NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP.410.006.03.2019

Pan
Krzysztof Kosiński
Prezydent Ciechanowa
Urząd Miasta Ciechanów
Plac Jana Pawła II 6, 06-400 Ciechanów

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 Ciechanów (dalej: Urząd)
Kierownik jednostki kontrolowanej	Krzysztof Kosiński, Prezydent Ciechanowa od 1 grudnia 2014 r. – dalej jako Prezydent lub Administrator.
Zakres przedmiotowy kontroli	1. Organizacja ochrony danych osobowych w jednostce. 2. Wykorzystywanie 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, tj. do 12 grudnia 2019 r. oraz dla zdarzeń wcześniejszych jeśli 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. Iwona Kasprzyk-Młynarczyk, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/80/2019 z 19.09.2019 r. 2. Krzysztof Stasiak, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr KAP/82/2019 z 26.09.2019 r. (akta kontroli str. 1-4)

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

II. Ocena ogólna kontrolowanej działalności[2]

OCENA OGÓLNA

W Urzędzie realizowano zadania zmierzające do wdrożenia przepisów 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.

Opracowane zostały nowe regulacje dotyczące ochrony i przetwarzania danych osobowych (m.in. *Polityka Ochrony Danych Osobowych w Urzędzie Miasta Ciechanów* (dalej: PODO)). Pracownik wyznaczony na stanowisko Inspektora Ochrony Danych (dalej IOD) posiadał odpowiednie kwalifikacje i realizował zadania określone w art. 39 ust. 1 RODO. Prezydent wywiązał się z obowiązku powiadomienia Prezesa Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO) o powołaniu IOD. Pracownicy Urzędu odbyli szkolenie z zakresu ochrony danych osobowych. W zależności od wykonywanych obowiązków, pracownicy posiadali wymagane upoważnienia do przetwarzania danych osobowych wydane przez Administratora.

Opracowano i przestrzegano procedur dotyczących zabezpieczeń technicznych i organizacyjnych. Monitoring wizyjny funkcjonował tylko w dozwolonych miejscach. Kontrola NIK nie stwierdziła przypadków ujawnienia danych osobowych w miejscach ogólnodostępnych Urzędu. Administrator, prawidłowo informował petentów i pracowników o przetwarzaniu ich danych osobowych.

Stwierdzone nieprawidłowości dotyczyły:
- nieujęcia w *Rejestrze czynności przetwarzania,* kompletnych informacji o zasobach Urzędu zawierających dane osobowe;
- sporządzenia *Rejestru kategorii czynności przetwarzania* po upływie ponad 18 miesięcy od wejścia w życie RODO, tj. w trakcie kontroli NIK;
- niejednolitego uregulowania w dwóch obowiązujących dokumentach wewnętrznych zagadnień dotyczących miejskiego monitoringu wizyjnego w Mieście Ciechanów;
- niedokonania przez Administratora wymaganego zgłoszenia do Prezesa UODO faktu naruszenia ochrony danych osobowych czterech osób fizycznych;
- niezamieszczenia informacji określonych w art. 13 ust. 1-3 RODO w ogłoszeniach o naborze na wolne stanowiska urzędnicze, ogłoszonych i przeprowadzonych w okresie objętym kontrolą.

Stwierdzono ponadto dwa przypadki niewydania kontrahentom upoważnień do przetwarzania danych osobowych oraz brak potwierdzenia przekazania klauzul o ochronie danych osobowych kontrahentom umów cywilnoprawnych.

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

OBSZAR

1. Organizacja ochrony danych osobowych w jednostce.

1.1 Przygotowanie dokumentacji wymaganej przepisami RODO.

Analizę ryzyka związanego z przetwarzaniem danych osobowych w Urzędzie w 2018 r. przeprowadził podmiot zewnętrzny, na podstawie umowy[5], której

---

[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., s. 1, ze zm..

[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.

[5] Umowa nr WZPI-ZP.272.3.337.2018 z dnia 17 kwietnia 2018 r .

przedmiotem były także usługi doradztwa prawnego z zakresu regulacji dotyczących ochrony danych osobowych, w tym określonych w RODO. Analiza ta została objęta kontrolą Prezesa UODO. W związku z wynikami tej kontroli[6], ponowna analiza ryzyka[7] została przeprowadzona przez IOD w dniu 23 lipca 2019 r. W zatwierdzonej 29 lipca 2019 r. ocenie ryzyka wskazane zostały sugerowane przez UODO działania minimalizujące zagrożenia dla ryzyk określonych na wysokim poziomie oraz termin realizacji tych działań i osoby odpowiedzialne. Działania korygujące zostały zaplanowane na 2020 r.

Z analizy arkusza oceny ryzyka oraz arkusza szacowania ryzyka dla przetwarzanych danych osobowych, wynikało, że do zasobów Urzędu podlegających ochronie przed zagrożeniami mającymi wpływ na bezpieczeństwo przetwarzanych danych osobowych, bez szczegółowego wyliczenia, zaliczono następujące grupy zasobów: procesy przetwarzania danych osobowych, dane osobowe, personel, sprzęt, oprogramowanie i aplikacje, sieć, siedziba, monitoring. Brak szczegółowego wyliczenia zasobów, nie pozwala na rozpoznanie wszystkich rodzajów zbiorów zawierających dane osobowe w Urzędzie.

Prezydent poinformował*, że w najbliższym czasie planowane jest przeprowadzenie powyższych czynności przy wykorzystaniu zakupionego oprogramowania.*

(akta kontroli str. 6-11, 210-230, 236-241, 282-287, 424-464, 665-670, 808-813, płyta nr 1 plik 6, 10 i 11)

Wraz z wejściem w życie RODO, w Urzędzie wprowadzono niżej wymienione uregulowania oraz rejestry dotyczące ochrony danych osobowych:

- PODO na podstawie zarządzenia Prezydenta Miasta Ciechanów nr 112/2018 z dnia 30 maja 2018 r.
- *Metodyka Szacowania Ryzyka dla danych osobowych przetwarzanych w Urzędzie Miasta Ciechanów*, zatwierdzona przez Prezydenta 1 lipca 2019 r.
- Zarządzenie Prezydenta Miasta Ciechanów nr 156/2019 z dnia 6 sierpnia 2019 r. w sprawie wprowadzenia i zatwierdzenia dokumentacji bezpieczeństwa systemu miejskiego monitoringu wizyjnego[8].
- *Instrukcja Zarządzania Zasobami Informatycznymi Urzędu Miasta Ciechanów* zatwierdzona przez Prezydenta 30 sierpnia 2019 r. (dalej: IZZI).
- *Rejestr czynności przetwarzania*, w formie pisemnej, w tym elektronicznej zgodnie z art. 30 ust. 1 RODO,
- *Rejestr naruszeń ochrony danych osobowych*, o którym mowa w art. 33 ust. 5 RODO.

Informacje o dokumentacji i zasadach dotyczących ochrony danych osobowych przekazywane są przez IOD kierownictwu Urzędu oraz kierownikom wydziałów i referatów podczas cyklicznych spotkań. Pracownicy mają również dostęp do aktualnej wersji dokumentów za pośrednictwem wydzielonej przestrzeni dyskowej w zasobach sieciowych Administratora. Ponadto pracownicy są zobowiązani do złożenia oświadczenia, że zostali zapoznani z przepisami

---

[6] Kontrola Prezesa UODO wykazała, m.in. naruszenie art. 24 ust. 1 art. 32 ust. 1 RODO poprzez nieprawidłowe opracowanie analizy ryzyka (nieujęcie w niej procesu przetwarzania danych osobowych w ramach miejskiego monitoringu miejskiego).

[7] Analizę ryzyka wykonano przy wykorzystaniu: arkusza szacowania ryzyka i arkusza oceny ryzyka stanowiących załączniki nr 3 i 4 do *Metodyki Szacowania Ryzyka dla danych osobowych przetwarzanych w Urzędzie Miasta Ciechanów*.

[8] W skład dokumentacji wchodzą: Polityka ochrony danych osobowych przetwarzanych w Systemie Miejskiego Monitoringu Wizyjnego, Instrukcja Zarządzania Systemem Miejskiego Monitoringu Wizyjnego, Regulamin Funkcjonowania stanowiska obserwacji Systemu Miejskiego Monitoringu Wizyjnego, Plan Systemu Miejskiego Monitoringu Wizyjnego.

o ochronie danych osobowych i zasadami przetwarzania i ochrony danych osobowych opisanych w PODO.

Kontrola wykazała, że opisana powyżej dokumentacja dotycząca przetwarzania i ochrony danych osobowych była przygotowywana i aktualizowana przez IOD. Prezydent wyjaśnił, że PODO podlega corocznym przeglądom i jest okresowo aktualizowana przez IOD (w badanym okresie aktualizacje dokonane zostały czterokrotnie - wszystkie w 2019 r.). W rozdziale III PODO zostało określone uprawnienie IOD do jej aktualizacji, jednak w dokumentacji wewnętrznej oraz w PODO nie został określony sposób dokonywania tych aktualizacji. IOD dokonuje tego w formie ręcznych poprawek na dokumencie, o których adnotacja znajduje się w arkuszu zmian i aktualizacji, a także w treści PODO.

Stwierdzono, że do dnia 9 grudnia 2019 r. nie prowadzono *Rejestru kategorii czynności*, o którym mowa w art. 30 ust. 2 RODO (opis w pkt 2.1 wystąpienia).

(akta kontroli str. 35-37, 51-131,149-241, 254-257, 259-263, 760-761, 841-846, 849-851, płyta nr 1 plik nr 1, 2,3 i 7)

1.2 Wyznaczenie i działanie Inspektora Ochrony Danych.

Zgodnie z art. 37 ust. 1 lit. a) RODO, zarządzeniem nr 108/2018 z dnia 24 maja 2018 r., Prezydent wyznaczył z dniem 25 maja 2018 r. pracownika Urzędu zatrudnionego w Referacie Bezpieczeństwa i Zarządzania Kryzysowego, na stanowisko IOD, równocześnie odwołując Administratora Bezpieczeństwa Informacji. W okresie objętym kontrolą nie zachodziły zmiany na tym stanowisku. W Urzędzie nie został powołany Zastępca IOD. Prezydent poinformował również, że na stanowisku IOD nie ma wyznaczonych zastępców na wypadek absencji IOD.

(akta kontroli str. 5, 35-37 i 330-331)

Informacja o powołaniu IOD została wysłana do UODO w wersji papierowej drogą pocztową 12 czerwca 2018 r., tj. cztery dni po terminie określonym w art. 10 ust. 1 ustawy z 10 maja 2018 r. o ochronie danych osobowych[9] (potwierdzenie odbioru przez UODO z 13 czerwca 2018 r.). W dniach 6 i 7 czerwca 2018 r. Prezydent podjął próbę przesłania do UODO drogą elektroniczną wspomnianego zawiadomienia na dedykowanej platformie BIZNES.GOV.PL. Jednak ze względu na trwające prace konserwacyjne przesłanie informacji drogą elektroniczną okazało się niemożliwe.

Prezydent wyjaśnił, że w związku z brakiem potwierdzenia odbioru zgłoszenia elektronicznego do godzin popołudniowych, w dniu 7 czerwca zostało przygotowane zgłoszenie w wersji papierowej, 8 czerwca 2018 r. korespondencja została przygotowana do wysyłki, lecz z uwagi na fakt dostarczenia pisma do wysyłki do Biura Podawczego po godzinie 14.30 (maksymalna godzina, do której należy złożyć pismo, aby zostało przekazane do wysłania tego samego dnia) pismo zostało zarejestrowane następnego dnia roboczego (tj. 11 czerwca 2018 r.) i w kolejnym dniu przekazane do wysłania tradycyjną drogą pocztową.

(akta kontroli str. 35-37, 332-345 i 792-793)

IOD jest pracownikiem Urzędu zatrudnionym na umowę o pracę na stanowisku Inspektora w Referacie Bezpieczeństwa i Zarządzania Kryzysowego. Ponadto powierzono mu następujące dodatkowe funkcje i zadania:

a) od 1 marca 2017 r. Pełnomocnik ds. ochrony informacji niejawnych,
b) od 8 maja 2018 r. Inspektor Bezpieczeństwa Teleinformatycznego,
c) od 21 maja 2018 r. operator drona.

[9] Dz.U. z 2018 r. poz. 1000, ze zm.

IOD prowadził m.in. także ewidencję służbowych nośników danych (pendrive). Wszystkie ww. zajęcia są wykonywane w ramach jednego etatu. Do czasu zakończenia kontroli, IOD w zakresie wszystkich wykonywanych przez siebie obowiązków, zgodnie z art. 38 ust. 3 RODO podlegał bezpośrednio Prezydentowi.
Prezydent wyjaśnił, że IOD prowadzi ww. sprawy, ze względu na brak pracowników posiadających odpowiednie kompetencje i kwalifikacje, a do chwili obecnej nie było żadnych negatywnych konsekwencji, wynikających z nałożenia na jedną osobę wskazanych funkcji.
Kontrola nie wykazała przypadków wskazujących na ryzyko konfliktu interesów. Zgodnie z art. 38 ust. 6 RODO, IOD może wykonywać inne zadania i obowiązki, jednakże to Administrator ma obowiązek zapewnienia, by ich wykonywanie nie powodowało konfliktu interesów.

(akta kontroli str. 346-365, 391-400, 420-423, 665-670, 686-692, 849-851, płyta nr 1 pliki 12-18)

Stosownie do art. 37 ust. 7 RODO dane kontaktowe do IOD podane były na stronie internetowej Urzędu[10] w dwóch miejscach:

- w zakładce Ochrona Danych Osobowych - Klauzule Informacyjne podany został adres email IOD,
- w zakładce Kontakt podane zostały imię i nazwisko IOD, telefon kontaktowy oraz adres email.

Ponadto adres email do IOD został podany w klauzulach informacyjnych o ochronie danych osobowych, które znajdują się w ogólnodostępnych miejscach w Urzędzie.

(akta kontroli str. 386-390, 401-419 i 665-670)

IOD posiadał kwalifikacje, o których mowa w art. 37 ust. 5 RODO, poparte odpowiednim wykształceniem (ukończył studia magisterskie na kierunku bezpieczeństwo wewnętrzne oraz studia podyplomowe z zakresu ochrony danych osobowych i informacji niejawnych), szkoleniami i kursami (m.in. z zastosowania RODO w gminnym systemie bezpieczeństwa, szacowania ryzyka i oceny skutków przetwarzania zgodnie z RODO, informacji publicznej w kontekście RODO, a także szkolenie nt. kontroli z UODO) oraz praktyką zawodową.

(akta kontroli str. 366-385)

Zgodnie z art. 39 ust. 1 RODO IOD informował Administratora, podmiot przetwarzający i pracowników o ich obowiązkach związanych z ochroną danych podczas organizowanych szkoleń i spotkań, a także poprzez zamieszczanie informacji i regulacji wewnętrznych w wydzielonej przestrzeni dyskowej. Informacje przekazywanie były ponadto na służbowe skrzynki pocztowe (email). W zakresie monitorowania przestrzegania RODO przeprowadził *analizę stanu faktycznego bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Ciechanów*[11], a także wskazywał o konieczności przestrzegania zasady tzw. „czystego biurka". Ponadto IOD udzielał instruktaży z zakresu działań dotyczących ochrony danych osobowych, co do oceny skutków tych działań oraz monitorował wykonanie tych zadań (np. w zakresie przetwarzania danych miejskiego monitoringu wizyjnego). IOD współpracował także z organem nadzorczym, biorąc udział w kontroli prowadzonej przez UODO oraz udzielając wyjaśnień w jej trakcie.

(akta kontroli str. 236-268, 281, 424-464, 665-670 i 686-692)

[10] Źródło: www.umciechanow.pl stan na 26 listopada 2019 r.

[11] Analiza przeprowadzona 16 sierpnia 2019 r., a jej wyniki przekazano tego samego dnia do informacji Prezydenta.

1.3 Inne działania jednostki związane z wdrażaniem RODO.

Na stronie internetowej Urzędu[12] w zakładce *Ochrona Danych Osobowych*, zamieszczone zostały informacje dotyczące ogólnej klauzuli informacyjnej ochrony danych osobowych, zawierającej elementy wskazane w art. 13 ust. 1 i ust. 2 RODO, a także klauzuli informacyjnej o ochronie danych osobowych dla Miejskiego Monitoringu Wizyjnego. Ponadto w zakładce *Polityka prywatności*, zostały wyjaśnione podstawowe pojęcia z zakresu ochrony danych osobowych oraz wskazane uprawnienia osób, których dane są przetwarzane.

W budynkach Urzędu nie było recepcji. Funkcjonowały dwa ogólnodostępne sekretariaty: jeden w budynku przy pl. Jana Pawła II 6 (sekretariat Prezydenta), oraz przy ul. Wodnej 1 (sekretariat Zastępcy Prezydenta oraz Sekretarza). W pomieszczeniach tych znajdowały się w widocznym miejscu ogólne klauzule informacyjne o ochronie danych osobowych.

(akta kontroli str. 12-25, 386-390, płyta nr 2)

W dniach od 26 do 30 listopada 2018 r. w Urzędzie została przeprowadzona przez Prezesa UODO, kontrola w sprawie przetwarzania danych osobowych przez Prezydenta Miasta Ciechanów. W jej efekcie Prezes UODO wszczął postępowanie[13] ws. nieprawidłowości, które zostały stwierdzone w trakcie kontroli. W wyniku przeprowadzonego postępowania Prezes UODO wydał decyzję[14] nakazującą usunięcie nieprawidłowości w procesie przetwarzania danych osobowych, polegających na:

1) nieprzeprowadzeniu oceny skutków dla ochrony i przetwarzania danych osobowych w ramach miejskiego monitoringu wizyjnego,
2) nieprawidłowym opracowaniu analizy ryzyka poprzez nieujęcie w niej procesu przetwarzania danych osobowych w ramach miejskiego monitoringu wizyjnego,
3) niezamieszczeniu przy wszystkich punktach kamerowych klauzul informacyjnych oraz nieprawidłowe wskazanie ich podstawy prawnej,
4) nieprawidłowym wskazaniu w klauzuli informacyjnej dotyczącej transmisji na żywo sesji rady miasta, jakie prawa przysługują uczestnikom obrad.

9 września 2019 r. do Urzędu wpłynęło pismo od Prezesa UODO[15], w którym potwierdził wykonanie zaleceń sformułowanych w decyzji.

W 2018 r. na zlecenie Prezydenta podmiot zewnętrzny[16],przeprowadził audyt którego efektem był raport z 24 maja 2018 r. pn.: *Audyt ochrona danych osobowych w świetle RODO - raport z audytu przeprowadzonego w Gminie Miejskiej Ciechanów – Urzędzie Miasta Ciechanów.* W raporcie sformułowane zostało łącznie 41 rekomendacji.

Kontrola NIK wykazała, że w Urzędzie nie zostały wdrożone rekomendacje wspomnianego audytu dotyczące: prowadzenia planu kontroli podmiotów przetwarzających dane osobowe na rzecz Administratora, wprowadzenia w pismach kierowanych do osób fizycznych informacji o przetwarzaniu danych osobowych oraz wzoru formularza dla obowiązku informacyjnego dla uczestników rekrutacji i osób, z którymi zawarto umowy cywilnoprawne. Nie wdrożono także mechanizmów kryptograficznej ochrony danych przesyłanych przez sieć publiczną oraz nie

[12] https://www.umciechanow.pl/samorzad/Ochrona_Danych_Osobowych, wg stanu na 26 listopada 2019 r.
[13] Pismo Prezesa UODO z dnia 15 marca 2019 r., znak ZSPU.421.9.2018.
[14] Decyzja UODO z dnia 27 maja 2019 r., znak ZSPU.421.9.2018.
[15] Pismo Prezesa UODO z dnia 6 września 2019 r., znak ZSPU.421.9.2018.
[16] Patrz przypis nr 5.

zaktualizowano wzoru skierowań na badania lekarskie z uwzględnieniem zasady minimalizacji danych (np. PESEL).

Prezydent wyjaśnił, że brak wprowadzenia poszczególnych rekomendacji w okresie objętym kontrolą wynikał w głównej mierze z braku możliwości fizycznych, technicznych i ograniczeń kadrowych, jednak zaznaczył, że w najbliższym czasie podjęte zostaną działania w celu ich realizacji.

W trakcie kontroli (25 listopada 2019 r.), Audytor wewnętrzny Urzędu, rozpoczęła czynności sprawdzające i doradcze w tym dotyczące problematyki ochrony danych osobowych, w ośmiu jednostkach podległych[17]. Do dnia zakończenia czynności kontrolnych audyt nie został zakończony.

(akta kontroli str. 282-287, 424-547, 783-789 płyta nr 1 plik nr 9)

W okresie objętym kontrolą pracownicy Urzędu uczestniczyli w szkoleniu z zakresu ochrony danych osobowych prowadzonym przez podmiot zewnętrzny[18]. W szkoleniu udział wzięło 87% pracowników Urzędu zatrudnionych w tym czasie. Pozostali pracownicy nie wzięli udział w szkoleniu ze względu na nieobecności w pracy spowodowane różnymi okolicznościami (m.in. urlopy i zwolnienia lekarskie).

Pracownicy nieobecni na szkoleniu w momencie otrzymywania upoważnienia do przetwarzania danych osobowych byli zobowiązani do złożenia oświadczenia o zapoznaniu z przepisami o ochronie danych osobowych, zasadami ich przetwarzania i ochrony zawartymi w PODO oraz z klauzulami informacyjnymi o przetwarzaniu danych osobowych stosowanych w Urzędzie.

W 2018 r. IOD przeprowadził szkolenie dla operatorów Systemu Miejskiego Monitoringu Wizyjnego oraz pracowników podmiotu zajmującego się serwisem opisywanego systemu, które było poświęcone omówieniu polityki miejskiego monitoringu wizyjnego.

W 2019 r. IOD przeprowadził dwa szkolenia dotyczące ochrony danych osobowych dla Straży Miejskiej w Ciechanowie[19], w których udział wzięli wszyscy pracownicy zatrudnieni w tym okresie.

(akta kontroli str. 236-241, 264-289, 420-423, 792-794 i 841-845)

W latach 2018 – 2019 na przygotowanie i realizację zadań związanych z ochroną danych osobowych w Urzędzie została wydatkowana łączna kwota 194,7 tys. zł. Środki te zostały wykorzystane na: usługi prawne w tym audyt i przygotowanie dokumentacji (12,3 tys. zł), zakupy sprzętu i oprogramowania informatycznego (131,6 tys. zł), szkolenie pracowników (11,9 tys. zł), zakup książek i prenumeratę periodyków branżowych (0,8 tys. zł), zakup licencji oprogramowania do analizy ryzyka (0,7 tys. zł), miesięczny dodatek za wykonywanie dodatkowych zadań IOD (10,5 tys. zł), zakup systemu do ewidencji czasu pracy (24,6 tys. zł) oraz refundację pierwszej raty studiów podyplomowych IOD w zakresie zarządzania bezpieczeństwem informacji (2,3 tys. zł).

(akta kontroli str. 288-329 i 686-692)

---

17 SP nr 1, SP nr 3, SP nr 4, SP nr 5, SP nr 6, SP nr 7, Centrum Usług Wspólnych, Miejska Biblioteka Publiczna.

18 Patrz przypis nr 5.

19 Dwa jednodniowe szkolenia pn.: *Zasady ochrony danych osobowych i bezpieczeństwa informacji* oraz *Co każdy pracownik powinien wiedzieć. Kontrola osobista oraz Polityka ochrony danych osobowych w Straży Miejskiej. Instrukcja zarządzania zasobami informatycznymi Urzędu Miasta Ciechanów.*

Prezydent poinformował, że w okresie od 25 maja 2018 r. do 25 listopada 2019 r. w Urzędzie nie było konieczności zapłaty kar pieniężnych oraz nie zastosowano innych sankcji związanych z niewłaściwym stosowaniem RODO.

(akta kontroli str. 236-241, 288-329 i 686-692)

1.4 Nadzór gminy nad podległymi jednostkami w obszarze stosowania RODO.

Gmina Ciechanów posiada 25 jednostek podległych[20]. Każda z jednostek powołała własnego IOD[21]. Analiza informacji zawartych na stronach internetowych poszczególnych jednostek[22], wykazała, że w ośmiu przypadkach nie było danych kontaktowych do IOD (jedna ze stron była nieaktywna)[23].

Prezydent wyjaśnił, że IOD Urzędu nie wykonywał jakichkolwiek czynności w jednostkach podległych. Administrator oraz IOD Urzędu nie weryfikowali oraz nie opiniowali regulacji wewnętrznych i procedur dotyczących ochrony danych osobowych w jednostkach podległych. Każda z jednostek to odrębny Administrator Danych Osobowych, który zgodnie z art. 4 pkt. 7 RODO decyduje (samodzielnie) o celach i środkach przetwarzania danych osobowych. Wyjaśnienia Prezydenta zostały poparte zestawieniem sporządzonym na podstawie danych przekazanych przez podległe jednostki.

W związku z wprowadzeniem RODO, w kwietniu 2018 r. zorganizowane zostało dla jednostek podległych instruktażowe spotkanie z podmiotem zewnętrznym[24], w zakresie zmiany przepisów w obszarze ochrony danych osobowych.

(akta kontroli str. 33-34, 236-241, 686-705, 761-773)

Analiza *Rejestru skarg i wniosków Urzędu Miasta Ciechanów* oraz *Rejestru Skarg do Rady Miasta Ciechanów* wykazała, że w badanym okresie do Urzędu nie wpłynęła żadna skarga na podległe i nadzorowane jednostki w zakresie przetwarzania danych osobowych.

UODO prowadzi postępowanie administracyjne (wszczęte 20 grudnia 2018 r.), dotyczące stosowania nieprawidłowych praktyk dotyczących przetwarzania danych osobowych za pośrednictwem urządzeń zainstalowanych na pojazdach Przedsiębiorstwa Usług Komunalnych w Ciechanowie. Ostatnie pismo w sprawie wpłynęło do Urzędu 14 lutego 2019 r. i zawierało informacje, że na podstawie zgromadzonego materiału dowodowego UODO wyda decyzję administracyjną.

Przekazana kontrolującym dokumentacja wskazuje, że do dnia 5 grudnia 2019 r., zarówno Prezydent jak i Prezes Zarządu Przedsiębiorstwa Usług Komunalnych w Ciechanowie nie otrzymali żadnych informacji na temat toczącego się postępowania.

(akta kontroli str. 38-50, 420-423, 706-727)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

Prezydent realizował zadania związane z przygotowaniem się do wdrożenia RODO. Opracowano dokumentację ochrony danych osobowych uwzględniającą przepisy

[20] 18 jednostek budżetowych, dwie instytucje kultury, pięć spółek z udziałem miasta.

[21] W czterech przypadkach był to pracownik danej jednostki, w czterech przypadkach funkcję te pełnił pracownik kancelarii doradztwa podatkowego, zaś w pozostałych 17 przypadkach funkcję IOD pełniły osoby fizyczne na podstawie zawartej umowy cywilnoprawnej.

[22] Stan na 3 grudnia 2019 r.

[23] SP nr 3 nie ma strony, Przedszkole nr 6 - strona niedostępna; SP nr 1, Przedszkole nr 3 i 4, Biblioteka, MOPS, Centrum Usług Wspólnych – brak danych IOD. Stan na dzień 3 grudnia 2019 r.

[24] Patrz przypis 5.

RODO, w tym *PODO.* Prawidłowo wyznaczono IOD. Pracownicy Urzędu zostali przeszkoleni w zakresie dotyczącym ochrony danych osobowych.
NIK zauważa przy tym, że zasadnym byłoby przeprowadzenie analizy ryzyka pozwalającej na szczegółowe zidentyfikowanie wszystkich zasobów zawierających dane osobowe.

OBSZAR

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

2.1 Prowadzenie rejestrów wymaganych przepisami RODO.

Kontrola wykazała, że *Rejestr czynności przetwarzania* w Urzędzie prowadzony od 30 maja 2018 r. został zaktualizowany w dniu 26 września 2019 r. Rejestr zawierał informacje, wymienione w art. 30 ust. 1 RODO. Zgodnie z danymi z rejestru Prezydent na podstawie powszechnie obowiązujących aktów prawnych wykonywał zadania administratora lub współadministratora w określonych przypadkach takich jak m.in: wydawanie dowodów osobistych, prowadzenie akt stanu cywilnego, ewidencja deklaracji opłat za gospodarowanie odpadami, ewidencja ludności.

Analiza *Kart informacyjnych* znajdujących się w *Rejestrze czynności przetwarzania* wykazała, że nie zawierał on kompletnych informacji o kategoriach danych osobowych, które są przetwarzane w Urzędzie (Szczegółowy opis w sekcji *Stwierdzone nieprawidłowości).*

Kontrola NIK wykazała, że do 9 grudnia 2019 r., w Urzędzie nie był prowadzony *Rejestr kategorii czynności przetwarzania*.
IOD stworzył *Rejestr kategorii czynności przetwarzania* w dniu 9 grudnia (po upływie ponad 18 miesięcy od wejścia w życie RODO). Rejestr zawierał elementy określone w art. 30 ust. 2 RODO (Szczegółowy opis w sekcji *Stwierdzone nieprawidłowości).*

Rejestry zawierały kategorie danych, które były adekwatne i określone wyłącznie w zakresie niezbędnym dla celów ich przetwarzania.

(akta kontroli str. 231-232, 841-851, płyta nr 1 plik 3)

2.2 Upoważnienia do przetwarzania danych.

W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych. W ewidencji tej ujęto aktualnych pracowników Urzędu, a także stażystów i praktykantów oraz osoby, z którymi zawarto umowy cywilnoprawne. Kontrola zgodności zakresu upoważnień do przetwarzania danych osobowych wydanych 25 pracownikom[25], z danymi przetwarzanymi przez nich w ramach wykonywanych obowiązków służbowych nie wykazała rozbieżności.

(akta kontroli str. 590-645 i 795-807)

Kontrola 10 umów zleceń zawartych w okresie objętym kontrolą i związanych z przetwarzaniem danych osobowych, wykazała że w dwóch przypadkach kontrahentom nie zostały wydane upoważnienia do przetwarzania danych osobowych oraz nie zostało złożone przez zleceniobiorcę oświadczenie dotyczące ochrony danych osobowych.
Prezydent wyjaśnił, że we wskazanych przypadkach omyłkowo nie wydano upoważnień w formie papierowej. Osoby upoważnione zostały jedynie na podstawie

[25] Do kontroli wybrano w sposób celowy wszystkich pracowników Urzędu Stanu Cywilnego, Wydziału Spraw Obywatelskich, Referatu ds. zatrudnienia, Z-cę Prezydenta Miasta, Sekretarza Miasta, Skarbnika Miasta, Kierowników wydziałów: Inżynierii Miejskiej i Utrzymania Infrastruktury Drogowej, Pozyskiwania Środków Zewnętrznych i Działań Strategicznych, Finansowo-Budżetowego, Organizacyjnego, Planowania Przestrzennego, Inwestycji. Kontrolą objęto również upoważnienia Komendanta Straży Miejskiej, jego Zastępcy oraz jednego strażnika miejskiego.

zawartych umów zlecenia, w których powierzono im wykonywanie konkretnych czynności oraz Prezydent ustnie upoważnił wskazane osoby.
NIK zauważa, że brak upoważnień w formie pisemnej może utrudnić wykazanie przez Administratora przestrzegania przepisów art. 5 ust. 1 i 2 RODO (zasada rozliczalności).

(akta kontroli str. 852-883, 891-897 i 1047-1057)

Kontrola 14 losowo wybranych kont dostępu do systemów teleinformatycznych byłych pracowników Urzędu oraz trzech osób, które zmieniły stanowisko w ramach struktur wewnętrznych wykazała, że konta byłych pracowników zostały zablokowane. Pracownikom zmieniającym miejsce zatrudnienia w ramach struktury wewnętrznej zostały zmienione zakresy uprawnień w związku z wykonywaniem nowych obowiązków. W przypadku zablokowanych kont byłych pracowników jedynie w 5 przypadkach istniała możliwość ustalenia ostatniej daty logowania do systemu (były to daty wcześniejsze niż rozwiązanie stosunku pracy), co było zgodne z uregulowaniami rozdziału V IZZI. W pozostałych przypadkach uzyskanie takich danych nie było możliwe, bowiem dane logowania znajdowały się w wygaszonym serwerze.

(akta kontroli str. 191-209, 646-662 i 795-807)

Analizą objęto 10 losowo wybranych umów powierzenia[26] (ogółem, w okresie objętym kontrolą zawarto 43 takie umowy) z podmiotami zewnętrznymi. Umowy objęte kontrolą dotyczyły takich kwestii jak: elektroniczna skrzynka podawcza, prowadzenie portalu *Wrota Mazowsza*, ewidencji miejscowości, ulic i adresów, obsługi monitoringu miejskiego, świadczenia usług hostingowych, usuwaniu azbestu z terenu gminy, profilaktyki oraz rozwiązywania problemów uzależnień, ochrony osób i mienia, systemu ewidencji ludności oraz rejestru wyborców.

Ww. analiza wykazała, że wszystkie zbadane umowy powierzenia, zawierają elementy wymagane art. 28 ust. 3 RODO. Umowy zostały ujęte w prowadzonym w Urzędzie *Rejestrze umów powierzenia danych osobowych, gdzie Gmina Miejska Ciechanów jest ADO.*

Umowy zawierały postanowienie o możliwości przeprowadzenia ich audytu/kontroli przez Administratora, jednak w okresie objętym kontrolą Administrator nie skorzystał z tego uprawnienia.

(akta kontroli str. 808-813, 949-1046, płyta nr 1-plik nr 4)

W związku z ochroną danych osobowych Prezydent wykonywał również zadania podmiotu przetwarzającego. Zgodnie z art. 28 ust. 3 RODO przetwarzanie odbywało się na podstawie umów powierzenia przetwarzania danych osobowych[27]. W Urzędzie wywiązywano się z obowiązków nałożonych tymi umowami w zakresie spraw związanych z ochroną danych osobowych.

(akta kontroli str. 849-851, 898-948, płyta nr 1-plik nr 5)

2.3 Prowadzenie monitoringu wizyjnego.

Monitoring wizyjny prowadzony był w Urzędzie na podstawie Zarządzenia nr 156/2019 Prezydenta Miasta Ciechanów z dnia 6 sierpnia 2019 r. w sprawie wprowadzenia i zatwierdzenia dokumentacji bezpieczeństwa Systemu Miejskiego Monitoringu Wizyjnego oraz na podstawie Polityki Systemu Miejskiego

[26] Umowy o znaku: IOD.142.1.WIMID.2.2019, IOD.142.1.M.1.2018, IOD.142.1.PU.9.2019, IOD.142.1.SM.1.2018, IOD.142.1.WO.2.2019, IOD.142.1.1.2018, IOD.142.1.WPPGN.1.2018, IOD.142.1.IMiOŚ.5.2018, IOD.142.1.WGOS.1.2019, IOD.142.1.WZPI.1.2018.

[27] Umowy powierzenia przetwarzania danych nr: IOD.142.2.WO.1.2018, IOD.142.1.2.WKS.1.2018, IOD.142.2.WO.2.2018, IOD.142.2.WIMID.1.2018, IOD.142.2.IMiOŚ.1.2018, IOD.142.2.FB.1.2018 IOD.142.2.IMiOŚ.2.2018,

Monitoringu Wizyjnego w Mieście Ciechanów, stanowiącej załącznik do PODO. W miejscach ogólnodostępnych umieszczone były piktogramy (rysunek kamery) z napisem „obiekt monitorowany", a także klauzule informacyjne. Zgodnie z art. 22^2 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy[28], monitoring nie obejmował pomieszczeń sanitarnych, szatni, czy innych obiektów socjalnych. Dostęp do nagrań miały wyłącznie osoby uprawnione. Dane zapisywane w systemie monitoringu przechowywane były – w zależności od ich wielkości – do nadpisania danych (ok 30 dni), nie dłużej niż 90 dni od dnia nagrania.

Stwierdzono, że zagadnienia dotyczące uregulowania zasad miejskiego monitoringu wizyjnego (16 kamer rozmieszczonych w mieście) do dnia zakończenia kontroli były niejednolicie uregulowane w dwóch jednocześnie obowiązujących dokumentach wewnętrznych, wprowadzonych w sierpniu 2019 r. i maju 2018 r. (Szczegółowy opis w sekcji *Stwierdzone nieprawidłowości).*

(akta kontroli str. 12-25, 132-190, 774-782 i 790-791)

2.4 Ochrona systemów informatycznych.

Zasady zabezpieczeń technicznych i organizacyjnych danych osobowych przetwarzanych w Urzędzie zostały określone w IZZI. Instrukcja określała m.in. mechanizmy zapewniające ciągłość działania zasobów, bezpieczeństwo fizyczne i środowiskowe, zasady zarządzania kopiami bezpieczeństwa, ochronę przed szkodliwym oprogramowaniem.

W serwerowniach Urzędu stworzone zostały warunki zapewniające właściwą pracę serwerów i urządzeń sieciowych, podtrzymanie zasilania i odpowiednią temperaturę oraz wilgotność powietrza. Znajdowały się w nich również czujniki dymu oraz sprzęt gaśniczy. Dostęp do pomieszczeń serwerowni możliwy był tylko w obecności pracowników zajmujących się procesami IT w Urzędzie.

Ustalono, że w pomieszczeniach serwerowni magazynowane były materiały łatwopalne. Uszkodzone były również zamki elektroniczne w drzwiach wejściowych do serwerowni. W trakcie kontroli łatwopalne materiały zostały usunięte, zaś uszkodzone zamki naprawione.

(dowód: akta kontroli str. 191-209 i 687-699)

Zasady dotyczące kopii bezpieczeństwa danych zostały określone w rozdziale XVI IZZI. Zgodnie z IZZI dane gromadzone w kopiach zapasowych mają zawierać dane osobowe oraz inne dane, które zostały wytworzone w toku pracy Urzędu oraz zapisane we współdzielonych dyskach sieciowych. Kopie zapasowe zapisywane były w oddzielnym serwerze, który znajduje się w innym pomieszczeniu niż nośniki z bazami, których są kopią. Kopie bezpieczeństwa były tworzone w sposób automatyczny zgodnie z *Harmonogramem tworzenia kopii bezpieczeństwa,* funkcjonującym w Urzędzie i w terminach w nim określonych.

(akta kontroli str. 191-209, 672-686, 696-699 i 795-807)

W celu zapewnienia właściwej ochrony przetwarzania informacji i zminimalizowania możliwości nieuprawnionego dostępu do zasobów informatycznych, w Urzędzie zostały wprowadzone zabezpieczenia polegające na zainstalowaniu programów antywirusowych zabezpieczających dostęp do serwera, poczty mailowej, komputerów pracowników (w tym przenośnych).

W Instrukcji IZZI, w rozdziale IX, zostały określone zasady dostępu pracowników do systemu informatycznego przy użyciu loginu oraz hasła dostępu, a także zasady przerw i zakończenia pracy w systemie.

(akta kontroli str. 191-209 i 696-699)

[28] Dz.U. z 2019 r. poz. 1040, ze zm.

Kontrola 11 stanowisk komputerowych (stacjonarnych)[29] pod kątem stosowanych przez użytkowników haseł dostępu oraz zawieszenia i zakończenia pracy w systemie, wykazała, że:

- sześciu pracowników (tj. 54% badanej próby) w celu uruchomienia komputerów i systemu używanego na danym stanowisku pracy, logowało się do systemu za pomocą hasła składającego się z mniejszej liczby znaków niż zostało to określone w procedurach.

Prezydent wyjaśnił, *że sytuacja ta była spowodowana wdrożeniem do działania nowego serwera i zmianą polityki haseł. 6 listopada została podjęta decyzja o natychmiastowym wymuszeniu zmiany haseł dla wszystkich pracowników Urzędu.*

Ponadto ustalono, że wszyscy pracownicy objęci badaniem potrafili zastosować odpowiednią kombinację klawiszy, służącą zabezpieczeniu danych wyświetlanych na ekranach komputerów, przed nieuprawnionym udostępnieniem.

(akta kontroli str. 191-209, 663-664 i 696-699)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Nieujęcie w prowadzonym *Rejestrze czynności przetwarzania* kompletnych informacji o kategoriach danych osobowych, które są przetwarzane w Urzędzie. Analiza wykazała, że *Rejestr* nie zawierał opisów czynności takich jak: prowadzenie rejestrów upoważnień do przetwarzania danych osobowych, zarządzeń, decyzji wydawanych przez Prezydenta Miasta Ciechanów; realizacji zadań audytowych, kontrolnych, zawierania i realizacji umów cywilnoprawnych; zasad dotyczących szkoleń pracowników, administrowania i nadawania uprawnień do pracy z systemami teleinformatycznymi.
Prezydent wyjaśnił, że *brak ujęcia wskazanych czynności wynika z tego, że pracownicy dostarczają uzupełnione i/lub brakujące karty informacyjne rejestru na podstawie swojej wiedzy w zakresie realizowanych czynności przez komórkę organizacyjną. Brak wskazanych procesów wynika z tego, że pracownicy błędnie sporządzili karty informacyjne lub ich nie wykonali. IOD nie posiada pełnej wiedzy dot. wszystkich procesów w Urzędzie i musi polegać wyłącznie na informacjach uzyskanych od pracowników. W najbliższym możliwym czasie zostanie przeprowadzony audyt, na podstawie którego między innymi możliwe będzie ustalenie i zweryfikowanie czynności przetwarzania w Urzędzie*.

W ocenie NIK nieujęcie kompletnych informacji o kategoriach danych osobowych przetwarzanych w Urzędzie oraz brak bieżącej aktualizacji rejestru jest działaniem nierzetelnym i nie pozwala zidentyfikować wszystkich zasobów informacyjnych zawierających dane osobowe.

2. Nieprowadzenie do dnia 9 grudnia 2019 r. *Rejestru kategorii czynności przetwarzania.* Prezydent wyjaśnił, że *Rejestr kategorii czynności przetwarzania* był prowadzony w formie rejestru umów powierzenia przetwarzania.
Kontrola NIK ustaliła, że rejestr umów powierzenia nie zawierał danych określonych w art. 30 ust. 2 RODO, w związku z czym nie można było go uznać za rejestr kategorii czynności przetwarzania.
Ze względu na fakt sporządzenia ww. rejestru w trakcie kontroli, NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

(akta kontroli str. 231-235, 841-851, płyta nr 1-plik nr 3)

[29] Losowo wybranych pracowników Biura Obsługi Interesanta, Referatu Bezpieczeństwa i Zarządzania Kryzysowego, Referatu ds. Zatrudnienia, Biura Rady Miasta, Referatu Gospodarki Odpadami, Referatu Utrzymania Infrastruktury Drogowej, Wydziału Podatków i Opłat oraz Wydziału Organizacyjnego.

3. Niejednolite uregulowanie w dwóch dokumentach wewnętrznych zagadnień dotyczących miejskiego monitoringu wizyjnego na terenie miasta Ciechanów.

Zagadnienia dotyczące monitoringu miejskiego zostały uregulowane Zarządzeniem Prezydenta Miasta Ciechanów nr 156/2019 z dnia 6 sierpnia 2019 r. w sprawie wprowadzenia i zatwierdzenia dokumentacji bezpieczeństwa systemu miejskiego monitoringu wizyjnego[30] . Uregulowania te odnosiły się do systemu monitoringu wizyjnego na terenie miasta Ciechanów (16 kamer znajdujących się w różnych punktach miasta).
Równocześnie system monitoringu wizyjnego (ww. 16 kamer rozmieszczonych na terenie miasta) był uregulowany w dokumencie *Polityka Miejskiego Monitoringu Wizyjnego w Mieście Ciechanów* zatwierdzonym przez Prezydenta 28 września 2018 r. Zagadnienia te były uregulowane odmiennie w obu dokumentach. Prezydent wprowadzając w 2019 r. zarządzenie nie uchylił obowiązujących w tym zakresie regulacji zawartych w Polityce z września 2018 r.
Prezydent wyjaśnił, że Polityka systemu miejskiego monitoringu wizyjnego z 2018 r., nie została dotychczas zaktualizowana, mimo wprowadzenia nowej polityki w sierpniu 2019 r.
Skutkowało to tym, że zagadnienia dotyczące monitoringu wizyjnego na terenie miasta Ciechanów - 16 kamer rozmieszczonych w różnych punktach miasta – do dnia zakończenia kontroli, były niejednolicie uregulowane w dwóch jednocześnie obowiązujących dokumentach wewnętrznych.

(akta kontroli str. 52-190 i 774-782)

OCENA CZĄSTKOWA W Urzędzie wdrożono przyjęte rozwiązania organizacyjne w zakresie ochrony danych osobowych. Pracownicy Urzędu posiadali wymagane upoważnienia, opracowano i przestrzegano procedur dotyczących zabezpieczeń technicznych i organizacyjnych, zaś monitoring wizyjny funkcjonował w miejscach dozwolonych. Wskazać jednak trzeba, że *Rejestr czynności przetwarzania* nie był kompletny, a *Rejestr kategorii czynności przetwarzania* został sporządzony w trakcie kontroli (po upływie ponad 18 miesięcy od wejścia w życie RODO). Nie sporządzono również jednolitych regulacji zagadnień dotyczących miejskiego monitoringu wizyjnego.

OBSZAR

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

3.1 Postępowanie w przypadku naruszenia ochrony danych osobowych.

W okresie objętym kontrolą cztery osoby fizyczne zgłosiły fakt naruszenia ochrony ich danych osobowych. Wszystkie związane były z nieprawidłowościami dotyczącymi głosowania w ramach budżetu obywatelskiego na 2020 r., przeprowadzonym w dniach od 3 do 27 września 2019 r. Do dnia zakończenia kontroli nie dokonano zgłoszenia naruszenia danych osobowych do UODO na podstawie art. 33 ust. 1 RODO (Szczegółowy opis w sekcji *Stwierdzone nieprawidłowości).*

(akta kontroli str. 420-423 i 728-761 i 841-845)

3.2 Postępowanie z danymi osobowymi.

Z analizy *Rejestru skarg i wniosków Urzędu Miasta Ciechanów* oraz *Rejestru naruszeń ochrony danych osobowych* oraz informacji przekazanych przez Prezydenta, wynikało, że według stanu na dzień 1 października 2019 r. do Urzędu nie wpłynęło żadne zgłoszenie dotyczące usunięcia danych osobowych, ich sprostowania, bądź uzupełnienia niekompletnych danych.

[30] Patrz przypis nr 8.

W ogólnodostępnych miejscach w budynkach Urzędu nie stwierdzono informacji, których upublicznianie mogłoby naruszać ochronę danych osobowych osób fizycznych. Przeprowadzone zostały oględziny wszystkich ogólnodostępnych pomieszczeń jednostek znajdujących się w strukturze organizacyjnej Urzędu (zlokalizowanych w sześciu miejscach na terenie Ciechanowa[31]). W trakcie oględzin sprawdzono informacje zamieszczone na tablicach w ogólnodostępnych miejscach (hole wejściowe, korytarze, klatki schodowe) oraz informacje zamieszczone w salach konferencyjnych i innych pomieszczeniach wykorzystywanych m.in. do zajęć grupowych w ramach działalności niektórych jednostek.

(akta kontroli str. 12-25, 35-49 i 760 płyta nr 2)

Zasady niszczenia danych na nośnikach elektronicznych zostały uregulowane w IZZI (rozdział XXII). W dokumencie tym wskazano m.in., że w odniesieniu do nośników przenośnych (pendrive) oraz nośników danych informatycznych przeznaczonych do złomowania stosowane są mechanizmy bezpiecznego kasowania informacji (za pomocą oprogramowania specjalistycznego, demagnetyzacji, fizyczne niszczenie nośników). Niszczenie nośnika zostaje odnotowane w protokole zniszczenia. Na podstawie przedłożonego protokołu zniszczenia danych na nośnikach[32] ustalono, że w okresie objętym kontrolą jeden raz dokonano zniszczenia danych w postaci 160 sztuk dysków twardych HDD i 36 sztuk taśm backupu.

W Urzędzie nie opracowano zasad dotyczących niszczenia dokumentów papierowych (trwają prace nad procedurą). Prezydent wyjaśnił, że dokumentacja wytwarzana w Urzędzie jest kwalifikowana na podstawie Jednolitego Rzeczowego Wykazu Akt z 2011 r. Po kwalifikacji zgodnej z wykazem, spisy dokumentacji, która straciła wartość użytkową dla Urzędu przekazywane są do Archiwum Państwowego. Po zaopiniowaniu spisów i wydaniu zgody, dokumenty zostają przekazane do zewnętrznej firmy w celu zniszczenia dokumentacji. Dokumentacja stanowiąca wartość archiwalną po 25 latach przekazywana jest na stan Archiwum Państwowego. Na podstawie sześciu protokołów zniszczenia danych w postaci dokumentów papierowych oraz trzech protokołów przekazania danych do Archiwum Państwowego (filia w Mławie), stwierdzono, że utylizacji dokumentów dokonywał wyspecjalizowany do tego podmiot, a z aktami przekazywanymi do Archiwum Państwowego postępowano w sposób wskazany przez Prezydenta.

Prezydent wyjaśnił ponadto, że dokumentacja papierowa zawierająca dane osobowe, wytworzona w ramach bieżącej pracy Urzędu, niszczona jest przy użyciu niszczarek. Niszczarki znajdują się w pokojach pracowników (przynajmniej jedna w pokoju).

(akta kontroli str. 191-209, 686-692 i 814-840)

3.3 Ochrona danych osobowych pracowników.

Na podstawie analizy akt osobowych 25 osób zatrudnionych w Urzędzie, ustalono, że pracodawca, jako Administrator danych osobowych powiadomił pracowników Urzędu o przetwarzaniu ich danych osobowych w związku z wejściem w życie w dniu 25 maja 2018 r. RODO. Pracownicy w momencie odbierania upoważnień do przetwarzania danych osobowych otrzymywali do zapoznania się dokumentację dotyczącą ochrony danych osobowych (w przypadku pracowników zatrudnionych po 25 maja 2018 r. odbywało się to w dniu rozpoczęcia przez nich pracy). Wszyscy

[31] Urząd Miasta przy ul. Wodnej 1, Urząd Miasta przy Placu Jana Pawła II 6, Park Nauki Torus przy ul. Płockiej 34, Biuro Profilaktyki i Rozwiązywania Problemów Uzależnień Budynek przy ul. Powstańców Wielkopolskich 1A, Pomieszczenie w budynku przy ul. 11 Pułku Ułanów Legionowych 25 – Monitoring Miejski, Straż Miejska przy Placu Jana Pawła II 7.

[32] Protokół z 12 grudnia 2018 r.

objęci kontrolą pracownicy złożyli pisemne oświadczenia o fakcie zapoznania się z przepisami i regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych. W pokojach pracowników oraz w miejscach ogólnodostępnych w Urzędzie znajdowały się również informacje dotyczące przetwarzania danych osobowych zawierające elementy określone w art. 13 ust. 1 i 2 RODO.

Ponadto pracownicy Urzędu mają możliwość zapoznania się z aktualnymi regulacjami w zakresie ochrony danych osobowych za pośrednictwem wydzielonej przestrzeni dyskowej w zasobach sieciowych Administratora.

(akta kontroli str. 12-24, 236-241, 256-257, 259-263, 401-419 i 590-645)

Kontrola losowo wybranych 10 umów cywilnoprawnych wykazała, że brak było potwierdzeń, dołączenia do nich klauzuli informacyjnej zawierającej elementy wskazane w art. 13 ust. 1 i 2 RODO. Prezydent wyjaśnił, *że do wszystkich umów cywilnoprawnych dołączone są klauzule informacyjne jako załącznik do egzemplarza przeznaczonego dla Zleceniobiorcy. Ponadto Zleceniobiorca otrzymuje do zapoznania klauzulę informacyjną w momencie podpisywania umowy.* NIK zauważa, że brak potwierdzenia przekazania kontrahentom klauzul informacyjnych zawierających informacje określone w art. 13 RODO, może utrudnić wykazanie przez Administratora przestrzegania przepisów art. 5 ust. 1 i 2 RODO (zasada rozliczalności).

(akta kontroli str. 420-423, 795-807, 841-845, 891-897 i 1047-1057)

W okresie objętym kontrolą przeprowadzono 45 postępowań rekrutacyjnych na stanowiska urzędnicze. Na podstawie analizy 15 zakończonych postępowań ustalono, że w sprawdzonych przypadkach, ogłoszenia o naborze na wolne stanowisko nie zawierały wszystkich informacji dotyczących prawa do przenoszenia danych oraz informacji o zautomatyzowanym przetwarzaniu danych określonych w art. 13 ust. 2 lit. b) i f) RODO oraz wskazanych w załączniku nr 7 do PODO. Ponadto stwierdzono, że obowiązujący *Regulamin naboru na wolne stanowiska urzędnicze*[33], na podstawie którego prowadzono postępowania rekrutacyjne nie zawierał informacji związanych z ochroną danych osobowych w związku z wejściem w życie przepisów RODO (Szczegółowy opis w sekcji *Stwierdzone nieprawidłowości).*

(akta kontroli str. 420-423, 548-589, 774-782, 808- 813, płyta nr 1-plik 19)

Zgodnie z postanowieniami rozdziału XI *Regulaminu naboru na wolne stanowiska urzędnicze*, dokumenty aplikacyjne kandydata, który zostanie wyłoniony w procesie rekrutacji zostają dołączone do jego akt osobowych. Okres przechowywania ofert osób, które przeszły ocenę formalną wynosił dwa lata w komórce zajmującej się sprawami pracowniczymi. Prezydent poinformował, że po tym okresie przekazywane były one do archiwum i po upływie pięciu lat przekazane do brakowania (co wynika z oznaczenia kategorii archiwalnej B5 dla konkursów na stanowiska w urzędach).

(akta kontroli str. 548-561, 795-807, płyta nr 1-plik 19)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Nieprzekazanie do UODO zgłoszenia naruszenia danych osobowych czterech osób fizycznych, które zgłosiły fakt naruszenia ich danych osobowych w związku z głosowaniem w ramach budżetu obywatelskiego na 2020 r.

[33] Zarządzenie Prezydenta Miasta Ciechanów nr 06/2009 z 14 stycznia 2009 r. w sprawie Regulaminu naboru na wolne stanowisko urzędnicze.

W dniach od 23 do 26 września 2019 r. cztery osoby poinformowały, że przy próbie oddania głosu otrzymały komunikat, że został już oddany głos z użyciem ich imienia, nazwiska i numeru PESEL mimo, że wcześniej nie głosowały.
Pracownik odpowiedzialny za sprawy budżetu obywatelskiego zawiadomił IOD o zaistniałej sytuacji. Dla każdego ze zgłoszeń został sporządzony raport z naruszenia danych (każdy ze zgłaszających potwierdził otrzymanie raportu). Stosownie do art. 34 i 12 RODO, Administrator poinformował również wszystkich zgłaszających o podejrzeniu naruszenia ich danych, przekazał im informację na które projekty został oddany głos i wskazał na konieczność zgłoszenia sprawy Policji. Równocześnie Administrator samodzielnie wystosował w tej sprawie pismo do KP Policji w Ciechanowie z prośbą o podjęcie czynności przewidzianych prawem (26 września 2019 r.).
Na podstawie umowy powierzenia przetwarzania danych osobowych z 31 stycznia 2019 r.[34], na podstawie której prowadzona była platforma do głosowania w ramach budżetu obywatelskiego, administratorem danych był Zamawiający czyli Gmina Miejska Ciechanów reprezentowana przez Prezydenta.
Prezydent wyjaśnił, *że z uwagi na okoliczności, zgłoszono sprawę do KP Policji w Ciechanowie, a całość postępowania wyjaśniającego prowadzona jest przez organ uprawniony, w tym weryfikacja pod kątem nieprawidłowości i nieuprawnionego wykorzystania danych osobowych. Nie dokonano zgłoszenia do UODO oraz nie ujęto go w rejestrze naruszeń danych osobowych, ponieważ w wyniku przeprowadzonej oceny, sytuacja nie miała charakteru naruszenia danych w zasobach administratora danych, z uwagi na to, że nie doszło do utraty poufności, integralności i dostępności danych. Urząd w zaistniałej sytuacji nie występuje jako strona, a jedynie jako świadek. Zaistniała sytuacja nie wynikła z zaniedbania czy też niedopatrzenia pracowników Urzędu oraz z niezastosowania odpowiednich środków techniczno-organizacyjnych. Urząd dołożył wszelkich starań aby głosowanie w ramach budżetu obywatelskiego było ogólnodostępne i zgodne z prawem, przy zachowaniu adekwatnych zabezpieczeń systemowych.*
Niezgłoszenie przez Administratora (Prezydent) faktu naruszenia ochrony danych osobowych, stanowi naruszenie art. 33 RODO, bowiem naruszenie poufności danych takich jak numer PESEL wraz z imieniem i nazwiskiem może skutkować naruszeniem praw i wolności osoby, której dane dotyczą.

(akta kontroli str. 728-761 i 841-845)

2. Niezamieszczanie w ogłoszeniach o wolnym stanowisku urzędniczym informacji o prawie do przenoszenia danych oraz informacji o zautomatyzowanym przetwarzaniu danych, określonych w art. 13 ust. 2 lit. b i f RODO oraz wskazanych w załączniku nr 7 do PODO.

Prezydent wyjaśnił, *że stwierdzone nieścisłości wynikają z braku kompleksowej aktualizacji Regulaminu naboru na wolne stanowiska pod kątem przepisów dotyczących ochrony danych osobowych. Zmiany we wspomnianym regulaminie zostaną wprowadzone w najbliższym możliwym terminie*.
Zdaniem NIK działanie Urzędu polegające na nieujęciu wszystkich informacji w ogłoszeniu było niezgodne z art. 13 ust. 2 lit. b) i f) RODO.

(akta kontroli str. 548-589, płyta nr 1-plik 19)

OCENA CZĄSTKOWA

Zarządzanie danymi osobowymi w Urzędzie na ogół było prowadzone zgodnie z RODO i regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych. W okresie objętym kontrolą do Urzędu nie wpływały wnioski o usunięcie lub sprostowanie zamieszczonych danych osobowych. Określone zostały i były przestrzegane zasady niszczenia danych osobowych znajdujących się na nośnikach

[34] Umowa nr IOD.142.1.WO.3.2019

elektronicznych. Wskazać jednak trzeba, że w okresie objętym kontrolą, Administrator nie wywiązał się z obowiązku dokonania zgłoszenia do UODO faktu naruszenia ochrony danych osobowych czterech osób, w związku z głosowaniem w ramach budżetu obywatelskiego na 2020 r. Ponadto w ogłoszeniach o prowadzonych naborach na wolne stanowisko urzędnicze nie umieszczano informacji określanych w art. 13 ust. 2 lit. b) i f) RODO. Brak też było uregulowań w zakresie niszczenia zbędnej dokumentacji papierowej (procedura jest w trakcie opracowywania), jednak w zakresie tym przestrzegano przepisów powszechnie obowiązujących i niszczenie danych odbywało się przez wyspecjalizowane w tym zakresie podmioty.

IV. Wnioski

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

Wnioski

1. Zaktualizować *Rejestr czynności przetwarzania* z uwzględnieniem wszystkich kategorii danych osobowych przetwarzanych w Urzędzie.
2. Uregulować w sposób jednolity zagadnienia dotyczące miejskiego monitoringu wizyjnego.
3. Zgłaszać naruszenia danych osobowych do UODO, w terminie określonym w art. 33 ust. 1 RODO.
4. Zamieszczać w ogłoszeniach o prowadzonych naborach na wolne stanowiska urzędnicze wszystkie informacje określone w art. 13 RODO.

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

Najwyższa Izba Kontroli
Departament Administracji Publicznej
Dyrektor
dr Bogdan Skwarka

.....
podpis

Krzysztof Stasiak
Starszy inspektor
kontroli państwowej

.....
podpis