecenie Prezydenta Miasta Sieradza przez firmę zewnętrzną, której powierzono zaprojektowanie i wdrożenie systemu zarzadzania bezpieczeństwem informacji oraz systemu przetwarzania i zabezpieczenia danych osobowych. Wyniki szacowania przedstawiono w raporcie z dnia 7 czerwca 2018 r., zawierającym m.in. opis postępowania z ryzykiem oraz zalecenia i wnioski.

We wnioskach wskazano m.in.: na brak klauzul powierzenia w niektórych umowach, brak zasad oraz ograniczeń w zakresie nośników danych i dostępnych stron internetowych, brak okresowych szkoleń pracowników w zakresie bezpieczeństwa informacji.

Zalecone w raporcie działania korygujące w zakresie ww. niezgodności zostały wprowadzone poprzez zawarcie stosownych umów powierzenia, przyjęcie zaktualizowanej dokumentacji bezpieczeństwa, wdrożenie systemu nadzorującego komputery oraz przeprowadzenie szkoleń.

(dowód: akta kontroli str. 8-15, 64-118, 236-287, 291-300, 612-681)

W Urzędzie zaktualizowano dokumentację z zakresu ochrony danych osobowych. Zarządzeniem z dnia 21 czerwca 2018 r. Prezydent Miasta Sieradza wprowadził do stosowania dokumentację *Systemu Zarządzania Bezpieczeństwem Informacji*, zawierającą m.in. *Politykę bezpieczeństwa informacji, Politykę bezpieczeństwa danych osobowych, Instrukcję zarządzania systemem informatycznym, Procedurę zarządzania incydentami*. Dokumentacja ta uwzględniała wymogi RODO.

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. 16-149)

Zatwierdzony przez Prezydenta Miasta Sieradza *System Zarządzania Bezpieczeństwem Informacji* został udostępniony za pośrednictwem poczty elektronicznej wszystkim pracownikom Urzędu, nie tylko osobom odpowiedzialnym za realizację poszczególnych czynności wymaganych tymi dokumentami.

(dowód: akta kontroli str. 150)

1.2. Wyznaczenie i działanie Inspektora Ochrony Danych

Zgodnie z art. 37 ust. 1 lit. a RODO, zarządzeniem z dnia 4 czerwca 2018 r. Prezydent Miasta Sieradza powołał Inspektora Ochrony Danych („IOD"). IOD posiadał niezbędne kwalifikacje, wynikające z art. 37 ust. 5 RODO. Poprzednio pełnił w Urzędzie funkcję Administratora Bezpieczeństwa Informacji.

Zarządzeniem z dnia 4 czerwca 2018 r. wyznaczono także podstawowe zadania i obowiązki IOD oraz jego zastępcę.

(dowód: akta kontroli str. 16-18, 151-199)

W okresie objętym kontrolą IOD i jego zastępca byli etatowymi pracownikami Urzędu. IOD zatrudniony był na samodzielnym stanowisku do spraw audytu i kontroli, a zastępca IOD na stanowisku inspektora w *Zespole do spraw Informatyki*.

---

[4] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

Zadania wykonywane w ramach umowy o pracę nie powodowały konfliktu interesów, o których mowa w art. 38 ust. 6 RODO.

(dowód: akta kontroli str. 151-156, 200)

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

(dowód: akta kontroli str. 151-156)

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

(dowód: akta kontroli str. 201-203)

O wyznaczeniu IOD i jego zastępcy poinformowano Prezesa Urzędu Ochrony Danych Osobowych. W odniesieniu do IOD zawiadomienie przesłano 12 czerwca 2018 r., tj. z zachowaniem czternastodniowego terminu, ustalonego w art. 10 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[5]. Dla zastępcy IOD zawiadomienie przesłano 20 maja 2019 r., tj. 16 dni po wejściu w życie zmiany ustawy o ochronie danych osobowych, wprowadzającej taki obowiązek (art. 11a ust. 3).

(dowód: akta kontroli str. 157-163)

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

(dowód: akta kontroli str. 200)

IOD realizował zadania określone w art. 39 RODO. Polegały one m.in. na informowaniu Administratora oraz pracowników o obowiązkach, jakie w zakresie ochrony danych nakładają na nich przepisy prawa oraz polityki wewnętrzne, a także doradzaniu w sprawie ich stosowania. Ponadto prowadził szkolenia pracowników Urzędu w zakresie ochrony danych osobowych oraz pełnił funkcję punktu kontaktowego dla organu nadzorczego oraz osób, których dane były przetwarzane.
IOD sporządził *Samoocenę realizacji obowiązków w zakresie ochrony danych osobowych w Urzędzie Miasta Sieradza w okresie od 21 czerwca 2018 r. do 14 czerwca 2019 r.* Weryfikacji poddano 32 obszary ochrony danych, z których 26 zostało ocenionych pozytywnie. W sześciu przypadkach wstrzymano się od oceny, ponieważ jednostka nie prowadziła działań podlegających sprawdzeniu. Na podstawie przeprowadzonej samooceny stwierdzono, że przetwarzanie danych osobowych w Urzędzie odbywało się zgodnie z prawem, a środki techniczne i organizacyjne wdrożone w celu zapewnienia bezpieczeństwa przetwarzanym danym osobowym były odpowiednie do poziomu zagrożenia i zapewniały skuteczną ochronę danych.

(dowód: akta kontroli str. 791-834)

1.3. Inne działania jednostki związane z wdrażaniem RODO

Zgodnie z art. 13 ust. 1 i 2 RODO oraz *Polityką bezpieczeństwa danych osobowych* (pkt 3.6), 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. 201-203,204-234)

W związku z wejściem w życie RODO firma zewnętrzna, której zlecono zaprojektowanie i wdrożenie systemu zarzadzania bezpieczeństwem informacji oraz systemu przetwarzania i zabezpieczenia danych osobowych, dokonała w ramach zamówienia weryfikacji systemu teleinformatycznego Urzędu oraz stosowanych zasad zarządzania informacją. Wyniki i zalecenia przedstawione zostały w *Raporcie z szacowania ryzyka utraty bezpieczeństwa informacji* z dnia 7 czerwca 2018 r. Zalecenia zostały zrealizowane (opisano w punkcie 1 niniejszego wystąpienia pokontrolnego).

---

[5] Dz. U. z 2019 r. poz. 1781.

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

(dowód: akta kontroli str. 64-118, 235-287, 291-300, 612-681)

Wszyscy pracownicy Urzędu zostali przeszkoleni w dniach od 15 maja do 15 czerwca 2018 r. w zakresie bezpieczeństwa informacji i ochrony danych osobowych. Ramowy program szkolenia obejmował m.in. bezpieczeństwo informacji w oparciu o Normę ISO/IEC 27001:2013, wybrane przepisy ustawy o ochronie danych osobowych, zasady bezpieczeństwa informacji, ataki socjotechniczne, postępowanie z naruszeniami bezpieczeństwa informacji. Ponadto, w dniu 23 maja 2018 r. kierownictwo Urzędu wzięło udział w szkoleniu dotyczącym zmiany przepisów w zakresie ochrony danych osobowych. Szkolenia przeprowadziła firma zewnętrzna, której w ramach umowy na zaprojektowanie i wdrożenie systemu przetwarzania i zabezpieczenia danych osobowych zlecono także organizację ww. szkoleń.

Wszyscy pracownicy Urzędu przyjęci do pracy po dniu 15 czerwca 2018 r. zostali zapoznani przez IOD z przepisami dotyczącymi ochrony danych osobowych oraz dokumentacją *Systemu Zarządzania Bezpieczeństwem Informacji*.

(dowód: akta kontroli str. 236-287)

W związku z wdrażaniem RODO w Urzędzie poniesiono wydatki w kwocie 110,2 tys. zł. W ramach tych środków firma zewnętrzna zaprojektowała i wdrożyła w Urzędzie i 18 jednostkach budżetowych system zarządzania bezpieczeństwem informacji, system przetwarzania i zabezpieczenia danych osobowych oraz przeprowadziła szkolenia w tym zakresie (79,4 tys. zł). Ponadto dokonano modernizacji systemu back-office, zapewniając m.in. zautomatyzowaną inwentaryzację sprzętu komputerowego i oprogramowania, kontrolę Internetu, monitoring komputerów, drukarek i nośników USB (30,8 tys. zł).

(dowód: akta kontroli str. 287-300)

W kontrolowanym okresie nie odnotowano incydentów i naruszeń ochrony danych osobowych. Na Gminę Miasto Sieradz nie zostały nałożone żadne kary pieniężne, inne sankcje lub obowiązki, zasadne w przypadku niewłaściwego stosowania przepisów RODO.

(dowód: akta kontroli str. 149, 301-303)

1.4. Nadzór nad podległymi jednostkami w obszarze stosowania RODO

We wszystkich 18 miejskich jednostkach organizacyjnych Gminy Miasta Sieradz zaprojektowanie i wdrożenie systemu przetwarzania i zabezpieczania danych osobowych, mającego spełniać wymagania RODO, zostało wykonane 15 czerwca 2018 r. przez podmiot zewnętrzny, na zlecenie Prezydenta Miasta Sieradza. W ramach umowy z wykonawcą wszyscy pracownicy tych jednostek ukończyli szkolenie z zakresu bezpieczeństwa informacji i ochrony danych osobowych. Kadra kierownicza wzięła udział w szkoleniu dotyczącym zmiany przepisów w zakresie ochrony danych osobowych.

(dowód: akta kontroli str. 239-244, 278-287,304-366)

W każdej z ww. 18 jednostek ustanowiono administratora (daną jednostkę) i inspektora ochrony danych, a klauzule informacyjne RODO zostały zamieszczone na stronach internetowych tych jednostek. W 16 jednostkach organizacyjnych Gminy Miasta Sieradz inspektorem ochrony danych został IOD Urzędu Miasta Sieradza, wyznaczony do pełnienia tej funkcji na podstawie zarządzenia Prezydenta Miasta Sieradza z dnia 4 czerwca 2018 r. Pozostałe dwie jednostki (miejskie instytucje kultury[6]) wyznaczyły inspektora ochrony danych we własnym zakresie.

(dowód: akta kontroli str. 151-152, 324-366)

[6] Sieradzkie Centrum Kultury i Miejska Biblioteka Publiczna.

IOD wyjaśnił, iż działania nadzorcze Gminy Miasta Sieradz w stosunku do podległych jednostek polegały na monitorowaniu, czy przestrzegane są przepisy obowiązujące w zakresie ochrony danych, a także udzielania merytorycznego i prawnego wsparcia. Zadania te realizowane były przez wspólnego IOD.

(dowód: akta kontroli str. 366)

Dyrektorzy miejskich instytucji kultury, posiadających osobowość prawną, zostali poinformowani przez pracowników Urzędu o konieczności samodzielnego wdrożenia regulacji wynikających z RODO. Jednostki te po wejściu w życie RODO wdrożyły system ochrony danych i wyznaczyły inspektorów ochrony danych.

(dowód: akta kontroli str. 365-372)

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

(dowód: akta kontroli str. 373-376)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

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

OBSZAR

2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych

Opis stanu faktycznego

2.2. 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.

W wyniku kontroli nie stwierdzono okoliczności uzasadniających konieczność aktualizacji rejestru.

(dowód: akta kontroli str. 121-148, 301-303)

Prowadzony w Urzędzie *Rejestr kategorii czynności przetwarzania* zawierał wszystkie wymagane informacje, wymienione w art. 30 ust. 2 RODO. W kontrolowanym okresie dokonano jednej aktualizacji tego rejestru, w związku z powierzeniem przetwarzania danych osobowych przez Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Łodzi. W wyniku kontroli nie stwierdzono innych przesłanek uzasadniających konieczność aktualizacji rejestru.

(dowód: akta kontroli str. 119-120, 301-303, 377-450)

2.3. Upoważnienia do przetwarzania danych

Zgodnie z wytycznymi określonymi w punkcie 2.6 *Polityki bezpieczeństwa 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 pracownikom[7], stażystom i praktykantom, z danymi przetwarzanymi przez nich w ramach wykonywanych obowiązków służbowych, nie wykazała rozbieżności.

(dowód: akta kontroli str. 77, 89, 245-247, 451-524)

[7] Do kontroli wybrano w sposób celowy wszystkich pracowników Referatu Profilaktyki Zdrowotnej i Świadczeń Społecznych i Referatu Podatków i Opłat.

W wyniku badania 10 celowo dobranych umów zleceń, związanych z przetwarzaniem danych osobowych, ustalono, że we wszystkich przypadkach Administrator udzielił zleceniobiorcy stosownego upoważnienia.

(dowód: akta kontroli str. 525-575)

Do przetwarzania danych osobowych upoważniony został także m.in. cały skład Miejskiej Komisji Profilaktyki i Rozwiązywania Problemów Alkoholowych, powołanej zarządzeniem Prezydenta Miasta Sieradza z dnia 9 czerwca 2015 r.

(dowód: akta kontroli str. 576-587)

Po dniu 25 maja 2018 r. w Urzędzie rozwiązano stosunek pracy z siedmioma osobami, w tym jedna zmieniła zajmowane stanowisko. Osoba, która zmieniła stanowisko, zachowała dostęp jedynie do systemów informatycznych obsługiwanych na nowym stanowisku. Pozostałym osobom zablokowano dostęp do systemów najpóźniej z ostatnim dniem okresu zatrudnienia.

(dowód: akta kontroli str. 451-456, 588-599)

W *Polityce bezpieczeństwa danych osobowych* ustalono zasady współpracy z podmiotami zewnętrznymi i zasady powierzania danych osobowych (pkt 7). Wskazano m.in., iż Gmina Miasto Sieradz może powierzyć przetwarzanie danych osobowych innemu podmiotowi 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. 77-90)

Analiza siedmiu losowo wybranych umów 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 bezpieczeństwa 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,
- w *Rejestrze podmiotów przetwarzających* ujęto trzy z siedmiu objętych kontrolą umów powierzenia.

Ogółem, według stanu na dzień 2 września 2019 r., w ww. rejestrze ujęto 23 z 71 obowiązujących umów powierzenia.

(dowód: akta kontroli str. 600-683)

W kontrolowanym okresie nie przeprowadzono żadnej kontroli sposobu wykonania umowy powierzenia przez przetwarzającego dane osobowe. Jak wyjaśnił Prezydent Miasta Sieradza, nie skorzystano z takiego uprawnienia, z uwagi na brak przesłanek świadczących o możliwości braku realizacji przez którykolwiek z podmiotów obowiązków wynikających z umowy i przepisów w zakresie ochrony danych osobowych. Nadzór nad wywiązaniem się z zapisów umowy powierzenia przetwarzania danych realizowany był w ramach całościowego nadzoru nad prawidłowym wykonaniem umowy merytorycznej (głównej).

(dowód: akta kontroli str. 835-878)

W kontrolowanym okresie Gmina Miasto Sieradz wykonywała zadania podmiotu przetwarzającego. Zgodnie z art. 28 ust. 3 RODO przetwarzanie odbywało się na podstawie umów powierzenia[8] przetwarzania danych osobowych, a także na

[8] Umowa z 8 stycznia 2018 r. o dofinansowanie projektu współfinansowanego ze środków Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020, umowa z 8 grudnia 2018 r. dotycząca dostępu do danych Powiatowego Zasobu Geodezyjnego i Kartograficznego drogą elektroniczną, umowa z 16 sierpnia 2019 r. dotycząca realizacji programu „Czyste powietrze", obsługiwanego przez Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Łodzi.

podstawie przepisów ustaw[9] i wytycznych wskazujących dodatkowe obowiązki podmiotu przetwarzającego. Analiza postanowień wszystkich obowiązujących umów powierzenia (3) i ww. wytycznych (1) wykazała, że w Urzędzie wywiązano się z obowiązków nałożonych na podmiot przetwarzający.

(dowód: akta kontroli str. 119-120, 377-450)

W Urzędzie nie prowadzono monitoringu wizyjnego.

(dowód: akta kontroli str. 690)

2.4. Ochrona systemów informatycznych

W Urzędzie obowiązywała instrukcja zabezpieczania pomieszczeń oraz postępowania z kluczami[10]. Zgodnie z tą instrukcją budynek Urzędu był wyposażony w system alarmowy. Dostęp do budynku wymagał łącznego użycia kodów dostępu oraz tradycyjnych kluczy. W instrukcji ustalono także m.in. procedury otwierania/ zamykania Urzędu oraz poszczególnych pomieszczeń, przechowywania i dysponowania kluczami, wskazano zasady i osoby upoważnione do dostępu do pomieszczeń.

Budynek Urzędu był wyposażany w system alarmu pożaru i system oddymiania.

(dowód: akta kontroli str. 691-705)

W serwerowniach zapewniono podtrzymanie zasilania oraz sprzyjające warunki środowiskowe pracy serwerów i urządzeń sieciowych. Zastosowane rozwiązania zabezpieczały te pomieszczenia przed nieuprawnionym ujawnieniem informacji będących w posiadaniu Urzędu, modyfikacją, usunięciem lub ich zniszczeniem. Znajdujące się w jednej z serwerowni materiały łatwopalne zostały usunięte z tego pomieszczenia w trakcie kontroli.

(dowód: akta kontroli str. 706-712)

Zasady tworzenia i przechowywania kopii zapasowych danych określono w *Instrukcji zarządzania systemem informatycznym* (dalej także *Instrukcja*).

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. W przypadku niepowodzenia przy wykonywaniu kopii zapasowych, informatycy otrzymywali wiadomość elektroniczną informującą o takim fakcie.

Starszy informatyk wyjaśnił m.in., że kopie weryfikowano raz w tygodniu, poprzez rozpakowanie archiwum. Ostatnie sprawdzenie miało miejsce 23 września 2019 r. W tym dniu równocześnie przywrócono bazy danych programu księgowego, w związku z nieudaną aktualizacją do najnowszej wersji.

(dowód: akta kontroli str. 92-93, 707-714)

Komputery Urzędu były zabezpieczone programem antywirusowym. Ponadto w Urzędzie stosowano zabezpieczenia na styku sieci lokalnej z siecią Internet.

(dowód: akta kontroli str. 93, 707, 711-712, 781-787)

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., że hasła użytkowników mają długość minimum 8 znaków (pkt 3.3). Tego rodzaju wymagania zostały centralnie wprowadzone w ustawieniach systemu umożliwiającego uruchomienie komputerów Urzędu.

(dowód: akta kontroli str. 91-92, 590,591)

---

[9] 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), ustawy z 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2019 r. poz. 653 ze zm.), ustawy z 28 listopada 2014 r. Prawo o aktach stanu cywilnego (Dz. U. z 2018 r. poz. 2224 ze zm.), ustawy z 24 września 2010 r. o ewidencji ludności (Dz. U. z 2019 r. poz. 1397).

[10] Zarządzenie nr 167/2017 Prezydenta Miasta Sieradza z dnia 7 lipca 2017 r.

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 (minimum osiem),
- ośmiu pracowników logowało się do kolejnych dwóch systemów, wykorzystywanych na danych stanowiskach pracy. Pięciu z nich wprowadziło hasło spełniające wymogi w zakresie liczby znaków. Pozostałych trzech uruchomiło systemy po wpisaniu mniejszej niż wymagana liczby znaków - od jednego do sześciu. W obu systemach nie wprowadzono ustawień wymuszających wprowadzenie haseł zgodnych z wymogami *Instrukcji*.
- dwóch z dziesięciu pracowników potrafiło blokować stację roboczą. Pozostali nie znali kombinacji klawiszy służącej zawieszeniu pracy komputera, wskazanej do stosowania w punkcie 4.2 *Instrukcji*.

(dowód: akta kontroli str. 92, 715-719)

W *Instrukcji* ustanowiono także zasady umożliwiające bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość (pkt 11).

Użytkowany w Urzędzie sprzęt mobilny (telefony, laptopy), służący do przetwarzania informacji wymagających ochrony, był zabezpieczony w sposób uniemożliwiający dostęp osobom nieuprawnionym, zgodnie z *Instrukcją*.

(dowód: akta kontroli str. 95, 759-777)

Stwierdzone nieprawidłowości

W działalności Urzędu w obszarze wykorzystywania wdrożonych rozwiązań organizacyjnych w zakresie bezpieczeństwa danych osobowych, stwierdzono następujące nieprawidłowości:

1. Dwa z trzech skontrolowanych systemów komputerowych, zawierających dane osobowe, nie zapewniały stosowania metod uwierzytelniania zgodnych z wymogami określonymi w punktach 3.3 i 3.8 *Instrukcji zarządzania systemem informatycznym*. W obu systemach brak było bowiem odpowiednich ustawień w zakresie złożoności hasła (mała i duża litera oraz znak specjalny), liczby znaków (minimum osiem) oraz zmiany hasła co 30 dni. System służący do ewidencji opłat za gospodarowanie odpadami komunalnymi uruchamiał się po wprowadzeniu jednego znaku, zaś system do ewidencji m.in. dodatków mieszkaniowych i energetycznych oraz podatków i opłat lokalnych po wprowadzeniu sześciu znaków.

Prezydent Miasta Sieradza wyjaśnił m.in., iż brak mechanizmów wymuszania zmiany hasła i określenia wymagań dotyczących ich złożoności nie wpływa na bezpieczeństwo przetwarzanych danych, ponieważ w celu uzyskania dostępu do zasobów, na których znajduje się oprogramowanie oraz bazy danych niezbędne jest uwierzytelnienie się do systemu Windows. Wskazał ponadto, iż w 2018 r. podjęto decyzję o wymianie systemów budżetowo-podatkowych.

Zdaniem NIK tego rodzaju zabezpieczeń nie można uznać za wystarczające w świetle ustalonych w Urzędzie procedur bezpieczeństwa, szczególnie w sytuacji braku stosowania przez pracowników Urzędu ustalonych zasad zawieszenia pracy na stanowiskach komputerowych (opisano poniżej).

(dowód: akta kontroli str. 91-92, 590,591, 715-719)

2. Trzech z ośmiu skontrolowanych pracowników (37,5%) posiadających dostęp do ww. systemów posługiwało się hasłami dostępu niespełniającymi wymogów określonych punkcie 3.3 *Instrukcji zarządzania systemem informatycznym* w zakresie minimalnej liczby znaków. Ich hasła zawierały od jednego do sześciu znaków, zamiast co najmniej osiem znaków.

Dodatkowo ośmiu na 10 skontrolowanych pracowników (80%) nie potrafiło w żaden sposób blokować stacji roboczej, a tym samym nie stosowało procedur zawieszania pracy określonych w punkcie 4.2 *Instrukcji*. Zgodnie z tymi procedurami, podczas

zawieszenia pracy użytkownik powinien zablokować stację roboczą poprzez kombinację klawiszy (Windows + L).
Zastosowanie haseł o mniejszej liczbie znaków niż wymagana pracownicy wyjaśnili niedopatrzeniem. Wskazali także, iż program nie odrzucał ich poprawności.
Odnośnie braku umiejętności blokowania stacji roboczej pracownicy wyjaśnili m.in., że odchodząc od komputera czekali do czasu pojawienia się wygaszacza ekranu lub podczas pilnego odejścia wyłączali komputer. Równocześnie zapewnili, że znane im są procedury zawieszenia pracy, jednak podczas kontroli zapomnieli ich zastosowania.
W ocenie NIK powyższe działania pracowników były niezgodne z zasadami ustalonymi w wewnętrznych procedurach bezpieczeństwa.

(dowód: akta kontroli str. 91-92, 590,591, 715-719, 743-758)

3. Wymagany w Urzędzie na podstawie procedur wewnętrznych[11] *Rejestr podmiotów przetwarzających* prowadzony był nierzetelnie. Według stanu na dzień kontroli wpisano do niego zaledwie 32% umów zawartych z podmiotami, którym Administrator powierzył przetwarzanie danych osobowych, tj. 23 z 71 umów.
IOD wyjaśnił, iż przyczyną nieujęcia w rejestrze wszystkich przypadków powierzenia danych był m.in. niewłaściwy przepływ informacji pomiędzy koordynatorami ochrony danych, którzy nadzorują podpisanie umów, a IOD, który prowadzi rejestr. IOD wskazał także, iż z uwagi na informacyjny charakter rejestru, przyjął praktykę jego aktualizacji dwa razy w roku – na koniec każdego półrocza. Z uwagi na sezon urlopowy, aktualizację rozpoczęto we wrześniu.
Na dzień zakończenia kontroli rejestr został zaktualizowany.

(dowód: akta kontroli str. 600- 689)

OCENA CZĄSTKOWA

Dane osobowe były przetwarzane wyłącznie przez osoby posiadające stosowne upoważnienie w tym zakresie. W Urzędzie wdrożono odpowiednie środki techniczne i organizacyjne dla zapewnienia zdolności do szybkiego przywrócenia dostępności danych osobowych. W części skontrolowanych systemów nie dostosowano jednak zasad złożoności haseł. Prezydent Miasta Sieradza zapowiedział stosowne zmiany w tym zakresie.
Wymagane przepisami RODO rejestry, tj. *Rejestr czynności przetwarzania danych osobowych* i *Rejestr kategorii czynności przetwarzania* prowadzone były zgodnie z obowiązującymi przepisami prawa. Wymagany na podstawie procedur wewnętrznych *Rejestr podmiotów przetwarzających* prowadzony był nierzetelnie.

OBSZAR

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

Opis stanu faktycznego

3.1. Postępowanie w przypadku naruszenia ochrony danych osobowych
W kontrolowanym okresie w Urzędzie nie doszło do naruszenia ochrony danych osobowych.

(dowód: akta kontroli str. 149, 301-303)

3.2. Postępowanie z danymi osobowymi
Do Urzędu nie zgłoszono żądań dotyczących usunięcia, sprostowania, bądź uzupełnienia niekompletnych danych osobowych.

(dowód: akta kontroli str. 301-303)

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

(dowód: akta kontroli str. 6-7, 203)

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

[11] Na podstawie punktu 7.7 Polityki bezpieczeństwa danych osobowych.

W *Polityce bezpieczeństwa informacji* wskazano m.in., że dokumenty papierowe zawierające informacje muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści, tj. w niszczarkach (pkt 10).
W *Polityce bezpieczeństwa danych osobowych* ujęto zalecenia odnośnie danych nadmiarowych – dane takie powinny zostać zamazane (w sposób uniemożliwiający odtworzenie), zniszczone w niszczarce lub usunięte z komputera/poczty elektronicznej, w tym również z „kosza", odesłanie (pkt 4).
W *Instrukcji zarządzania systemem informatycznym* wskazano, że kopiowanie informacji objętych ochroną na nośniki wymienne powinno być realizowane wyłącznie w uzasadnionych przypadkach. W każdym przypadku należy zapewnić niezwłoczne usunięcie danych (pkt 6). W *Instrukcji* przewidziano także wymontowanie/formatowanie dysków w przypadku napraw zewnętrznych/utylizacji sprzętu (pkt 9).

(dowód: akta kontroli str. 73, 79, 93-94)

W kontrolowanym okresie w Urzędzie miała miejsce wymiana 31 komputerów. W wyłączonych z użytkowania komputerach wyczyszczono dyski twarde. Sprzęt stosownie zabezpieczono.

(dowód: akta kontroli str. 713, 720)

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 doręczone pracownikom na piśmie. Kopie informacji, potwierdzone podpisami pracowników, znajdowały się w ich aktach osobowych.

(dowód: akta kontroli str. 721-725, 788-790)

Obowiązku informacyjnego z art. 13 RODO dopełniono także przypadku zawierania umów cywilnoprawnych[12] oraz przy rekrutacji pracowników. Ustaleń dokonano na podstawie badania losowo wybranych siedmiu umów cywilnoprawnych oraz dwóch postępowań konkursowych.

(dowód: akta kontroli str. 203, 726-742)

W zarządzeniach Prezydenta Miasta Sieradza w sprawie naborów wskazano, iż dane osobowe kandydatów będą przechowywane *do ustania ich przydatności przez co najmniej okres 5 lat liczonych od dnia zakończenia procesu rekrutacji*. Okres ten był zgodny z terminem usunięcia danych, wskazanym w *Rejestrze czynności przetwarzania danych osobowych*.
Powyższy okres przechowywania wynikał z oznaczenia kategorii archiwalnej (B5 dla konkursów na stanowiska w urzędach), ujętej w załączniku nr 2 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[13].

(dowód: akta kontroli str. 139, 728-740, 788-790)

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 jednostce.

---

[12] Z wyjątkiem prawników, którzy posiadali już te informacje – zastosowano art. 13 ust. 4 RODO.
[13] Dz. U. z 2011 r. Nr 14 poz. 67 ze zm..

IV. Uwagi i wnioski

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

Wnioski

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

1. Dostosowanie parametrów haseł dostępu do wymogów systemu bezpieczeństwa informacji.
2. Stosowanie procedur zawieszenia pracy w systemach komputerowych.

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.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni 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.

Łódź, dnia 6 listopada 2019 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi

Kontroler
Emilia Wyciszkiewicz
główny specjalista kontroli państwowej

podpis

Dyrektor
Przemysław Szewczyk

podpis