NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ.410.021.04.2019

Pan Władysław Diakun
Burmistrz Polic

Urząd Miejski w Policach
Ul. Stefana Batorego 3
72-010 Police

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Policach[1],
Kierownik jednostki kontrolowanej	Władysław Diakun, Burmistrz Polic[2] od 19 listopada 1998 r.
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 23 października 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[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Szczecinie
Kontroler	Agata Prochotta - Miłek, specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/16/164/2019 z 23 września 2019 r. (akta kontroli str. 1-2, 3)

[1] Dalej: Urząd.
[2] Dalej: Burmistrz, lub Administrator.
[3] Dz. U. z 2019 r. poz. 489 ze zm., dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

W dniu wejścia w życie RODO[5], tj. 25 maja 2018 r., Urząd został organizacyjnie przygotowany do przetwarzania danych osobowych. Wymagane art. 30 ust. 1 oraz ust. 2 Rozporządzenia rejestry, w tym: czynności przetwarzania danych osobowych oraz kategorii czynności przetwarzania, Administrator zatwierdził 24 maja 2018 r. Burmistrz prawidłowo powołał Inspektora Ochrony Danych[6] i zgłosił ten fakt Prezesowi Urzędu Ochrony Danych Osobowych[7]. IOD prawidłowo realizował zadania wynikające z RODO, a jego przygotowanie i kwalifikacje zawodowe spełniały wymagania określone w Rozporządzeniu. Pracownicy posiadali odpowiednie upoważnienia do przetwarzania danych osobowych. Poprawnie realizowano wynikający z art. 13 RODO obowiązek informacyjny w procesie przetwarzania danych osobowych osób fizycznych. Na stronach internetowych Urzędu oraz tablicach ogłoszeniowych w trzech lokalizacjach Urzędu[8], Administrator udostępnił tożsamość oraz dane kontaktowe swoje i IOD, cel przetwarzania danych i okres ich przechowywania, informacje o odbiorcach oraz prawach żądania dostępu do treści danych, ich sprostowania i przenoszenia, a także informacje o prawie wniesienia skargi do UODO. Nie stwierdzono w miejscach ogólnodostępnych informacji naruszających ochronę danych osobowych osób fizycznych. Umowy, którymi powierzono podmiotom zewnętrznym przetwarzanie danych osobowych, określały przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, a także obowiązki i prawa Administratora, co było zgodne z art. 28 ust. 3 RODO.

Dwóm pracownikom, z którymi rozwiązano stosunek pracy, odebrano z opóźnieniem wynoszącym 14 i 62 dni dostęp do systemów informatycznych zawierających dane osobowe.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

1. Organizacja ochrony danych osobowych w jednostce

Opis stanu faktycznego

1.1 W dniu 22 maja 2018 r. zakończono w Urzędzie opracowywanie analizy ryzyka związanego z przetwarzaniem danych osobowych, w tym rozpoznano rodzaje zbiorów zawierających dane osobowe oraz czynności, w których niezbędne jest przetwarzanie danych osobowych, ryzyko skutków niezapewnienia ochrony danych osobowych oraz wskazano zalecenia. Wyniki analizy przedstawiono w raporcie.

---

[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[5] Rozporządzenie 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) Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1, ze zm. Dalej RODO lub Rozporządzenie.

[6] Dalej: IOD.

[7] Dalej: UODO.

[8] Tj. przy ul. Stefana Batorego, ul. Bankowej i Pl. Bolesława Chrobrego.

[9] 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.

Zidentyfikowano dziesięć możliwych zagrożeń, w tym w szczególności: włamanie, kradzież, awarie serwera, stacji roboczej i infrastruktury sieciowej, nielegalny dostęp, błędy pracowników, nielegalne oprogramowanie, pożar, zalanie. Każdy rodzaj ryzyka oceniono pod kątem prawdopodobieństwa wystąpienia oraz pod kątem skutków. Jako nieakceptowalne uznano 22 rodzaje ryzyka[10]. W celu zminimalizowania ryzyka zalecano dla każdego z nich odpowiednie działania zaradcze, m.in. zapewnienie obsługi informatycznej w celu szybkiej naprawy, odpowiedniego poziomu złożoności haseł oraz ich okresowej wymiany, stosowanie macierzy dyskowej.
Zgodnie z zaleceniami wskazanymi w analizie ryzyka przeprowadzono szkolenia pracowników oraz opracowano procedury wewnętrzne w zakresie ochrony danych osobowych, co zostało szerzej opisane w pkt. 1.2 oraz 1.11.

(akta kontroli str. 38-45)

W sprawie przeprowadzenia analizy ryzyka związanego z przetwarzaniem danych osobowych Burmistrz wyjaśnił: Administrator[11] *na etapie wdrożenia RODO opracował rejestr czynności przetwarzania danych oraz katalog możliwych form naruszeń i incydentów w zakresie ochrony danych osobowych wg kodów normy PN-ISO/IEC 27001:2007 i 17799:2007. Opisana została charakterystyka zdarzeń wpływających na zabezpieczenie danych osobowych. Na podstawie analizy prawdopodobieństwa i skutków oraz obliczonych wartości określono poziom ryzyka akceptowalnego i nieakceptowalnego. Opisano działania będące odpowiedzią na ryzyko i podjęto szereg działań w zakresie bezpieczeństwa przetwarzania danych. Kolejną analizę ryzyka wykonano z użyciem większej ilości zmiennych, tj. w zakresie prawdopodobieństwa opisano zmienne określające prawdopodobieństwo wystąpienia zdarzenia, ekspozycję oraz czas. Określono wpływ na poufność, integralność oraz dostępność danych osobowych. Ryzyko obliczono na podstawie prawdopodobieństwa i wpływu na przetwarzanie. Obecnie prowadzona jest analiza ryzyka z podziałem na obszary przetwarzania (arkusze wydziałowe/komórek samodzielnych) w celu analizy różnic w stosunku do poprzednio przeprowadzonych postępowań w zakresie analizy ryzyka.*

(akta kontroli str. 46, 49,57)

W dniu 2 grudnia 2018 r. sporządzono kolejną analizę ryzyka badając prawdopodobieństwo wystąpienia określonego ryzyka (w podziale na wystąpienie zdarzenia, ekspozycję i czas) oraz wpływ na aktywa (poufność, integralność, dostępność). W analizie przedstawiono już podjęte działania minimalizujące, takie jak np. przeprowadzony przegląd zabezpieczeń, tworzenie reguł firewall, zakup dodatkowych urządzeń sieci.

(akta kontroli str. 55-56)

1.2 Do 22 sierpnia 2019 r. obowiązywały regulacje wewnętrzne, w tym Zarządzenie Nr 130/2015 Burmistrza z 29 maja 2015 r. w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji" oraz „Instrukcji zarządzania systemem informatycznym" w Urzędzie Miejskim w Policach[12], w którym określono obowiązek Administratora Danych Osobowych do zapewnienia ochrony przetwarzanych danych w systemach informatycznych i tradycyjnych bez wskazania środków, w tym m.in.: techniczną ochronę danych i ich przetwarzanie, zasady autoryzacji użytkownika, ochronę antywirusową, zasady zabezpieczenia przed

[10] Awaria serwera (sprzęt i oprogramowanie), awaria infrastruktury sieciowej, ataki wirusów komputerowych, błędy użytkownika, uzyskanie dostępu osoby nieupoważnionej do serwera, do szafy teleinformatycznej, awarie zasilania, awarie UPS stacji roboczej, awarie UPS serwerów, złośliwe działania użytkowników, błędy użytkowników, użytkowanie prywatnych nośników danych, brak wykonywania kopii danych, uszkodzenia powodowane przez burze (pioruny), utrata danych lokalnych z dysków, awarie dysków serwera, używanie zbyt prostych haseł, pożar, zalanie.
[11] Burmistrz powołał Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Policach zarządzeniem Nr 129/2015 z dnia 29 maja 2015 r.
[12] Dalej Zarządzenie Nr 130/2015.

nieautoryzowanym dostępem do danych poprzez sieć publiczną oraz instrukcję postępowania w przypadku naruszenia ochrony danych osobowych.

(akta kontroli str. 5-25)

Politykę ochrony danych osobowych wprowadzono w Urzędzie Zarządzeniem Nr 217/2019 Burmistrza z 22 sierpnia 2019 r. w sprawie wprowadzenia „Polityki ochrony danych osobowych" oraz „Instrukcji eksploatacji systemów informatycznych" w Urzędzie Miejskim w Policach[13], w którym określono zabezpieczenia techniczne, fizyczne oraz organizacyjne danych osobowych w systemach papierowych i informatycznych[14], w tym m.in.: zbiory będące podstawą opracowania rejestru czynności przetwarzania danych osobowych, procedury nadawania uprawnień i rejestrowanie tych uprawnień w systemie informatycznym, procedury tworzenia kopii zapasowych zbiorów danych, zasady postępowania w przypadku naruszenia ochrony danych osobowych.
Rejestry czynności przetwarzania danych osobowych oraz kategorii czynności przetwarzania 25 maja 2018 r. została podana do wiadomości pracownikom Urzędu za pośrednictwem poczty elektronicznej.
Wymagane art. 30 ust. 1 oraz ust. 2 RODO rejestry, w tym: czynności przetwarzania danych osobowych oraz kategorii czynności przetwarzania w imieniu administratora prowadzi od 25 maja 2018 r.[15] IOD.

(akta kontroli str. 59-73,74-77)

1.3 Zgodne z obowiązkiem określonym w art. 37 RODO w zw. z art. 158 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[16], z dniem 17 lipca 2018 r. Zarządzeniem Nr 174/2018 w sprawie wyznaczenia Inspektora Ochrony Danych w Urzędzie Miejskim w Policach, wyznaczono IOD. Funkcja ta została powierzona osobie zatrudnionej w Urzędzie na stanowisku Administratora Bezpieczeństwa Informacji. W tym samym dniu określono zakres jego czynności.

(akta kontroli str. 57, 58, 59)

Dane IOD oraz sposób i formę kontaktu[17] opublikowano w miejscach ogólnodostępnych, w tym na stronie BIP Urzędu[18] oraz w klauzulach informacyjnych na tablicach w budynkach zajmowanych przez Urząd[19], spełniając obowiązek wynikający z art. 37 ust 7 RODO oraz art. 11 ustawy o ochronie danych osobowych.

(akta kontroli str. 95-99, 288-301)

1.4 Przygotowanie i kwalifikacje zawodowe IOD spełniały wymagania art. 37 ust. 5 RODO. Osoba realizująca zadania IOD posiadała wykształcenie wyższe magisterskie[20] oraz ukończyła studia podyplomowe o specjalności *Administrator Bezpieczeństwa Informacji.* Ponadto, odbyła cykl zewnętrznych szkoleń w zakresie wdrażania i stosowania przepisów RODO.

(akta kontroli str. 100-108)

1.5 Zakres działania IOD określono w Regulaminie organizacyjnym Urzędu Miejskiego w Policach[21]. W dokumencie tym oraz w zakresie czynności pracownika wskazano zadania IOD określone w art. 39 ust. 1 RODO oraz dodatkowo m.in.: analizę umów w zakresie usług zewnętrznych związanych z powierzeniem

[13] Dalej: Zarządzenie Nr 217/2019.
[14] W tym: Polityką ochrony danych osobowych (Załącznik nr 1), Instrukcją Eksploatacji Systematów Informatycznych (Załącznik nr 2). Procedura reagowania na naruszenia ochrony danych stanowiła odrębny dokument, do którego załącznik stanowił wzór rejestru incydentów naruszeń ochrony danych osobowych oraz Raport z naruszenia ochrony danych osobowych ze wskazaniem na okoliczności i skutki naruszeń oraz podjęte działania
[15] Zatwierdzone przez Burmistrza 24 maja 2018 r.
[16] Dz. U. poz. 1000, ze zm., dalej: ustawa o ochronie danych osobowych.
[17] Dane aktualne w okresie objętym kontrolą.
[18] http://bip.police.pl/artykul/301/11221/ochrona-danych-osobowych
[19] Tj. w Policach przy ulicy Stefana Batorego i Bankowej oraz w USC przy Pl. Bolesława Chrobrego.
[20] W zakresie cybernetyki ekonomicznej i informatyki.
[21] Wprowadzonym Zarządzeniami Burmistrza Polic w sprawie Regulaminu organizacyjnego Urzędu Miejskiego w Policach 22/2019 z 2 stycznia 2019 r. (od 2 stycznia 2019 r.). Dalej: Regulamin organizacyjny.

przetwarzania danych osobowych, analizę i ocenę stanu zabezpieczenia danych osobowych.

Podległość służbową komórek organizacyjnych jednostki wyznaczał schemat organizacyjny Urzędu[22], zgodnie z którym IOD podlegał bezpośrednio i wyłącznie Burmistrzowi, co zapewniało niezależność IOD, wymaganą art. 38 ust 3 RODO.[23]

(akta kontroli str. 109-112, 113-116)

1.6 O wyznaczeniu IOD poinformowano Prezesa UODO drogą elektroniczną 24 lipca 2018 r., tj. w terminie wynikającym z art. 10 ust. 1 ustawy o ochronie danych osobowych.

(akta kontroli str. 117-121)

1.7 W badanym okresie nie było zmian na stanowisku IOD.

(akta kontroli str. 34, 418-420)

1.8 W okresie objętym kontrolą zgodnie z art. 39 ust. 1 RODO, realizowane przez IOD zadania polegały na:

- informowaniu Administratora i pracowników o ich obowiązkach związanych z ochroną danych,
- nadzorowaniu prowadzenia rejestrów czynności przetwarzania danych przez poszczególne wydziały Urzędu oraz osób upoważnionych do przetwarzania danych osobowych,
- przeprowadzeniu ankiet sprawdzających stan wiedzy pracowników Urzędu na tematy związane z RODO,
- przeprowadzaniu szkoleń tematycznych na naradach roboczych poszczególnych wydziałów

(akta kontroli str. 173-215)

Burmistrz wyjaśnił, że IOD (…) *organizował szkolenie z zakresu ochrony danych osobowych dla pracowników urzędu i spotkania konsultacyjne z pracownikami. Szkolenie prowadzone było przez audytora wiodącego systemu zarządzania bezpieczeństwem informacji. IOD przekazuje pracownikom dokumentację ochrony danych i informację o zmianach w przepisach prawnych oraz inne treści (publikowane artykuły, wykładnie prawne, wyroki, wskazówki), na bieżąco informuje o zagrożeniach, organizowanych szkoleniach dziedzinowych. IOD nadzoruje i kontroluje działalność wydziałów w zakresie zadań wynikających z ochrony danych osobowych. Prowadzi bieżące konsultacje w zakresie czynności przetwarzania, obowiązków wynikających z przepisów prawa. Prowadzi konsultacje w zakresie umów, prowadzenia ewidencji udostępniania danych osobowych. Inspektor wraz z administratorami sieci komputerowej konsultuje wdrożenia w zakresie podniesienia bezpieczeństwa tj. zakupu urządzeń ochrony, oprogramowania zabezpieczającego, nośników danych, itp.*

(akta kontroli str. 34, 51)

1.9 Petenci Urzędu informowani byli o przetwarzaniu ich danych osobowych poprzez zamieszczenie klauzul informacyjnych dotyczących przetwarzania danych osobowych na: stronie BIP Urzędu[24] oraz tablicach i gablotach w miejscach ogólnodostępnych budynków zajmowanych przez Urząd[25], w tym: w punkcie informacyjno-kancelaryjnym, w Biurze Obsługi Klienta oraz na korytarzach. Klauzule informacyjne zawierały w szczególności: dane administratora oraz IOD, cel

[22] Załącznik do Regulaminu organizacyjnego.

[23] W poprzednio obowiązującym Regulaminie organizacyjnym Urzędu Miejskiego w Policach (zarządzenie Nr 26/09 Burmistrza Polic z dnia 28 stycznia 2009 r., obowiązującym od 2 8 stycznia 2009 r.) uregulowano zakres działań ABI, który był również podległy bezpośrednio i wyłącznie Burmistrzowi.

[24] http://bip.police.pl/artykul/301/11221/ochrona-danych-osobowych.

[25] Policach przy: ul. Stefana Batorego oraz ul. Bankowej.

przetwarzania danych, okres przetwarzania danych, podmioty i organy, którym dane mogą być przekazywane, pouczenie o prawie dostępu do danych oraz o prawie wniesienia skargi do organu nadzorczego, co było zgodne z obowiązkiem wynikającym z art. 13 ust. 1-2 RODO.

(akta kontroli str. 95-99, 127-129, 288-297)

1.10 W okresie objętym kontrolą zagadnienia dotyczące ochrony danych osobowych, w tym dotyczące przygotowania do wdrożenia przepisów określonych w RODO, nie były przedmiotem kontroli zewnętrznych w Urzędzie ani audytu wewnętrznego bądź zewnętrznego.

(akta kontroli str. 122-124, 125-126)

1.11 W okresie objętym kontrolą szkolenia pracowników Urzędu w zakresie ochrony danych osobowych na podstawie regulacji RODO, prowadzone były przez podmiot zewnętrzny oraz IOD. W dniu 9 maja 2018 r. zorganizowano szkolenie dla wszystkich pracowników Urzędu. Szkolenie miało charakter obowiązkowy. Wzięło w nim udział 144 osoby z 156 zatrudnionych na dzień szkolenia[26].

(akta kontroli str. 130-139)

Burmistrz wyjaśnił, *że Pracownicy, którzy nie wzięli udziału w szkoleniu w dniu 9 maja 2018 r. mieli możliwość odbycia takich szkoleń realizowanych przez IOD w trakcie narad poszczególnych wydziałów. Ponadto przeprowadzono w maju 2019 r. ankiety szkoleniowe utrwalające i rozszerzające wiedzę z zakresu RODO. W ankietach pracownicy opracowywali i konsultowali zagadnienia z zakresu ochrony danych osobowych z IOD. Ankieta wykazała również brak potrzeb szkoleniowych w tym zakresie ze strony samych pracowników i ich przełożonych. IOD na bieżąco przekazuje również wiedzę, wyjaśnienia, nowości i wydarzenia z zakresu RODO wszystkim pracownikom z dedykowanego do tego celu konta pocztowego.*

(akta kontroli str. 418-420)

1.12 Na przygotowanie i realizację zadań dotyczących wdrożenia obowiązków związanych z RODO, poniesiono wydatki w wysokości 93,3 tys. zł, w tym: 14 tys. zł na szkolenia, konferencje i warsztaty, 2,5 tys. zł studia podyplomowe IOD, 5,9 tys. zł zakup oprogramowania szyfrującego.

(akta kontroli str. 48, 51-52, 140-157)

1.13. W okresie objętym kontrolą[27] nie poniesiono wydatków w związku z niewłaściwym stosowaniem RODO. Ponadto, nie nałożono na Urząd administracyjnych kar pieniężnych oraz innych sankcji lub obowiązków naprawczych.

(akta kontroli str. 48, 52, 160-169)

1.14. W kontrolowanym okresie we wszystkich 25 podległych Gminie jednostkach[28] administratorem danych osobowych ustanowiono kierowników tych instytucji lub osoby ich reprezentujące. We wszystkich jednostkach wyznaczono IOD, w tym w 15 przypadkach pracowników jednostek, natomiast w pozostałych dziesięciu zawarto odrębne umowy z podmiotem zewnętrznym.

(dowód: akta kontroli 216, 223-224)

Burmistrz wyjaśnił, że jednostki *opracowują własną dokumentację oraz we własnym zakresie stosują środki organizacyjne i techniczne ochrony danych. Wydział Oświaty i Kultury Urzędu Miejskiego, jako organ nadzorujący, dokonał sprawdzenia czy zgodnie z przepisami RODO wyznaczono Inspektora Ochrony Danych Osobowych we wszystkich podległych jednostkach. Zobowiązano również jednostki do*

[26] Spośród 12 pozostałych pracowników czterech przebywało na urlopach, dwóch na zwolnieniach lekarskich, pozostałych sześciu zwolniono z przyczyn losowych.

[27] Dane na 19 listopada 2019 r.

[28] W tym: 22 jednostkach budżetowych, trzech instytucjach kultury oraz siedmiu spółkach miejskich.

udzielenia informacji nt. prowadzonej dokumentacji ochrony danych, przyjętych zasadach i procedurach i sposobie wywiązania się z obowiązku informacyjnego wobec osób, których dane osobowe są przetwarzane w formie tablic informacyjnych, stosownej informacji na stronach internetowych placówki. Tematy z zakresu ochrony danych osobowych były również tematem odbywających się cyklicznych spotkań naczelnika wydziału z kierownikami jednostek. Omawiane były również tematy związane z koniecznością powierzenia przetwarzania danych osobowych w przypadkach korzystania z usług podmiotów zewnętrznych.

(akta kontroli str. 47, 52-53)

1.15. W okresie objętym kontrolą do Urzędu nie wpłynęły skargi na podległe gminie Police jednostki organizacyjne w zakresie dotyczącym przetwarzania danych osobowych.

(akta kontroli str. 122-126)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

Z dniem 25 maja 2018 r. Urząd był organizacyjnie przygotowany do przetwarzania danych osobowych zgodnie z RODO. Wprowadzono wymagane rejestry czynności przetwarzania danych osobowych oraz kategorii czynności przetwarzania. Prawidłowo powołano IOD oraz terminowo zgłoszono ten fakt Prezesowi UODO. Dane IOD oraz sposób i formę kontaktu podano do publicznej wiadomości, spełniając obowiązek wynikający z art. 37 ust 7 RODO oraz art. 11 ustawy o ochronie danych osobowych. IOD posiadał wymagane przygotowanie i kwalifikacje zawodowe, zgodne z art. 37 ust. 5 RODO. W strukturach Urzędu zapewniono niezależność IOD. Pracownicy Urzędu zostali przeszkoleni w zakresie ochrony danych osobowych.

OBSZAR

2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych

Opis stanu faktycznego

2.1 Zgodnie z obowiązkiem wynikającym z art. 30 ust. 3 RODO, rejestr czynności przetwarzania danych osobowych prowadzono w Urzędzie w formie papierowej oraz elektronicznej[29]. Wskazany dokument zawierał wymagane art. 30 ust. 1 wymienionego Rozporządzenia informacje, w tym m.in.: nazwę i dane kontaktowe Administratora oraz IOD, cele przetwarzania, opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych, kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, planowane terminy usunięcia poszczególnych kategorii danych oraz ogólny opis technicznych i organizacyjnych środków bezpieczeństwa[30].

Za podstawę przetwarzania danych we wskazanych zbiorach danych osobowych przyjęto warunki określone w art. 6 ust. 1 lit. a-c RODO.

(akta kontroli str. 79-84)

2.2 W okresie od 25 maja 2018 r. do 12 grudnia 2019 r. dokonano jednej aktualizacji rejestru czynności przetwarzania danych osobowych w zakresie czynności Zakładowego Funduszu Świadczeń Socjalnych.

(akta kontroli str. 94)

2.3. Na podstawie art. 30 ust. 2 RODO w rejestrze kategorii czynności przetwarzania dokonywanych w imieniu innych administratorów zamieszczono dane

[29] Arkusz Excel.

[30] O których mowa w art. 32 ust. 1 RODO.

zgodnie z art. 30 ust. 2 RODO. Stosownie do art. 30 ust. 3 RODO, wskazany rejestr prowadzono w formie papierowej oraz elektronicznej[31].

(akta kontroli str. 78, 418-420)

2.4 W okresie od 25 maja 2018 r. do 13 grudnia 2019 r. dokonano dwóch aktualizacji rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innych administratorów, w tym z powodu rozpoczęcia przetwarzania zbiorów danych osobowych związanych z realizacją nowych zadań lub zmianą umów.

(akta kontroli str. 94)

W rejestrze kategorii czynności przewarzania danych wskazano kategorie przetwarzań dokonywanych w imieniu każdego z administratorów[32], w tym m.in.: obsługę systemu teleinformatycznego *ŹRÓDŁO*[33] w zakresie spraw petentów, obsługę systemu teleinformatycznego pn. *System Informacji Oświatowej SIO*[34] odnośnie danych nauczycieli, dyrektorów szkół oraz uczniów, realizację zadań[35] pn.: *Zachodniopomorska Karta Rodziny* i *Zachodniopomorska Karta Seniora*, obsługę wyborów.

Zgodnie z art. 5 ust. 1 lit. c RODO informacje zawarte w wymienionych rejestrach były niezbędne, adekwatne i stosowne do celów ich przetwarzania.

(akta kontroli str. 78-94, 217-222, 224-229, 231-240)

2.5 W okresie objętym kontrolą, 179 pracowników działających z upoważnienia administratora wpisanych było do prowadzonego przez IOD *Rejestru upoważnień – poleceń przetwarzania danych*[36]. Ewidencja zawierała: imię i nazwisko pracownika, datę nadania i ustania upoważnienia[37] oraz uwagi. Do przetwarzania danych osobowych Burmistrz upoważnił 13 z 14 zatrudnionych w wydziale[38] pracowników oraz siedem osób pracujących w wydziale Oświaty i Kultury[39]. Weryfikacja upoważnień pracowników obu wydziałów wykazała, że ich zakres odpowiadał zakresowi wykonywanych obowiązków służbowych. Wskazane upoważnienia wydano 25 maja 2018 r. i umieszczono w aktach personalnych pracowników.

(akta kontroli str. 230, 302-309, 310-351)

Badanie upoważnień do przetwarzania danych osobowych osób zatrudnionych przez Urząd na podstawie umowy zlecenia, przeprowadzono na próbie 10 umów cywilnoprawnych[40]. Wszystkie osoby zatrudnione na podstawie poddanych badaniu umów, przetwarzały dane osobowe wyłącznie na polecenie Administratora, co było zgodne z art. 29 oraz 32 ust. 4 RODO. Upoważniono zleceniobiorców do przetwarzania danych osobowych i zobowiązano ich m.in. do zapewnienia odpowiednich środków technicznych i organizacyjnych by przetwarzanie odbywało się zgodnie z RODO, zapewnienia poufności informacji uzyskanych w związku z realizacją umowy oraz zabezpieczenia tych danych przed ich udostępnieniem osobom nieupoważnionym.

(akta kontroli str. 352-353)

---

[31] Arkusz Excel.

[32] W tym: Krajowego Biura Wyborczego, Województwa Zachodniopomorskiego oraz Ministrów: Cyfryzacji, Spraw Wewnętrznych i Administracji, Edukacji Narodowej, Inwestycji i Rozwoju oraz Spraw Wewnętrznych i Administracji.

[33] Program do edycji oraz przetwarzania danych gromadzonych w Systemie Rejestrów Państwowych.

[34] Elektroniczny system baz danych służący gromadzeniu informacji o szkołach, placówkach oświatowych, nauczycielach oraz uczniach; dalej: SIO.

[35] W tym wynikających z realizacji przez Województwo Zachodniopomorskie Wojewódzkiego Programu Wspierania Rodziny i Systemu Pieczy Zastępczej na lata 2014 – 2020. pn. Region dla Rodziny, przyjętego Uchwałą Nr XXXVIII/517/14 Sejmiku Województwa Zachodniopomorskiego 30 września 2014 r.

[36] Rejestr prowadzony w formie papierowej od 25 maja 2018 r.

[37] Jeżeli dotyczyło.

[38] Nie upoważniono pracownika wykonującego zadania w ramach robót publicznych.

[39] Badaniem objęto dwa wydziału Urzędu: ME oraz GG.

[40] Zawartych przez Urząd od 25 maja 2018 r.

2.6 W okresie objętym kontrolą żaden pracownik Urzędu nie zmienił komórki organizacyjnej w ramach Urzędu, stosunek pracy rozwiązano z 20 pracownikami.
Weryfikacja uprawnień dostępu do systemów informatycznych łącznie czterech pracowników wydziałów Gospodarki Odpadami[41] i Finansowo-Budżetowego[42] wykazała, że:

- dwóm pracownikom FN, odebrano dostęp do systemów informatycznych z dniem rozwiązania stosunku pracy, stosownie do art. 5 ust. 1 lit. f w zw. z art. 29 oraz 32 ust. 4 RODO;
- jednemu pracownikowi z wydziału GO dostęp do systemu odebrano 14 dni po terminie rozwiązania stosunku pracy i jednemu pracownikowi dostęp ten odebrano 62 dni po terminie ustania stosunku pracy, co było niezgodne z powyżej powołanym przepisem i zostało szerzej opisane w sekcji *Stwierdzone Nieprawidłowości*.

(akta kontroli: 170-172)

2.7 Urząd powierzył przetwarzanie danych osobowych na podstawie 62 umów[43] zawartych z podmiotami zewnętrznym. Wśród wskazanych umów, w sześciu przypadkach aktualizowano umowy, na podstawie których w okresie wcześniejszym powierzano przetwarzanie danych osobowych podmiotom zewnętrznym. Przedmiot umów obejmował m.in.: wykonanie projektu zmiany planu zagospodarowania przestrzennego, przewóz dzieci do szkół, inwentaryzację komunalnych budynków mieszkalnych oraz asystę techniczną i konserwację części składowych i modułów Polickiego Systemu Informacji Przestrzennej.
Na podstawie weryfikacji postanowień pięciu umów[44], którymi powierzono przetwarzanie danych osobowych stwierdzono, że zgodnie z art. 28 ust. 3 RODO określono przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczyły, a także obowiązki i prawa administratora. Ponadto, na postawie art. 28 ust. 9 wymienionego rozporządzenia wskazane umowy zostały zawarte w formie pisemnej.

(akta kontroli str. 250-287)

2.8 W badanym okresie kontrolowana jednostka wykonywała zadania podmiotu przetwarzającego:

- w czterech przypadkach z tytułu zadań zleconych z zakresu administracji rządowej w imieniu: Ministra Cyfryzacji oraz Ministra Spraw Wewnętrznych i Administracji na podstawie: ustawy z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego[45], ustawy o ewidencji ludności, ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych[46] oraz w imieniu Ministra Edukacji Narodowej na podstawie ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej[47];
- na podstawie dwóch umów, w tym z upoważnienia Krajowego Biura Wyborczego w zakresie realizacji wyborów[48] oraz Województwa Zachodniopomorskiego w zakresie zadań wynikających z realizacji programu Zachodniopomorska Karta Rodziny i Zachodniopomorska Karta Seniora[49].

[41] Dalej: GO.

[42] Dalej: FN.

[43] W tym umowy zawarte w okresie objętym kontrolą oraz przed 25 maja 2018 r., tj. przed wejściem w życie RODO.

[44] W tym w związku ze świadczeniem usług: niszczeniem nośników i informacji, wykonania projektu zmiany miejscowego planu zagospodarowania przestrzennego Gmina Północ i Gmina Południe, eutanazja ślepych miotów.

[45] Dz.U. z 2018 r. poz. 2224 ze zm.

[46] Dz.U. z 2019 r. poz.653 ze zm.

[47] Dz.U. z 2018 r. poz. 1900 ze zm.

[48] Umowa o wzajemnym powierzeniu przetwarzania danych osobowych z 25 lipca 2018 r.

[49] Porozumienie Partnerskie nr ROPS/III/17/15 z 24 sierpnia 2015 r. zawarte w związku z realizacją przez Województwo Zachodniopomorskie Wojewódzkiego Programu Wspierania Rodziny i Systemu Pieczy Zastępczej na lata 2014-2020

W związku z wykonywaniem zadań podmiotu przetwarzającego z tytułu realizacji zadań zleconych z zakresu administracji rządowej, otrzymywano od administratorów wytyczne, instrukcje, itp. odnośnie prowadzenia baz danych lub stosowania obowiązujących przepisów, w tym m.in.:

- Minister Spraw Wewnętrznych i Administracji wspólnie z Ministerstwem Cyfryzacji w związku z realizacją zadań z zakresu spraw obywatelskich przygotowali i przekazali informacje na temat stosowania przepisów rozporządzenia RODO wraz z wzorami klauzul informacyjnych w zakresie rejestracji stanu cywilnego, ewidencji ludności i dowodów osobistych[50];
- Minister Edukacji Narodowej zwracał się o monitorowanie terminowego i zgodnego ze stanem faktycznym przekazywania danych do SIO przez zobowiązane podmioty[51] oraz przekazywał wytyczne odnośnie pracy w systemie[52].

Analiza porozumienia z Województwem Zachodniopomorskim w związku z realizacją programu Zachodniopomorska Karta Rodziny i Zachodniopomorska Karta Seniora wykazała, że zgodnie z art. 28 ust. 3 RODO wskazane dokumenty określały przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczyły, a także obowiązki i prawa administratora. Ponadto, podmiot przetwarzający wywiązywał się z obowiązków umownych, w tym m.in.: upoważniono pracowników do przetwarzania danych osobowych oraz prowadzono ewidencję w tym zakresie, zobowiązano pracowników do zapoznania się z przepisami prawa regulującymi kwestie danych osobowych oraz do zachowania w tajemnicy przetwarzanych danych, stosowano wymagane klauzule informacyjne RODO oraz prowadzono rejestr wszystkich kategorii czynności przetwarzania.

(akta kontroli str. 418-420)

2.9 W kontrolowanym okresie w Urzędzie nie prowadzono monitoringu wizyjnego. Na podstawie art. 20 ust. 1 b ustawy z dnia 8 marca 1990 r. o samorządzie gminnym[53] obrady Rady Miejskiej w Policach transmitowano i utrwalano za pomocą urządzeń rejestrujących obraz i dźwięk. Na sali sesyjnej, w której odbywały się obrady Rady Miejskiej w Policach umieszczono informację o transmitowaniu i utrwalaniu, zgodnie z art. 20 ust. 1b uosg za pomocą urządzeń rejestrujących obraz i dźwięk obrad Rady Miejskiej. W informacji tej wskazano m.in.: administratora danych osobowych pozyskanych w trakcie nagrywania obrad, cel i zakres przetwarzania danych, wyznaczenie IOD oraz pouczenie o prawie wniesienia skargi do UODO.

(akta kontroli: str. 47, 53)

2.10 Zgodnie z Zarządzeniem Nr 217/2019[54] przewidziano środki fizyczne polegające na ochronie obszaru przetwarzania danych osobowych poza godzinami pracy poprzez m.in.: ochronę fizyczną budynku Urzędu oraz zastosowanie systemu alarmowego[55] w wyznaczonych lokalizacjach. Do zabezpieczeń technicznych zaliczono[56]: odrębne zasilanie sprzętu komputerowego oraz zastosowanie zasilaczy awaryjnych UPS, ochronę serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy awaryjnych UPS o podwyższonej mocy, ochronę przed utratą zgromadzonych danych przez robienie kopii zapasowych na nośnikach

pn. Region dla Rodziny, zmienione w zakresie powierzania przetwarzania danych osobowych Aneksem Nr 1/2018 z 28 listopada 2018 r.

[50] Pismo Ministerstwa Spraw Wewnętrznych i Administracji DSO-WSC-6000-17-25/2018 z 21 maja 2018 r.

[51] W tym pisma Ministra Edukacji Narodowej: DWST-WS.72.338.2019.AK oraz DWST-WS.71.432.2019.KP odpowiednio z 24 oraz 27 września 2019 r.

[52] Informacja z 3 października 2019 r. dotycząca weryfikacji danych w SIO.

[53] Dz. U. z 2019 r. poz. 506 ze zm.; dalej uosg.

[54] Załącznik Nr 1 - Polityka Ochrony Danych (punkt 4 a-e w zakresie fizycznej ochrony danych).

[55] Wraz z monitorowaniem sygnałów przesyłanych z tego systemu.

[56] Załącznik Nr - 1 Polityka Ochrony Danych (punkt 4 a-h w zakresie technicznych i informatycznych ochrony danych).

zewnętrznych oraz dedykowanych urządzeniach pamięci masowej UPS, z których w wypadku awarii miały być odtwarzane dane, kontrolę dostępu użytkowania, autoryzację na poziomie programu, szyfrowanie danych, firewall, system antywirusowy na każdym komputerze, szyfrowanie transmisji. Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych przewidziano[57] wykonywanie kopii zapasowych zbiorów danych, na wydzielonym zasobie serwera. Do tworzenia kopii używano narzędzi przewidzianych w systemach serwerów lub narzędzi baz danych. Kopie zapasowe były przechowywane w innych pomieszczeniach niż były wykonywane. W celu ochrony przed nieautoryzowanym dostępem do sieci lokalnej przewidziano[58] m.in.: zastosowanie zabezpieczeń typu firewall, stosowanie mechanizmów kontroli dostępu do sieci, zabezpieczenia sieci bezprzewodowej oraz stosowanie mechanizmów monitorujących przeglądnie stron internetowych.

(akta kontroli: str. 26-33, 59-73)

W kontrolowanym okresie, fizyczną ochronę danych osobowych przetwarzanych w Urzędzie realizowano w szczególności poprzez zlecenie podmiotom zewnętrznym usług:

- całodobowej ochrony w systemie monitoringu sygnałów alarmowych pomieszczeń objętych lokalnym systemem alarmowym monitorowanym przez Alarmowe Centrum Odbiorcze; zleceniobiorcę zobowiązano m.in. do monitorowania (dozoru) sygnałów przesyłanych z lokalnego systemu alarmowego po łączach radiowych, niezwłocznego wysyłania patrolu ochronnego po odebraniu sygnału o zagrożeniu osób lub mienia w obiekcie oraz zawiadamiania Policji, Straży Pożarnej lub Pogotowia Ratunkowego w celu podjęcia właściwych działań;
- okresowych przeglądów, zabiegów konserwacyjnych i napraw serwisowych instalacji alarmowej pomieszczeń objętych lokalnym systemem alarmowym[59];
- konserwację i bieżące naprawy urządzeń i instalacji automatycznej sygnalizacji pożaru[56] w budynkach zajmowanych przez Urząd;

co było zgodne z Zarządzeniem Nr 217/2019[60].

(akta kontroli str. 418-420)

Ponadto, w dwóch zajmowanych przez Urząd budynkach wydzielano serwerownie[61]. Weryfikacja rozwiązań zabezpieczających pomieszczenie przed utratą danych wykazała m.in., że:

- wszystkie urządzenia informatyczne zamontowano w specjalnie do tego przystosowanych szafach,
- na wypadek czasowego zaniku zasilania zastosowano układy podtrzymujące napięcie UPS,
- pomieszczenia wyposażono w systemy klimatyzacji oraz czujki dymu;
- przez żadną z serwerowni nie przebiegają rury wodno-kanalizacyjne;
- pomieszczenia zostały wyposażone w atestowane zabezpieczenia.

(akta kontroli str. 288-300)

Zgodnie z Zarządzeniem Nr 217/2019 ryzyko działania szkodliwego oprogramowania oraz próby nieautoryzowanego dostępu do sieci informatycznej minimalizowano poprzez zabezpieczenie wewnętrznej sieci komputerowej urządzeniami firewall, wyposażeniem stanowisk komputerowych w antywirusową

[57] Załącznik nr 2 - Instrukcja eksploatacji systemów informatycznych w Urzędzie Miejskim w Policach (rozdział Procedura tworzenia kopii zapasowych oraz programów i narzędzi programowych służących do ich przetwarzania).
[58] Załącznik Nr 1 - Polityka Ochrony Danych (punkt 4 a-c Zabezpieczenia przed nieautoryzowanym dostępem do danych poprzez sieć publiczną).
[59] Na podstawie odrębnych dla każdej lokalizacji (ul. Batorego, ul. Bankowa, Pl. Chrobrego (Urząd Stanu Cywilnego) umów zawartych firmą na lata 2018 i 2019.
[60] Załącznik Nr 1 - Polityka Ochrony Danych.
[61] Przy ul. Bankowej i ul. Batorego.

ochronę indywidualną i kontrolę dostępu do nich oraz monitorowanie przeglądania stron internetowych.

(akta kontroli str. 26-33, 59-73)

Zgodne z § 5 Instrukcji Eksploatacji Systemów Informatycznych kopie danych tworzone były codziennie i przechowywane na pamięciach dyskowych o określonej strukturze katalogowania. Plik kopii zawierał w swej nazwie datę powstania. Kopie systemu przechowywano na pamięciach dyskowych wraz z oprogramowaniem i bazami danych.

(akta kontroli str. 26-33, 59-73)

2.11 Zgodnie z *Instrukcją Zarządzenia Systemami Informatycznymi w zakresie przetwarzania danych osobowych* w celu zapewnienia zabezpieczenia dostępu do sieci lokalnej przyjęto użycie identyfikatora oraz hasła[62]. Proces ten wymagał uwierzytelnienia uprawnionego użytkownika za pomocą identyfikatora i hasła dostępu[63]. Przy każdorazowym opuszczeniu stanowiska komputerowego pracownicy zobowiązani byli m.in. do ręcznego ustawienia blokady ekranu.
Analiza dostępu do 10 stanowisk komputerowych wykazała, że zgodnie ze wskazaną procedurą pracownicy dostęp do sieci lokalnej uzyskiwali za pomocą hasła składającego się z wymaganej procedurą ilości znaków. Pracownicy przygotowani byli również do wykonania czynności blokady ekranu, stosując odpowiednią kombinację klawiszy.

(akta kontroli: str. 26-33, 59-73, 354-356)

Stwierdzone nieprawidłowości

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

1. Z opóźnieniem odebrano dwóm pracownikom, z którymi rozwiązano stosunek pracy, dostęp do systemów informatycznych pozwalających na przetwarzanie danych osobowych. Pracownikowi GO dostęp do systemu *Gospodarowanie Odpadami - Opłaty* odebrano 14 stycznia 2019 r., zamiast w dniu rozwiązania z nim stosunku pracy, tj. 31 grudnia 2018 r. Pracownikowi FN dostęp do systemu *Ewidencja Opłat Dzierżawy* odebrano 14 stycznia 2019 r., zamiast z dniem rozwiązania z nim stosunku pracy, tj. 13 listopada 2018 r. W konsekwencji, pracownicy mieli dostęp do tych systemów przez odpowiednio 14 dni i 62 dni po ustaniu stosunku pracy.
Powyższe było niezgodne z art. 5 ust. 1 lit. f w zw. z art. 29 oraz art. 32 ust. 4 RODO.

Na podstawie art. 5 ust. 1 lit. f RODO, dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym m.in. ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem. Ponadto art. 29 oraz art. 32 ust. 4 tego Rozporządzenia wprowadzają wymóg, aby każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego, przetwarzała je wyłącznie na polecenie administratora.
W związku z tym osoby, które nie są już pracownikami jednostki nie mogą działać z upoważnienia administratora i tym samym nie mogą mieć możliwości dokonywania żadnych czynności związanych z przetwarzaniem danych.

Burmistrz wyjaśnił, że: *Urząd Miejski w Policach przystąpi w ramach rozbudowy systemów informatycznych do wymiany oprogramowania systemowego i dziedzinowego funkcjonującego w Urzędzie (…). Nowe systemy umożliwią większą*

[62] Załącznik nr 2 do Zarządzenia Nr 217/2019, Procedura nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności, Metody i środki uwierzytelnienia oraz procedura związana z ich zarządzaniem i użytkowaniem.
[63] Załącznik nr 2 do Zarządzenia Nr 179/2018, rozdział 3 pkt 3.1, ppkt 4.

funkcjonalność w zakresie rozliczalności użytkowników systemów operacyjnych w zakresie autoryzacji i kontroli użytkowników. Obecnie funkcjonują reguły logowania do systemów i określono zasady zmiany haseł użytkowników. Kontrola użytkowników w tym zakresie wykazuje, że postępują oni zgodnie z przyjętymi zasadami. Jednakże systemy operacyjne i ich logi nie umożliwiają dostępu do historii tych operacji i pełnej rozliczalności użytkownika. O ile aplikacje dziedzinowe zostały dostosowane do wymogów rozliczalności, o tyle systemy serwerowe Windows i systemy stacji roboczych Windows wymagają wdrożenia nowych funkcjonalności. W związku z tym, że w 2019 roku zostanie ogłoszony przetarg na kompleksowe rozwiązania, Administrator nie chciał ponosić kosztów wdrożenia poza postępowaniem w sprawie realizacji projektu, aby nie ponosić dodatkowych kosztów. Przygotowanie projektu zaczęto realizować na początku 2018 roku. Opóźnienia w ogłoszeniu postępowania wynikają z konieczności szczegółowych ustaleń technicznych, ponieważ projekt obejmuje zarówno systemy urzędu jak i podległych jednostek.

(akta kontroli: akta kontroli: 170, 171-172,400-401)

OCENA CZĄSTKOWA

Prowadzone rejestry czynności przetwarzania danych osobowych oraz wszystkich kategorii czynności przetwarzania zawierały zgodnie z art. 30 ust. 2-3 RODO wszystkie wymagane elementy. Na podstawie art. 28 ust. 3 tego Rozporządzenia, przy zawieraniu umów, którymi powierzono dane osobowe podmiotom zewnętrznym, wskazywano przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, a także obowiązki i prawa Administratora.

Zgodnie z procedurami wewnętrznymi ryzyko działania szkodliwego oprogramowania oraz próby nieautoryzowanego dostępu do sieci informatycznej minimalizowano poprzez zabezpieczenie wewnętrznej sieci komputerowej urządzeniami firewall, wyposażeniem stanowisk komputerowych w antywirusową ochronę indywidualną oraz kontrolę dostępu do nich, a także monitorowanie przeglądania stron internetowych.

Ponadto, przez odpowiednio 14 i 62 dni nie odebrano dostępu do systemów informatycznego zawierającego dane osobowe, dwóm pracownikom, z którymi rozwiązano stosunek pracy.

OBSZAR

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

Opis stanu faktycznego

3.1. W okresie objętym kontrolą nie zgłaszano do UODO przypadków naruszenia ochrony danych osobowych.

(akta kontroli str. 418-420)

3.2 W okresie objętym kontrolą nie zgłaszano do Urzędu żądań dotyczących usunięcia, sprostowania bądź uzupełnienia niekompletnych danych osobowych.

(akta kontroli str. 418-420)

3.3 Na stronie BIP Urzędu[64] oraz w pomieszczeniach ogólnodostępnych w budynkach zajmowanych przez Urząd[65] nie umieszczano publikacji, które zawierały informacje mogące naruszać ochronę danych osobowych. Nie upubliczniano również zbędnych i nieadekwatnych do celu, informacji o osobach fizycznych.

(akta kontroli str. 95-99, 127-129, 288-301)

[64] http://bip.police.pl/

[65] Tj. w Policach przy ul. Stefana Batorego, ul. Bankowej oraz Pl. Bolesława Chrobrego.

3.4 W regulacjach wewnętrznych odniesienie do usuwania i niszczenia zbędnej dokumentacji zawarto w szczególności w Zarządzeniu 217/2019, poprzez wskazanie, że dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, należy zniszczyć fizycznie, przez sprzętowe kasowanie danych tak, aby nie było możliwe odczytanie jakiegokolwiek ich fragmentu oraz, że nośniki z danymi osobowymi należy niszczyć zgodnie z przepisami dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi i prawnymi.
W okresie objętym kontrolą w związku z usuwaniem zbędnej dokumentacji zawarto jedną umowę[66] z podmiotem zewnętrznym. Wykonawcę zobowiązano do jednorazowego i całkowitego zniszczenia dokumentacji niearchiwalnej w ilości szacunkowej 200 mb. Wykonanie usługi potwierdzono protokołem zniszczenia z 17 października 2018 r.

(akta kontroli str. 26-33, 59-73, 357-367)

3.5 Pracownicy Urzędu informowani byli przez administratora o przetwarzaniu ich danych osobowych poprzez podpisanie przyjęcia do wiadomości informacji w tym zakresie. Wskazane dokumenty gromadzone były przez IOD i nie zamieszczano ich w aktach personalnych osób zatrudnionych. Analiza dokumentacji w zakresie wskazanego obowiązku Administratora dotycząca pracowników zatrudnionych w wydziałach Ochrony Środowiska oraz Gospodarki Gruntami wykazała, że

- w informacji podano m.in.: tożsamość i dane kontaktowe Administratora oraz IOD, cel przetwarzania danych i okres ich przechowywania, informacje o odbiorcach oraz prawach: żądania dostępu do treści swoich danych, ich sprostowania oraz przenoszenia, a także prawie wniesienia skargi do UODO;
- w okresie od 25 maja 2018 r. do 10 lipca 2019 r. informację o przetwarzaniu danych osobowych przyjęli do wiadomości wszyscy pracownicy zatrudnieni w ww. wydziałach.

(akta kontroli str. 418-420)

3.6 W dniu 30 września 2019 r. zawarto z osobami fizycznymi 21 umów zlecenia na obsługę informatyczną obwodowych komisji wyborczych powołanych do przeprowadzenia wyborów do sejmu i senatu. Weryfikacja 10 umów odnośnie obowiązku informacyjnego Administratora w zakresie przetwarzania danych osobowych zleceniobiorcy wykazała, że wszystkie osoby, z którymi zwarto umowy, pisemnie potwierdziły przyjęcie do wiadomości informacji w tym zakresie. Zgodnie z art. 13 RODO w informacji podane zostały m.in.: tożsamość i dane kontaktowe Administratora oraz IOD, cel przetwarzania danych i okres ich przechowywania, informacje o odbiorcach oraz prawach: żądania dostępu do treści swoich danych, ich sprostowania oraz przenoszenia, a także prawie wniesienia skargi do UODO.

(akta kontroli str. 418-420)

3.7 W okresie objętym kontrolą przeprowadzono w Urzędzie 14 zewnętrznych naborów na stanowiska urzędnicze. Zgodnie z art. 13 ust. 1-4 RODO publikowane na stronie BIP Urzędu ogłoszenia o naborze pracowników zawierały m.in.: dane kontaktowe Administratora oraz IOD, cel[67], podstawę prawną i okres[68] przetwarzania danych osobowych kandydata. Ponadto, w ogłoszeniach informowano o prawie wniesienia skargi do UODO, a także prawach dostępu do danych oraz możliwości żądania ich sprostowania i usunięcia.

(akta kontroli str. 368, 369-399,401-410)

[66] Umowa z 3 października 2019 r.

[67] W tym: wypełnienie obowiązku prawnego, jakim jest zgodne z przepisami zatrudnianie pracownika w Urzędzie Miejskim w Policach.

[68] W tym informację, że dane osobowe będą przetwarzane do momentu zakończenia postępowania rekrutacyjnego i rozstrzygnięcia naboru, następnie po okresie trzech miesięcy niszczone (oferty rozpatrzone negatywnie) lub archiwizowane przez okres pięciu lat.

3.8 Zgodnie z zarządzeniem Nr 31/06 Burmistrza z 3 lutego 2006 r. w sprawie ustalenia procedury naboru kandydatów na wolne stanowiska urzędnicze, w tym kierownicze w Urzędzie Gminy w Policach oraz wolne stanowiska kierowników jednostek organizacyjnych Gminy Police[69] przyjęto, że dokumenty aplikacyjne kandydata, który zostanie wyłoniony w procesie rekrutacji, zostaną dołączone do jego akt osobowych. Dokumenty aplikacyjne osób, które w procesie rekrutacji zakwalifikowały się do dalszego etapu i zostały umieszczone w protokole z posiedzenia komisji rekrutacyjnej, będą przechowywane zgodnie z instrukcją kancelaryjną, przez okres dwóch lat, a następnie przekazywane do archiwum zakładowego. Dokumenty aplikacyjne pozostałych osób będą odsyłane lub odbierane osobiście przez zainteresowanych. Zgodnie z rejestrem czynności przetwarzania danych osobowych, dla przechowywania informacji o kandydatach przyjęto okres dwuletni.
Burmistrz wyjaśnił, że: *zarządzenie w sprawie ustalenia procedury naboru kandydatów na wolne stanowiska urzędnicze z 2006 r. sprowadziło się i dlatego też przeniesiono dwuletni okres przechowywania dokumentacji rekrutacyjnej do rejestru czynności przetwarzania danych osobowych*.

(akta kontroli str. 400, 411-417)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli pozytywnie ocenia zarządzanie danymi osobowymi przetwarzanymi, w tym gromadzonymi w jednostce.

IV. Uwagi i wnioski

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

Wnioski

Odbieranie, bez zbędnej zwłoki, dostępu do systemów informatycznych pracownikom, z którymi rozwiązano stosunek pracy.

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

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 Szczecinie. 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.

[69] Ze zmianami wprowadzonymi zarządzeniem Nr 168/09 Burmistrza z 16 lipca 2019 r.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 14 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.

Szczecin, 31 grudnia 2019 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie
Dyrektor

Kontroler
Agata Prochotta Miłek
Specjalista kontroli państwowej

..... *podpis*

..... *podpis*