NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ.410.021.03.2019

Rafał Zając
Prezydent Miasta Stargard

Urząd Miejski w Stargardzie
ul. Hetmana Stefana Czarnieckiego 17
73-110 Stargard

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 Stargardzie, ul. Hetmana Stefana Czarnieckiego 17, 73-110 Stargard
Kierownik jednostki kontrolowanej	Rafał Zając, Prezydent Miasta Stargard[1] od 14 kwietnia 2017 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 zdarzenia wcześniejsze, które miały wpływ na kontrolowaną działalność.
Podstawa prawna podjęcia kontroli	art.2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Szczecinie
Kontroler	Katarzyna Kozłowska, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LSZ/147/2019 z 30 sierpnia 2019 r. (akta kontroli str.1-2, 12-15)

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

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

W dniu wejścia w życie RODO[4], tj. 25 maja 2018 r. Urząd nie został organizacyjnie przygotowany do przetwarzania danych osobowych zgodnie z tym rozporządzeniem. Proces analizy ryzyka związanego z przetwarzaniem danych osobowych rozpoczęto dopiero od dnia obowiązywania wskazanej regulacji. W konsekwencji, polityki ochrony danych osobowych oraz pozostałe dokumenty wymagane tym rozporządzeniem, takie jak rejestry czynności przetwarzania danych osobowych i kategorii czynności przetwarzania opracowano z opóźnieniem od siedmiu do 26 dni. Również upoważnienia do przetwarzania danych osobowych zostały wydane dopiero 6 września 2018 r. Ponad 90% (tj.19 z 21) objętych kontrolą pracowników od czterech do 104 dni przetwarzało dane osobowe bez polecenia Administratora. Nieterminowe wdrożenie polityk ochrony danych osobowych oraz utworzenie po 25 maja 2018 r. rejestrów czynności przetwarzania danych osobowych i kategorii czynności przetwarzania było niezgodne z art. 24 ust.1 i 2 oraz art. 30 ust. 1 i 2 RODO, a przetwarzanie danych bez stosownego polecenia stanowiło naruszenie art. 29 oraz 32 ust. 4 wskazanego rozporządzenia.

Prezydent prawidłowo powołał Inspektora Ochrony Danych[5] i zgłosił ten fakt Prezesowi Urzędu Ochrony Danych Osobowych[6]. Nie zapewnił jednak niezależności tej funkcji, w wyniku wskazania procedurami wewnętrznymi, merytorycznego podporządkowania IOD Sekretarzowi Miasta[7], co było niezgodne z art. 38 ust. 3 RODO.

Pomimo powyższego, IOD prawidłowo realizował wynikające z art. 39 ust. 1 wskazanego rozporządzenia zadania oraz posiadał odpowiednie przygotowanie i kwalifikacje zawodowe. Również poprawnie realizowano wynikający z art. 13 RODO obowiązek informacyjny w procesie przetwarzania danych osobowych osób fizycznych. Administrator udostępnił tożsamość i dane kontaktowe zarówno swoje jak 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 prawie wniesienia skargi do UODO. W miejscach ogólnodostępnych nie zamieszczano informacji naruszających ochronę danych osobowych osób fizycznych. Umowy, którymi powierzono do przetwarzania dane osobowe podmiotom zewnętrznym, 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.

Stosowane zabezpieczenia fizyczne oraz techniczne nie zapewniały pełnej ochrony danych osobowych przed ich utratą. Stan taki spowodowany był możliwością nieautoryzowanego dostępu do pomieszczenia serwerowni przez osoby postronne oraz niedostateczne zminimalizowanie ryzyka zagrożenia pożarowego w tym pomieszczeniu. Kopie bezpieczeństwa przechowywano jedynie w jednym pomieszczeniu Urzędu, zamiast zgodnie z Instrukcją Zarządzania Systemami Informatycznymi[8], w dodatkowej serwerowni w innej lokalizacji Urzędu. Przez 11 dni nie odebrano dostępu do systemu informatycznego zawierającego dane osobowe,

---

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

[4] 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

[5] Dalej: IOD.

[6] Dalej: UODO.

[7] W strukturze organizacyjnej Urzędu IOD podlegał również bezpośrednio Prezydentowi będącemu jednocześnie Administratorem danych.

[8] Załącznik Nr 2 do Zarządzania Nr 179/2018 Prezydenta Miasta Stargard z dnia 20 czerwca 2018 r.

pracownikowi, który w związku ze zmianą komórki organizacyjnej Urzędu przestał być uprawniony do pracy w tym systemie.

Zgodnie z obowiązującymi w Urzędzie procedurami wewnętrznymi podjęto działania w celu minimalizacji ryzyka dostępu do sieci informatycznej poprzez m.in. zabezpieczenie wewnętrznej sieci komputerowej aplikacją firewall, wyposażenie stanowisk komputerowych w antywirusową ochronę indywidualną oraz kontrolę dostępu, a także monitorowanie przeglądania stron internetowych.

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 okresie od 25 do 30 maja 2018 r. w Urzędzie przeprowadzono analizę ryzyka związanego z przetwarzaniem danych osobowych, w tym rozpoznano rodzaje zbiorów zawierających dane osobowe oraz czynności w których niezbędne jest przetwarzanie danych osobowych, ustalono ryzyko skutków niezapewnienia ochrony danych osobowych oraz wskazano zalecenia.

W obszarach: integralności, poufności oraz dostępności danych osobowych zidentyfikowano od dziewięciu do 10 możliwych zagrożeń, w tym w szczególności: zniszczenie, kradzież, nielegalny dostęp, błędy pracowników, nielegalne oprogramowanie, nieautoryzowany dostęp do sieci informatycznej, awarie sprzętu, klęski żywiołowe. Przyjęto cztery poziomy prawdopodobieństwa wystąpienia ryzyka, tj.: niskie, średnie, wysokie oraz krytyczne. Oszacowane ryzyko ustalono na poziomie niskim oraz średnim. W celu zminimalizowania ryzyka zalecano w szczególności: podnoszenie świadomości pracowników, przestrzeganie obowiązujących przepisów oraz dbałość o powierzone mienie i dokumenty. Przeprowadzenie oceny ryzyka potwierdzone zostało pisemnymi raportami w formie odręcznych notatek IOD[10] oraz zatwierdzonymi przez Prezydenta dokumentami pn. *Analiza Szacowania Ryzyka przy przetwarzaniu danych osobowych w Urzędzie Miejskim w Stargardzie*[11] oraz *Ocena skutków zagrożenia w kontekście danego aktywu/zasobu oraz zabezpieczenie przed skutkami zagrożeń i plan działania w przypadku urzeczywistnienia się zagrożenia*[12]. Wskazane dokumenty określały min. ogólne wymogi bezpieczeństwa, ewentualne koszty związane z utratą aktywów, analizę zagrożeń i pomiar ryzyka oraz plan działań zapobiegawczych.

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 1.3.

W okresie od lutego do maja 2018 r. kierownicy poszczególnych komórek organizacyjnych Urzędu przedkładali Administratorowi bezpieczeństwa informacji[13] materiały dotyczące przetwarzanych zbiorów danych osobowych.

(akta kontroli str. 3, 306-313, 318-319, 331-333, 344-345, 349-350, 359-360, 367-368, 372-373, 377-380, 385-387, 396-402, 407, 409-422, 688-690)

[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.

[10] Sporządzonych od 25 do 30 maja 2018 r.

[11] Z 31 lipca 2018 r.

[12] Z 20 września 2018 r.

[13] Administratora bezpieczeństwa informacji wyznaczono Zarządzeniem Nr 18 Prezydenta Miasta Stargardu Szczecińskiego z 6 lipca 1999 r. w sprawie wyznaczenia administratora bezpieczeństwa informacji.

Prezydent wyjaśnił m.in.: *Analizę ryzyka przeprowadzono w odniesieniu do zbiorów danych osobowych przedłożonych (...) przez kierowników poszczególnych komórek organizacyjnych (...) w okresie od lutego do maja 2018 r. Ocena ryzyka dotyczyła konkretnych czynności lub zbiorów, zarówno dla dokumentacji papierowej, jak i elektronicznej. Została zastosowana skala dla określenia miary ryzyka. Poszczególne analizy zostały ujęte w sposób jakościowy oraz ilościowy. (...). W analizie zostały uwzględnione trzy atrybuty, o których mowa w RODO: poufność, integralność i dostępność. W oparciu o wskazane atrybuty oraz potencjalne zagrożenia dla aktywów (zasobów) zostały stworzone macierze oceny ryzyka. Z przedstawionych danych wynikało, że ryzyko przetwarzania danych mieści się w wielkościach: niskie i średnie. Nie zidentyfikowano ryzyka wysokiego oraz krytycznego.*

(akta kontroli str. 9, 240)

1.2 Do 19 czerwca 2018 r. w zakresie ochrony danych osobowych obowiązywało Zarządzenie Nr 255/2014 Prezydenta Miasta Stargardu Szczecińskiego z dnia 30 października 2014 r. w sprawie organizacji zarządzania bezpieczeństwem przetwarzanych informacji w Urzędzie Miejskim w Stargardzie[14]. W zarządzeniu określono zasady przetwarzania danych w systemach informatycznych, w tym m.in.: nadawanie uprawnień, metody i środki uwierzytelniania, tworzenie i przechowywanie kopii bezpieczeństwa, zasady przechowywania papierowych i elektronicznych nośników informacji, środki ochrony systemu, monitorowanie dostępu do danych, procedury przeglądu i konserwacji systemu, zasady przetwarzania danych w zbiorach doraźnych i przy wykorzystaniu urządzeń przenośnych, opis struktury danych osobowych[15] oraz instrukcję postępowania w przypadku naruszenia ochrony danych osobowych.

Polityki ochrony danych osobowych, które uwzględniały wymogi RODO wprowadzono do stosowania w Urzędzie od 20 czerwca 2018 r. Zarządzeniem Nr 179/2018 Prezydenta Miasta Stargard z dnia 20 czerwca 2018 r. w sprawie wprowadzenia dokumentacji w zakresie ochrony danych w Urzędzie Miejskim w Stargardzie[16]. W zarządzeniu określono zabezpieczenia techniczne, fizyczne oraz organizacyjne danych osobowych w systemach papierowych i informatycznych[17], w tym m.in.: zbiory będące podstawą opracowania rejestru czynności przetwarzania danych osobowych, procedury nadawania uprawnień oraz metody i środki uwierzytelniania w systemach informatycznych, zasady tworzenia kopii zapasowych, sposób przechowywania nośników informacji oraz środki ochrony systemu informatycznego, zasady postępowania w przypadku naruszenia ochrony danych osobowych[18]. Wskazana dokumentacja została podana do wiadomości pracownikom Urzędu[19]. Fakt ten pracownicy potwierdzili podpisem na listach prowadzonych przez Dyrektorów Wydziałów.

Wymagane przepisami art. 30 ust. 1 oraz ust. 2 RODO rejestry, w tym: czynności przetwarzania danych osobowych[20] oraz kategorii czynności przetwarzania dokonywanych w imieniu administratora prowadzi IOD odpowiednio od 1 oraz 4 czerwca 2018 r.

---

[14] Dalej: Zarządzenie Nr 255/2014.

[15] W tym nazwa i struktura zbioru.

[16] Dalej: Zarządzenie Nr 179/2018.

[17] W tym: Polityką ochrony danych w Urzędzie Miejskim w Stargardzie (Załącznik nr 1 Instrukcją Zarządzania Systemami Informatycznymi (Załącznik nr 2) oraz Procedurą postępowania w przypadku naruszenia ochrony danych osobowych (Załącznik nr 3).

[18] W tym: wzór rejestru incydentów naruszeń ochrony danych osobowych ze wskazaniem na okoliczności i skutki naruszeń oraz podjęte działania.

[19] Poprzez przekazanie od 25 do 28 czerwca 2018 r. Dyrektorom Wydziałów Urzędu pisemnej informacji z prośbą o zapoznanie podległych osób z nowymi regulacjami.

[20] Na podstawie zbiorów danych osobowych przedłożonych przez kierowników komórek organizacyjnych Urzędu.

Niedostosowanie organizacyjne Urzędu z dniem 25 maja 2018 r.[21] do wymogów RODO poprzez opóźnienie wdrożenia polityk ochrony danych osobowych oraz utworzenia rejestrów czynności przetwarzania danych osobowych i kategorii czynności przetwarzania było niezgodne odpowiednio z art. 24 ust.1 i 2 oraz art. 30 ust. 1 i 2 w zw. z art. 99 ust. 2 RODO. Nieprawidłowości szerzej opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.3, 9-10, 240-241, 248-267, 423-430, 460, 463-466, 592-620, 658-660, 682-684)

1.3 Zgodne z obowiązkiem określonym w art. 37 ust. 1 RODO z dniem 25 maja 2018 r.[22] wyznaczono IOD. Funkcja ta została powierzona osobie zatrudnionej w Urzędzie na stanowisku inspektora do spraw archiwum[23]. Wyznaczona pracownica przez 485 dni nie posiadała zakresu obowiązków, pomimo wskazania wymienionym zarządzeniem, że zakres zadań IOD wynika m.in. ze szczegółowego zakresu czynności pracownika. W trakcie kontroli NIK opracowano kartę uprawnień, obowiązków i odpowiedzialności IOD, która została przyjęta do wiadomości i stosowania przez pracownicę[24].

Prezydent wyjaśnił, m.in. że: *Zakres zadań IOD został wprowadzony w § 50 Regulaminu Organizacyjnego (...), z którym IOD został zapoznany. (...); w trakcie kontroli zakres czynności IOD został opracowany oraz podpisany 23 września 2019 r. przez Prezydenta Miasta, przyjęty do wiadomości i stosowania przez Inspektora Ochrony Danych i znajduje się w aktach osobowych pracownika.*

W okresie objętym kontrolą nie wyznaczono zastępcy IOD.

(akta kontroli str.3, 10,16-20,242, 464, 466, 476-477)

Dane IOD oraz sposób i formę kontaktu[25] opublikowano na stronie BIP Urzędu[26] oraz umieszczono w klauzulach informacyjnych wywieszonych na tablicach w budynkach zajmowanych przez Urząd[27], spełniając tym samym obowiązek wynikający z art. 37 ust. 7 RODO oraz art. 11 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[28].

(akta kontroli str.40-43, 47-49, 52-54, 60)

1.4 Zgodnie z art. 37 ust. 5 RODO IOD posiadał stosowne przygotowanie i kwalifikacje zawodowe. Osoba realizująca zadania IOD posiadała wykształcenie wyższe magisterskie oraz ukończyła studia podyplomowe o specjalności *Inspektor Ochrony Danych Osobowych.* Ponadto, odbyła cykl zewnętrznych szkoleń w zakresie ochrony danych osobowych[29], jak również związanych z archiwizacją dokumentów i ich zarządzaniem w systemach tradycyjnym oraz elektronicznym[30]:

(akta kontroli str. 21-32)

1.5 Zakres działania IOD określono w Regulaminie organizacyjnym Urzędu Miejskiego w Stargardzie[31], W regulaminie wskazano zadania IOD, w tym:

---

[21] Termin wymagany art. 99 ust. 2 RODO.

[22] Zarządzeniem Nr 152/2018 Prezydenta Miasta Stargard z dnia 23 maja 2018 r. w sprawie powołania Inspektora Ochrony Danych w Urzędzie Miejskim w Stargardzie, po zmianie Zarządzeniem Nr 339/2018 Prezydenta Miasta Stargard z dnia 7 listopada 2018 r. zmieniającym zarządzenie w sprawie powołania Inspektora Ochrony Danych w Urzędzie Miejskim w Stargardzie.

[23] Z dniem 25 maja 2018 r. pracownik został zatrudniony w wymiarze po ½ etatu na stanowiskach: inspektora ochrony danych osobowych oraz inspektora do spraw archiwum.

[24] Dokument przyjęty do stosowania dnia 23 września 2019 r.

[25] Dane aktualne w okresie objętym kontrolą.

[26] http://bipstargard.pl/BIP.aspx?Sel=7870&ident=23724

[27] Tj. w Stargardzie przy ul. Hetmana Stefana Czarnieckiego oraz Rynku Staromiejskim.

[28] Dz. U. poz. 1000, ze zm., dalej: ustawa o ochronie danych osobowych.

[29] W tym: dwa w 2018 r. oraz jedno w 2019 r.

[30] W tym: trzy w 2016 r. oraz po jednym w latach 2018-2019.

[31] Wprowadzonym Zarządzeniami Prezydenta Miasta Stargard w sprawie nadania Regulaminu organizacyjnego Urzędu Miejskiego w Stargardzie Nr: 38/2017 z dnia 30 sierpnia 2017 r.[31] (w okresie od 23 maja do 30 listopada 2018 r.) oraz 15/2018 z dnia 30 listopada 2018 r.[31] (od 1 grudnia 2018 r.); dalej: Regulamin organizacyjny.

określone w art. 39 ust. 1 RODO oraz dodatkowo m.in.: nadzorowanie, opracowanie, aktualizowanie i prowadzenie na bieżąco dokumentacji związanej z przetwarzaniem danych osobowych[32], nadzorowanie procesu wydawania i anulowania upoważnień do przetwarzania danych osobowych, jak również prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych.

Zgodnie ze schematem organizacyjnym Urzędu[33], IOD podlegał bezpośrednio Prezydentowi oraz pod względem merytorycznym Sekretarzowi Miasta[34]. Tym samym nie została zapewniona niezależność IOD, wymagana przepisami art. 38 ust 3 RODO. Nieprawidłowość szerzej opisano w sekcji *Stwierdzone nieprawidłowości.*

Opisana w pkt. 1.3 wystąpienia działalność IOD związana z pełnieniem obowiązków inspektora do spraw archiwum nie powodowała konfliktu interesów.

(akta kontroli str. 18-20, 464, 466, 572-591)

1.6 Prezes UODO o wyznaczeniu IOD został poinformowany drogą elektroniczną 8 czerwca 2018 r., tj. w terminie wynikającym z art. 10 ust.1 ustawy o ochronie danych osobowych.

(akta kontroli str. 3, 35-38)

1.7 W badanym okresie nie było zmian na stanowisku IOD.

(akta kontroli str. 3, 10,16-17, 60, 242)

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[35],
- monitorowaniu przestrzegania przepisów w zakresie ochrony danych osobowych poprzez m.in.: szkolenia pracowników uczestniczących w operacjach przetwarzania danych osobowych[36] oraz działalność audytową[37],
- prowadzenie rejestrów czynności przetwarzania danych oraz osób upoważnionych do przetwarzania danych osobowych,
- współpracy z organem nadzorczym oraz pełnieniu funkcji punktu kontaktowego dla organu nadzorczego[38].

(akta kontroli str. 3-4,141, 211-230, 246-279, 280-305, 423-462)

Ponadto, Prezydent wyjaśnił, że IOD realizował swoje zadania również m.in.: *(...) poprzez kontakty osobiste, telefoniczne i mailowe z Prezydentem oraz innymi pracownikami, przekazywanie bieżących informacji związanych z wdrożeniem i przestrzeganiem uregulowań zawartych w RODO i innymi przepisami dotyczącymi ochrony danych, (...) przeglądy przepisów obowiązujących w danych wydziałach*

---

[32] W tym m.in.: prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, prowadzenie rejestru czynności przetwarzania danych osobowych, odpowiadanie za korespondencję w obszarze danych osobowych, nadzorowanie procesu wydawania i anulowania upoważnień do przetwarzania danych osobowych, prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych.

[33] Załącznik do Regulaminu organizacyjnego.

[34] Dalej: Sekretarz.

[35] Uczestnictwo w naradach z udziałem Prezydenta i jego Zastępców, Sekretarza, Skarbnika, Dyrektorów Wydziałów Urzędu oraz Dyrektorów jednostek podległych w 2018 r. w dniach: 5 i 19 czerwca, 3 lipca,16 października, 20 listopada oraz w 2019 r. w dniach 15 stycznia, 16 kwietnia, 21 maja, 16 lipca, 3 września; przekazanie w dniach od 25 do 28 czerwca 2018 r. Dyrektorom Wydziałów Urzędu pisemnej informacji z prośbą o zapoznanie podległych osób z Zarządzeniem Nr 179/2018.

[36] W okresie od 13 czerwca 2018 r. do 12 sierpnia 2019 r. IOD przeszkoliła łącznie 66 pracowników Urzędu.

[37] Audyty przeprowadzone w obszarach: zabezpieczenia danych osobowych w Stargardzkim Centrum Wspierania Organizacji Pozarządowych (październik 2018 r.), prawidłowości przetwarzania danych osobowych w działalności Zakładowego Funduszu Świadczeń Socjalnych (czerwiec 2019 r.) oraz legalności pozyskiwania danych osobowych w procesie rekrutacji pracowników. W drugiej połowie 2019 r. zaplanowano przeprowadzenie audytów w obszarze powierzenia przetwarzania danych na podstawie umów ze Stargardzkim Towarzystwem Budownictwa Społecznego sp. z o.o. oraz w zakresie organizacji konkursów i imprez w Wydziale Kultury, Sportu i Turystyki oraz Wydziale Polityki Społecznej.

[38] W związku ze złożoną 15 maja 2019 r. skargą na pracownika Urzędu IOD konsultowała z przedstawicielem UODO obowiązek zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu.

w zakresie przetwarzania i ochrony danych osobowych; wyrywkowe przeglądy strony internetowej Urzędu Miasta (...). IOD w okresie od 25 maja do 11 września 2019 r. nie udzielał na żądanie zaleceń, co do oceny skutków - nie było przesłanek. (...).

(akta kontroli str. 10, 242-243)

1.9 Petenci Urzędu informowani byli o przetwarzaniu ich danych osobowych poprzez zamieszczenie klauzul informacyjnych na: stronie BIP Urzędu[39] oraz tablicach i w gablotach w miejscach ogólnodostępnych budynków zajmowanych przez Urząd[40], w tym: w punkcie informacyjno-kancelaryjnym, Biurze Obsługi Klienta oraz na korytarzach. Klauzule informacyjne zawierały w szczególności: dane administratora oraz IOD, cel 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. 39-55, 60-71)

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.

(akta kontroli str. 3-4,111-113)

Od 18 kwietnia[41] do 22 maja 2018 r. w obszarze przygotowania Urzędu do zmiany przepisów związanych z ochroną danych osobowych określonych w RODO, przeprowadzono jeden wewnętrzny audyt doradczy pn. *Wdrożenie nowych przepisów o ochronie danych osobowych (RODO) w Urzędzie Miejskim w Stargardzie*. Wskazany audyt[42] miał na celu pomoc oraz określenie kierunków niezbędnych działań służących dostosowaniu funkcjonowania Urzędu do nowych przepisów RODO. W trakcie czynności audytowych m.in.: dokonano analizy przepisów prawa w zakresie danych osobowych, wskazano konieczność opracowania przepisów wewnętrznych[43] oraz przeszkolenia pracowników mających dostęp do danych osobowych, a także przedstawiono propozycje wzorów dokumentów[44].

(akta kontroli str. 3-4,74, 76-110)

1.11 W okresie objętym kontrolą szkolenia pracowników Urzędu w zakresie ochrony danych osobowych na podstawie regulacji RODO, prowadzone były przez podmioty zewnętrzne oraz IOD. Od 13 czerwca 2018 r. do 12 sierpnia 2019 r. IOD przeszkoliła łącznie 66 pracowników Urzędu. Analiza szkoleń osób zatrudnionych w wydziałach: Ekonomicznym[45] oraz Gospodarki Nieruchomościami[46] wykazała, że:

– w okresie od 7 czerwca 2018 r. do 20 września 2019 r. obowiązkowe szkolenia związane z ochroną danych osobowych na podstawie regulacji RODO[47] odbyło

[39] http://bipstargard.pl/BIP.aspx?Sel=7870&ident=23724.
[40] W tym w Stargardzie przy: Rynku Staromiejskim oraz ul. Hetmana Stefana Czarnieckiego.
[41] Upoważnienie Nr 6/2018 dla Dyrektora Wydziału Audytu i Kontroli Urzędu Miejskiego w Stargardzie do przeprowadzenia audytu wewnętrznego.
[42] Informacja z audytu doradczego z 22 maja 2018 r. (MK.1720.2.2018.1)
[43] W tym m.in.: zasad szyfrowania i anonimizacji przy przetwarzaniu danych osobowych, procedur odpowiedzi na żądanie dostępu, aktualizowania, zaprzestania i ograniczania przetwarzania danych osobowych oraz procedur reagowania na naruszenie prywatności danych osobowych.
[44] W tym: zarządzenia w sprawie powołania IOD, upoważnień do przetwarzania danych osobowych, oświadczeń pracowników o przeszkoleniu w zakresie ochrony danych osobowych wraz z zobowiązaniem do zgodnego z prawem postępowania w zakresie danych osobowych, rejestru osób upoważnionych do przetwarzania danych osobowych, klauzuli informacyjnej zgodnej z RODO, formularza zgody na przetwarzanie danych osobowych, zgłoszenia w sprawie naruszania ochrony danych osobowych, raportu z naruszenia bezpieczeństwa danych osobowych, rejestru incydentów naruszeń bezpieczeństwa danych osobowych oraz umowy powierzenia przetwarzania danych osobowych.
[45] Dalej: ME.
[46] Dalej: TG.
[47] Szkolenie przeprowadzone przez: iCentrum - 17 osób oraz IOD – sześć osób.

12 pracowników na 13 zatrudnionych w ME[48] oraz 11 z 12 zatrudnionych w TG[49], w tym udział pracowników przeszkolonych w stosunku do osób upoważnionych do przetwarzania informacji wynosił odpowiednio 120%[50] i 100 %,

- w okresie od 27 do 28 maja 2019 r. dodatkowe szkolenie[51] dla chętnych odbyły dwie osoby[52],
- ze względu na długotrwałą usprawiedliwioną nieobecność nie przeszkolono dwóch pracowników[53].

(akta kontroli str. 206, 209-210,215, 218-219, 228-229, 231-234,246-247, 467-475)

1.12 Od 25 maja 2018 r. do 11 września 2019 r. na przygotowanie i realizację zadań dotyczących wdrożenia wymaganych obowiązków RODO, poniesiono wydatki w wysokości 32,7 tys. zł, w tym: 15,9 tys. zł na szkolenia i studia podyplomowe pracowników, 15,2 tys. zł na dodatkowe wynagrodzenie IOD, 0,8 tys. zł na publikacje książkowe i prenumeratę czasopism związanych z ochroną danych osobowych oraz 0,8 zł na wykonanie tablic informacyjnych z klauzulą RODO.

(akta kontroli str. 4, 6,10,176-205, 243)

1.13 W okresie objętym kontrolą[54] nie poniesiono wydatków w związku z niewłaściwym stosowaniem RODO. Ponadto, nie zostały nałożone na Urząd administracyjne kary pieniężne oraz inne sankcje lub obowiązki naprawcze.

(akta kontroli str. 4, 7, 10, 59, 243)

1.14 W kontrolowanym okresie we wszystkich 32 podległych Gminie jednostkach[55] administratorem danych osobowych ustanowiono wskazane instytucje lub osoby je reprezentujące. We wszystkich jednostkach wyznaczono IOD, w tym w sześciu przypadkach pracowników jednostek, natomiast w każdej z pozostałych 26 zawarto odrębne umowy z podmiotem zewnętrznym. W zakresie nadzoru nad podległymi jednostkami w obszarze stosowania przepisów RODO zaplanowano audyt IOD w obszarze powierzenia przetwarzania danych na podstawie umów ze Stargardzkim Towarzystwem Budownictwa Społecznego sp. z o.o.[56]. W okresie od 28 czerwca 2018 r. do 24 czerwca 2019 r. IOD Urzędu współpracował przy tworzeniu klauzul informacyjnych dotyczących prowadzonego przez Straż Miejską monitoringu miejskiego.

Prezydent wyjaśnił, że nadzór polegał również m.in. na przeglądaniu stron internetowych podległych mu instytucji w celu sprawdzenia obowiązku wyznaczenia IOD oraz zamieszczenia informacji w tym zakresie. Weryfikowano również prowadzony w Urzędzie rejestr skarg odnośnie zgłoszeń dotyczących naruszenia ochrony danych osobowych w tych jednostkach. Kierownicy 15 podległych instytucji[57] uczestniczyli w organizowanych przez Prezydenta naradach wraz z udziałem IOD Urzędu, który konsultował kwestie związane z ochroną danych osobowych. Prezydent wskazał także m.in., że: *Jednostki podległe (...) są odrębnymi Administratorami danych osobowych i (...), spoczął na nich obowiązek wyznaczenia IOD. Każda z tych jednostek wskazała iż jest osoba, która taką funkcje sprawuje. (...). W szczególnych przypadkach Inspektorzy ochrony*

[48] W tym upoważnienie do przetwarzania danych osobowych posiadało dziesięciu pracowników.
[49] W tym upoważnienie do przetwarzania danych osobowych posiadało 11 pracowników.
[50] W zakresie RODO przeszkolono również pracowników, którzy nie byli upoważnieni do przetwarzania danych, stąd udział pracowników przeszkolonych w stosunku do osób upoważnionych do przetwarzania danych osobowych wynosi 120%.
[51] Szkolenie pn. „Ochrona danych osobowych".
[52] Po jednej zatrudnionej w ME oraz TG.
[53] W tym ze względu na nieobecność: od 1 sierpnia 2016 r. do dnia zakończenia czynności kontrolnych upoważnionej do przetwarzania danych osobowych pracownicy ME oraz od 11 kwietnia 2018 r. do 20 października 2019 r. pracownicy TG.
[54] Dane na 4 września 2019 r.
[55] W tym: 22 jednostkach budżetowych, trzech instytucjach kultury oraz siedmiu spółkach miejskich.
[56] Audyt zaplanowano na drugą połowę 2019 r. Do dnia zakończenia kontroli audyt nie został przeprowadzony.
[57] W tym: pięciu jednostek budżetowych, trzech instytucji kultury oraz siedmiu spółek miejskich.

danych z jednostek podległych kontaktują się z IOD Urzędu Miejskiego Stargard bezpośrednio lub za pośrednictwem wydziału merytorycznego. (...)

(akta kontroli str. 3-4, 8-9, 268-279, 303-305,539-560)

1.15 W okresie objętym kontrolą do Urzędu nie wpłynęły skargi na podległe Miastu Stargard jednostki organizacyjne w zakresie dotyczącym przetwarzania danych osobowych. W dniu 15 maja 2019 r. złożono skargę na pracownika Urzędu w związku z naruszeniem ochrony danych osobowych, co zostało szerzej opisane w pkt 3.1 wystąpienia pokontrolnego.

(akta kontroli str.4, 126-131, 175, 235)

Stwierdzone nieprawidłowości

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

1. Zgodnie z obowiązującym w Urzędzie Regulaminem organizacyjnym, IOD podlegał[58] bezpośrednio Prezydentowi oraz pod względem merytorycznym Sekretarzowi, co było niezgodne z art. 38 ust. 3 RODO. Na podstawie tego przepisu, administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

   Prezydent wyjaśnił, że *IOD zapewniono niezależność organizacyjną poprzez odpowiednie usytuowanie w strukturze organizacyjnej. IOD jest bowiem wyodrębnioną organizacyjnie komórką, która podlega bezpośrednio Prezydentowi Miasta (co zostało wskazane na schemacie organizacyjnym pogrubioną linią). Jest on niezależny i obiektywny w realizacji swoich zadań, w zakresie których kontaktuje się bezpośrednio z Administratorem Danych. Natomiast, wskazana w schemacie organizacyjnym dodatkowa podległość Inspektora Ochrony Danych Sekretarzowi Miasta (zaznaczona przerywaną linią), dotyczy w swoich zamierzeniach głównie bieżących spraw administracyjnych. Absolutnie Sekretarz nie ingeruje w realizację zadań przez IOD. Wskazać należy, iż w § 18 pkt 9 Regulaminu organizacyjnego zapisano, że do zadań Sekretarza należy nadzór merytoryczny nad pracą podległych bezpośrednio Prezydentowi Wydziałów, w tym Inspektora Ochrony Danych. Być może niewłaściwie użyto sformułowania „merytoryczny", gdyż zapis ten nie miał na celu ograniczenia samodzielności i niezależności działania Inspektora.*

   Zdaniem NIK, merytoryczny nadzór Sekretarza nad IOD stwarza możliwość władczego oddziaływania na istotne przedmioty spraw pozostających w gestii IOD. Powyższe nie gwarantuje niezależności tego stanowiska. Podobny pogląd w sprawie gwarancji niezależności w wykonywaniu obowiązków IOD prezentuje Urząd Ochrony Danych Osobowych, który wskazuje m.in., że: *(...) bezpośrednia podległość oznacza, że w ramach podejmowanych przez siebie czynności IOD nie może podlegać jakimkolwiek innym osobom lub jednostkom organizacyjnym wchodzącym w skład struktury administratora danych (...)*[59].

   (akta kontroli str. 18-20, 464, 466, 572-591)

2. W dniu wejścia w życie RODO, tj. 25 maja 2018 r. nie przygotowano organizacyjnie Urzędu do przetwarzania danych osobowych zgodnie z wymogami tego rozporządzenia. Środki organizacyjne, służące przetwarzaniu

[58] § 11 ust. 8 Regulaminu organizacyjnego stanowiącego Załącznik do Zarządzenia Nr 338/2017 Prezydenta Miasta Stargard z dnia 30 sierpnia 2017 r. po zmianie wprowadzonej § 1 pkt 3 Zarządzenia Nr 153/2018 Prezydenta Miasta Stargard z dnia 23 maja 2018 r. oraz § 11 ust. 8, § 18 pkt 9 Regulaminu organizacyjnego stanowiącego Załącznik do Zarządzenia Nr 15/2018 Prezydenta Miasta Stargard z dnia 30 listopada 2018 r. ze zmianami wprowadzonymi Zarządzeniem Nr 64/2019 Prezydenta Miasta Stargard z dnia 1 lutego 2019 r.

[59] https://uodo.gov.pl/pl/223/713.

danych osobowych wprowadzono po obowiązującym terminie stosowania wskazanego przepisu, w tym:

- z opóźnieniem wynoszącym 26 dni wydano Zarządzenie Nr 179/2018[60], którym określono zabezpieczenia techniczne, fizyczne oraz organizacyjne danych osobowych w systemach papierowych oraz informatycznych, jak również zasady postępowania w przypadku naruszenia ochrony danych osobowych;
- siedem dni po terminie wejścia w życie wymaganych przepisów[61] utworzono rejestr czynności przetwarzania danych osobowych;
- ze zwłoką dziesięciu dni[62] wprowadzono rejestr kategorii czynności przetwarzania danych w imieniu administratora.

Obowiązujące do 19 czerwca 2018 r. regulacje wewnętrzne, w tym Zarządzenie Nr 255/2014, określały jedynie zasady przetwarzania danych w systemach informatycznych i nie spełniały wymagań RODO, w szczególności w zakresie przetwarzania danych poza tymi systemami.

Zgodnie z art. 24 ust.1 RODO uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, wymienione środki obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych (art. 24 ust.2 RODO). Na podstawie art. 30 ust. 1 i 2 RODO każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych oraz rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.

Brak dostosowania organizacyjnego Urzędu z dniem 25 maja 2018 r.[63] do wymogów RODO poprzez opóźnienie wprowadzenia polityk ochrony danych osobowych oraz utworzenia rejestrów czynności przetwarzania danych osobowych i kategorii czynności przetwarzania, było niezgodne odpowiednio z art. 24 ust.1 i 2 oraz art. 30 ust. 1 i 2 wymienionego rozporządzenia.

Prezydent wyjaśnił, m.in. że *(...) Proces ten wymagał znacznej pracy i zaangażowania. (...) osoba wyznaczona w dniu 25 maja 2018 r. na stanowisko IOD, oprócz opracowywania wymaganej dokumentacji, wykonywała inne obowiązki. Kumulacja wszystkich zadań spowodowała opóźnienie we wdrożeniu regulacji (...). Ostateczne zatwierdzenie rejestrów: czynności przetwarzania danych oraz kategorii przetwarzania danych, (...) spowodowane było faktem, że IOD został powołany do pełnienia swojej funkcji z dniem 25 maja 2018 r. W ramach realizacji swoich zadań, (...), przystąpił niezwłocznie do weryfikacji i nadzoru projektu przedmiotowych rejestrów. Po uzgodnieniu (...) ostatecznej wersji informacji wskazanych w dokumentach, zostały one przedłożone do zatwierdzenia przez administratora danych.*

(akta kontroli str.3, 9-10, 240-241, 248-267, 423-430, 460, 463-466, 592-620, 658-660, 682-684).

OCENA CZĄSTKOWA

Z dniem 25 maja 2018 r. Urząd nie został organizacyjnie przygotowany do przetwarzania danych osobowych zgodnie z RODO. Polityki ochrony danych osobowych oraz rejestry czynności przetwarzania i kategorii czynności przetwarzania danych osobowych opracowano z opóźnieniem od siedmiu do 26 dni.

[60] Zarządzenie wydano 20 czerwca 2018 r.
[61] Tj. 1 czerwca 2018 r.
[62] Tj. 4 czerwca 2018 r.
[63] Termin wymagany art. 99 ust. 2 RODO.

Prawidłowo powołano IOD oraz terminowo zgłoszono ten fakt Prezesowi UODO. Dane IOD oraz sposób i formę kontaktu podano do publicznej wiadomości. Nie zapewniono jednak wymaganej przepisami art. 38 ust. 3 RODO niezależności tej funkcji, ze względu na podporządkowanie IOD w procedurach wewnętrznych pod względem merytorycznym Sekretarzowi Miasta, zamiast Prezydentowi.
Wywiązano się z obowiązku przeszkolenia pracowników Urzędu w zakresie ochrony danych osobowych.

OBSZAR

2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych

Opis stanu faktycznego

2.1 Zgodnie z art. 30 ust. 3 RODO, rejestr czynności przetwarzania danych osobowych prowadzono w Urzędzie w formie papierowej oraz elektronicznej[64]. 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[65].

Za podstawę przetwarzania danych we wskazanych zbiorach danych osobowych przyjęto warunki określone w art. 6 ust. 1 lit. a-c RODO, w tym gdy: osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów, przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy oraz przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

(akta kontroli str. 3, 423-438)

2.2 W okresie od 4 czerwca do 9 września 2019 r. dokonano 28 aktualizacji rejestru czynności przetwarzania danych osobowych, w tym m.in. z powodu: uzupełnienia lub zmiany nazwy zbioru, dodania zbioru, usunięcie danych z kategorii lub zmiany nazwy komórki organizacyjnej Urzędu. Zaktualizowane dokumenty prowadzono w formie papierowej oraz elektronicznej.

(akta kontroli str. 439-458)

2.3 Na podstawie art. 30 ust. 2 RODO w rejestrze wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innych administratorów zamieszczono: nazwę, dane kontaktowe IOD, podmiotu przetwarzającego i administratorów, w imieniu których działa podmiot, a także ogólny opis technicznych i organizacyjnych środków bezpieczeństwa[66]. Zgodnie z obowiązkiem wynikającym z art. 30 ust. 3 RODO, wskazany rejestr prowadzono w formie papierowej oraz elektronicznej.

(akta kontroli str. 3, 459-460)

2.4 W okresie od 1 czerwca do 11 września 2019 r. dokonano pięciu 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. Zaktualizowane dokumenty prowadzono w formie papierowej oraz elektronicznej.

(akta kontroli str.461-462)

[64] Arkusz Excel.
[65] O których mowa w art. 32 ust. 1 RODO.
[66] O których mowa w art. 32 ust. 1 RODO.

2.5 W rejestrze czynności przetwarzania danych, wśród kategorii zbiorów danych osobowych przetwarzanych przez komórki organizacyjne Urzędu[67], wyodrębniono w szczególności: akta pracowników, kasę zapomogowo-pożyczkową, rekrutację, ubezpieczenia pracowników, kandydatów na członków komisji wyborczej, oświadczenia majątkowe, zapytania mieszkańców, sprawy sądowe i egzekucyjne, centralny system teleinformatyczny beneficjentów, ewidencję podatków lokalnych, ulgi w spłacie zobowiązań podatkowych, wypłatę odszkodowań za działki przejęte przez gminę, ubezpieczenia-wypadki drogowe, zezwolenia na lokalizację infrastruktury w pasie drogowym, zajęcia pasa drogowego, strefę płatnego parkowania, lokalny transport zbiorowy, utrzymanie czystości i porządku, zieleń gminną i zadrzewienia, użytkowanie wieczyste, teczki zbiorcze nieruchomości, wpłata odszkodowań właścicielom nieruchomości, trwały zarząd, zbywanie nieruchomości, wykaz uczniów, wynagrodzenia z tytułu umów zleceń i umów o dzieło, pomoc społeczną, zdrowie publiczne, działania w ramach profilaktyki antyalkoholowej, konkursy, patronaty oraz akta stanu cywilnego.

Kategorie przetwarzanych danych obejmowały m.in.: imiona, nazwisko, adres osoby fizycznej, PESEL, imiona rodziców, numer księgi wieczystej, numer geodezyjny działki, wartość i powierzchnię nieruchomości, numer aktu notarialnego, serię i numer dowodu osobistego, stan majątkowy, koszt utrzymania gospodarstwa domowego, dochody członków gospodarstwa domowego, numer telefonu, e-mail, numer rachunku bankowego, powierzchnię gospodarstwa rolnego oraz stan cywilny.

W rejestrze kategorii czynności przewarzania danych wskazano kategorie przetwarzań dokonywanych w imieniu każdego z administratorów[68], w tym m.in.: obsługę systemu teleinformatycznego *ŹRÓDŁO*[69] w zakresie spraw petentów, obsługę systemu teleinformatycznego pn. *System Informacji Oświatowej SIO*[70] odnośnie danych nauczycieli, dyrektorów szkół oraz uczniów, realizację zadań[71] pn.:*Zachodniopomorska Karta Rodziny* i *Zachodniopomorska Karta Seniora*, obsługę wyborów oraz wynikające z realizacji umów i projektów współfinansowanych z Unii Europejskiej.
Zgodnie z art. 5 ust. 1 pkt c RODO informacje zawarte w wymienionych rejestrach były niezbędne, adekwatne i stosowne do celów ich przetwarzania.

(akta kontroli str. 439-446, 461)

2.6 W okresie objętym kontrolą, 210 pracowników działających z upoważnienia administratora wpisanych było do prowadzonego przez IOD *Rejestru osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miejskim w Stargardzie*[72]. Ewidencja zawierała: imię i nazwisko pracownika, datę nadania i ustania upoważnienia[73] oraz zakres upoważnienia. Do przetwarzania danych osobowych Prezydent upoważnił dziesięciu z 13 zatrudnionych w wydziale ME pracowników oraz 11 z 12 osób pracujących w wydziale TG[74]. Weryfikacja upoważnień pracowników wydziałów ME oraz TG wykazała, że zakres ich obejmował m.in. działania w obszarze odpowiednio podatków lokalnych oraz nieruchomości i odpowiadał danym przetwarzanym w ramach obowiązków

[67] W tym np. Wydziały: ME, TG, Finansowy, Inżynierii, Gospodarki Komunalnej i Ochrony Środowiska, Polityki Społecznej, Kultury, Sportu, Turystki i Promocji, Spraw Obywatelskich, Edukacji, Urząd Stanu Cywilnego oraz Biura: Prezydenta Miasta oraz Funduszy Europejskich i Rozwoju Gospodarczego.
[68] W tym: Krajowego Biura Wyborczego, Województwa Zachodniopomorskiego oraz Ministrów: Cyfryzacji, Spraw Wewnętrznych i Administracji, Edukacji Narodowej, Inwestycji i Rozwoju oraz Spraw Wewnętrznych i Administracji.
[69] Program do edycji oraz przetwarzania danych gromadzonych w Systemie Rejestrów Państwowych.
[70] Elektroniczny system baz danych służący gromadzeniu informacji o szkołach, placówkach oświatowych, nauczycielach oraz uczniach; dalej: SIO.
[71] 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.
[72] Rejestr prowadzony elektronicznie od czerwca 2018 r.
[73] Jeżeli dotyczyło.
[74] Badaniem objęto dwa wydziału Urzędu: ME oraz TG.

służbowych. Wskazane upoważnienia wydano w okresie od 6 września 2018 r. do 10 czerwca 2019 r. i umieszczono w aktach personalnych pracowników.

Przez okres od czterech do 104 dni, 19 pracowników[75] (tj. 90 % spośród 21 kontrolowanych[76]), przetwarzało dane bez polecenia Administratora, co było niezgodne z art. 29 oraz 32 ust. 4 RODO i zostało szerzej opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 4, 209-230, 467-475, 561, 563, 621-643)

2.7 W okresie objętym kontrolą zawarto 25 umów zlecenia z pracownikami Urzędu na dostarczenie adresatom na terenie Miasta Stargard decyzji wymiaru podatku na 2019 r. Weryfikacja 10 umów wykazała, że Administrator osobnym dokumentem upoważnił zleceniobiorcę do czynności przetwarzania danych osobowych w zakresie doręczenia decyzji podatkowych. Upoważnienie wydano na okres obowiązywania umowy, tj. od 24 stycznia do 6 marca 2019 r. Ponadto, zleceniobiorcy podpisali oświadczenie o przeszkoleniu w zakresie ochrony danych osobowych w stosunku do obowiązków powierzonych umową oraz zobowiązali się m.in. do: przetwarzania danych wyłącznie w zakresie powierzonych obowiązków, zachowania w tajemnicy danych osobowych w zw. z realizacją umowy (tj. imienia, nazwiska, adresu kontaktowego), niewykorzystywania danych osobowych w celach pozasłużbowych oraz ochrony danych przed udostępnieniem osobom nieupoważnionym, ochrony danych przed przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Wskazane osoby przetwarzały dane osobowe z upoważnienia Administratora, tj. zgodnie z art. 29 oraz 32 ust. 4 RODO.

(akta kontroli str. 4, 566-569)

2.8 W okresie objętym kontrolą stosunek pracy rozwiązano z 24 pracownikami[77], natomiast 15 osób zmieniło podległość w ramach komórki organizacyjnej Urzędu[78]. Weryfikacja uprawnień dostępu do systemów informatycznych łącznie czterech pracowników ME oraz Spraw Obywatelskich i Urzędu Stanu Cywilnego[79] wykazała, że:

- trzem pracownikom MSO USC odebrano dostęp do systemów informatycznych z dniem zmiany komórki organizacyjnej lub rozwiązania stosunku pracy;
- jednej osobie z ME dostęp do systemu odebrano 11 dni po terminie zmiany komórki organizacyjnej, co było niezgodne z art. 5 ust. 1 pkt f RODO oraz art. 20 ust. 2 pkt 5 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[80] i zostało szerzej opisane w sekcji *Stwierdzone Nieprawidłowości*.

(akta kontroli: 206-208, 467, 206-208, 562, 564, 644-657)

2.9 Kontrolowana jednostka powierzyła przetwarzanie danych osobowych na podstawie 23 umów[81] zawartych z podmiotami zewnętrznymi. Wśród wskazanych umów, w czterech przypadkach[82] aktualizowano umowy, na podstawie których w okresie wcześniejszym powierzano przetwarzanie danych osobowych

[75] W tym ośmiu pracowników Wydziału ME oraz 11 pracowników Wydziału TG.
[76] Wśród pozostałych dwóch pracowników wydziału ME: jedna osoba ze względu na usprawiedliwioną nieobecność od 1 sierpnia 2016 r. do dnia zakończenia czynności kontrolnych nie przetwarzała danych w tym okresie, a drugą upoważniono w dniu zatrudnienia, tj. 10 czerwca 2019 r.
[77] W tym jedną osobą z Wydziału Spraw Obywatelskich i Urzędu Stanu Cywilnego.
[78] W tym: jedna osoba z Wydziału ME oraz dwie osoby z Wydziału Spraw Obywatelskich i Urzędu Stanu Cywilnego.
[79] Dalej: MSO USC.
[80] Dz.U. z 2017 r. poz. 2247, dalej rozporządzenie KRI.
[81] W tym umowy zawarte w okresie objętym kontrolą oraz przed 25 maja 2018 r., tj. przed wejściem w życie RODO.
[82] W tym umowy zawarte przed 25 maja 2018 r. na: świadczenie usług na pośrednictwem portalu edugrand.pl, serwis nadzoru autorskiego nad programami autorskimi, usługi zarządzania budżetem obywatelskim oraz usługi ubezpieczeniowe.

podmiotom zewnętrznym. Przedmiot umów obejmował w szczególności: świadczenie usług serwisu i nadzoru autorskiego w systemach i programach informatycznych, zarządzanie systemem budżetu obywatelskiego, usługi ubezpieczeniowe, transmisję audio-video z obrad Rady Miejskiej, wykonanie projektu planu zagospodarowania przestrzennego, asystę techniczną lokalnej bazy danych urzędu Stanu Cywilnego, asystę techniczną w zakresie oprogramowania PB_EWID oraz PB-USC, usługi w zakresie platformy zakupowej do obsługi zamówień publicznych, a także niszczenie nośników i informacji z archiwum zakładowego.

Na podstawie weryfikacji postanowień pięciu umów[83], 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 dotyczą, a także obowiązki i prawa administratora.

W zakresie monitorowania poprawności przetwarzania powierzonych danych osobowych Prezydent wyjaśnił min.: *Zakresy umów w ramach, których następuje powierzenie przetwarzania danych osobowych są monitorowane na bieżąco. (...) IOD ma za zadanie sprawdzenia poprawności i legalności zapisów danej umowy. Warunki wynikające z zapisów umowy są weryfikowane i kontrolowane przez Dyrektorów wydziałów merytorycznych. (..). W okresie od 25 maja 2018 do dnia dzisiejszego nie doszło do incydentu związanego z naruszeniem ochrony danych (przykładem jest rejestr skarg). Wykonawcy wywiązują się ze swoich obowiązków w sposób rzetelny i staranny, czego dowodem jest podpisywanie kolejnych umów z tym samym podmiotem. Nie posiadamy żadnej korespondencji związanej z nadzorowaniem podmiotów, którym powierzono przetwarzanie danych osobowych, gdyż nie było zgłoszenia z wydziału merytorycznego odnośnie nieprawidłowego wykonania umowy.*

(akta kontroli str. 4, 10, 169-174, 244, 486-488, 561, 563, 682-686)

2.10 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[84], ustawy z dnia 24 września 2010 r. o ewidencji ludności[85], ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych[86] oraz w imieniu Ministra Edukacji Narodowej na podstawie ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej[87];
- na podstawie dwóch umów, w tym z upoważnienia Krajowego Biura Wyborczego w zakresie realizacji wyborów[88] oraz Województwa Zachodniopomorskiego w zakresie zadań wynikających z realizacji programu Zachodniopomorska Karta Rodziny i Zachodniopomorska Karta Seniora[89];

[83] W tym w związku ze świadczeniem usług: transmisji audio-video z obrad Rady Miejskiej, niszczeniem nośników i informacji, serwisu i nadzoru autorskiego w systemach i programach informatycznych (22 programy), asysty technicznej w zakresie oprogramowania PB_EWID oraz wykonania projektu miejscowego planu zagospodarowania przestrzennego Miasta Stargard.
[84] Dz.U. z 2018 r. poz. 2224 ze zm.
[85] Dz.U. z 2019 r. poz. 1397.
[86] Dz.U. z 2019 r. poz.653 ze zm.
[87] Dz.U. z 2019 r. poz. 1942 ze zm.
[88] Umowa o wzajemnym powierzeniu przetwarzania danych osobowych z 25 lipca 2018 r.
[89] 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 pn. Region dla Rodziny, zmienione w zakresie powierzania przetwarzania danych osobowych Aneksem Nr 1/2018 z 28 listopada 2018 r.

– z tytułu realizacji czterech umów o dofinansowanie projektów ze środków Unii Europejskiej[90] w zakresie zadań dotyczących: modernizacji transportu miejskiego[91], podniesienia jakości usług w Urzędzie[92] oraz wsparcia miejsc wychowania przedszkolnego[93] w imieniu innych podmiotów[94], działających z upoważnienia administratora.

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[95];
– Minister Edukacji Narodowej zwracał się o monitorowanie terminowego i zgodnego ze stanem faktycznym przekazywania danych do SIO przez zobowiązane podmioty[96] oraz przekazywał wytyczne odnośnie pracy w systemie[97].

Analiza trzech umów, w tym zawartych z: DGA S.A. na rzecz projektu Przyjazny e-urząd – podniesienie jakości usług w zakresie podatków i opłat lokalnych oraz zarządzania nieruchomościami, Centrum Unijnych Projektów Transportowych w związku z modernizacją transportu miejskiego oraz 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 określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora. Ponadto, podmiot przetwarzający wywiązywał się również 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 oraz do zachowania w tajemnicy przetwarzanych danych, stosowano wymagane klauzule informacyjne RODO oraz prowadzono rejestr wszystkich kategorii czynności przetwarzania.

(akta kontroli str. 10, 244, 658-681)

2.11 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[98] obrady Rady Miejskiej w Stargardzie transmitowano i utrwalano za pomocą urządzeń rejestrujących obraz i dźwięk. Wskazany obowiązek

---

[90] W tym z: Funduszu Spójności oraz Europejskiego Funduszu Społecznego.
[91] Umowa o dofinansowanie nr POIS.06.01.00-00-0020/16-00 pn. Modernizacja transportu miejskiego polegająca na zakupie 16 autobusów energooszczędnych o najmniejszej emisji CO_2 i zanieczyszczeń zawarta 3 sierpnia 2017 r. z Centrum Unijnych Projektów Transportowych oraz zmieniona w zakresie powierzenia przetwarzania danych osobowych 12 października 2018 r. Aneksem nr 2.
[92] Umowa partnerska na rzecz realizacji Projektu Przyjazny e-urząd – podniesienie jakości usług w zakresie podatków i opłat lokalnych oraz zarządzania nieruchomościami w sześciu Miastach: Stargard, Gryfino, Mińsk Mazowiecki, Głogów, Nowy Targ oraz Zgorzelec zawarta 5 października 2018 r. z DGA S.A.
[93] W tym 1 kwietnia 2019 r. zawarto z Fundacją Milion dwie umowy wsparcia miejsc wychowania przedszkolnego, tj. dotyczące Przedszkola Miejskiego nr 1 oraz Przedszkola Miejskiego nr 5.
[94] W tym w imieniu: Centrum Unijnych Projektów Transportowych na zlecenie Ministra Inwestycji i Rozwoju, DGA S.A. na zlecenie Ministra Spraw Wewnętrznych i Administracji oraz Fundacji „Milion" na zlecenie Województwa Zachodniopomorskiego.
[95] Pismo Ministerstwa Spraw Wewnętrznych i Administracji DSO-WSC-6000-17-25/2018 z 21 maja 2018 r.
[96] 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.
[97] Informacja z 3 października 2019 r. dotycząca weryfikacji danych w SIO.
[98] Dz. U. z 2019 r. poz. 506 ze zm.; dalej uosg.

realizowano w wyniku zawarcia umów z podmiotami zewnętrznymi[99]. Na stronie BIP Urzędu[100] oraz przed wejściem do Sali Sesyjnej, w której odbywały się obrady Rady Miejskiej w Stargardzie umieszczono informację o transmitowaniu i utrwalaniu, zgodnie z art. 20 ust. 1b uosg za pomocą urządzeń rejestrujących obraz i dźwięk. 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. 10, 50, 55-58, 60, 66, 114-125, 164-174, 244)

2.12 Zgodnie z Zarządzeniem Nr 179/2018[101] przewidziano środki fizyczne polegające na ochronie obszaru przetwarzania danych osobowych poza godzinami pracy poprzez m.in: ochronę fizyczną budynku Urzędu oraz zastosowanie systemu alarmowego[102] w wyznaczonych lokalizacjach. Do zabezpieczeń technicznych zaliczono[103]: zabezpieczenie wewnętrznej sieci komputerowej urządzeniem firewall, wyposażanie stanowisk komputerowych w antywirusową ochronę indywidualną oraz kontrolę dostępu do nich. Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych przewidziano[104] wykonywanie kopii zapasowych zbiorów danych, w tym przyrostowych oraz awaryjnych - przed oraz po dokonaniu istotnych zmian konfiguracyjnych systemu. Ponadto, wskazano że, wykonywane w danym dniu kopie zapasowe zabezpieczone są przed nieumyślnym skasowaniem i przechowywane w dwóch różnych lokalizacjach Urzędu. Strategiczne kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych polecono przechowywać w kasie pancernej. W celu ochrony przed nieautoryzowanym dostępem do sieci lokalnej przewidziano[105] 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. 603, 610, 613)

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

- dozorowania, w tym ochrony mienia terenu oraz obiektu Urzędu; do obowiązków pracownika ochrony należała w szczególności systematyczna kontrola pod względem bezpieczeństwa wszystkich kondygnacji obiektu oraz ogrodzenia terenu poprzez sprawdzenie zabezpieczeń, urządzeń i zamknięć;
- całodobowej ochrony w systemie monitoringu sygnałów alarmowych[106] 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;

---

[99] W tym umowy zawarte: 25 czerwca 2018 r. na okres od 1 września 2018 r. do 31 sierpnia 2019 r. oraz 27 sierpnia 2019 r. na okres od 1 września 2019 r. do 31 sierpnia 2020 r.

[100] http://bipstargard.pl/BIP.aspx?Sel=7870&ident=23724&js=1

[101] Załącznik Nr 1- Polityka Ochrony Danych (§10 ust. 4).

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

[103] Załącznik Nr - 1 Polityka Ochrony Danych (§10 ust. 30 oraz Załącznik nr 2 - Instrukcja Zarządzania Systemami informatycznymi w zakresie przetwarzania danych osobowych (rozdział 7, pkt 7.1.-7.2).

[104] Załącznik nr 2 - Instrukcja Zarządzania Systemami informatycznymi w zakresie przetwarzania danych osobowych (rozdział 5, pkt 5.1.-5.2).

[105] Załącznik nr 2 - Instrukcja Zarządzania Systemami informatycznymi w zakresie przetwarzania danych osobowych (rozdział 7, pkt 7.2).

[106] Na podstawie umowy zawartej ze spółką z o.o. 20 grudnia 2016 r. z okresem obowiązywania od 1 stycznia 2017 r. do 31 grudnia 2019 r.

- okresowych przeglądów, zabiegów konserwacyjnych i napraw serwisowych instalacji alarmowej pomieszczeń objętych lokalnym systemem alarmowym[107];
- monitorowania sygnałów z systemu sygnalizacji pożaru, zainstalowanego w budynku Urzędu[108]; zleceniobiorcę zobowiązano m.in. do monitorowania sygnałów z systemu sygnalizacji pożaru poprzez przyjmowanie sygnałów z tego systemu i przekazywanie sygnałów alarmu pożaru do Państwowej Straży Pożarnej;
- konserwację i bieżące naprawy urządzeń i instalacji automatycznej sygnalizacji pożaru[109] w budynkach zajmowanych przez Urząd;

co było zgodne z Zarządzeniem Nr 179/2018[110].

(akta kontroli str. 570-571)

Ponadto, w jednym z budynków zajmowanych przez Urząd wydzielano pomieszczenie będące środowiskiem pracy komputerów pełniących rolę serwerów – tzw. serwerownię. 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,
- pomieszczenie wyposażono w systemy klimatyzacji oraz czujników monitorujących wilgotność i temperaturę, a także jedną czujkę dymu;
- przez serwerownię nie przebiegają rury wodno-kanalizacyjne;
- pomieszczenie nie zostało dostatecznie zabezpieczone przed utratą danych, co było niezgodne z art. 32 ust. 1 pkt b w zw. z art. 5 ust. 1 pkt f rozporządzenia RODO i zostało szerzej opisana w Sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 520-531, 533-535, 561-563)

Zgodnie z Zarządzeniem Nr 179/2018[111] ryzyko działania szkodliwego oprogramowania oraz próby nieautoryzowanego dostępu do sieci informatycznej minimalizowano poprzez zabezpieczenie wewnętrznej sieci komputerowej aplikacją firewall, wyposażeniem stanowisk komputerowych w antywirusową ochronę indywidualną i kontrolę dostępu do nich oraz monitorowanie przeglądania stron internetowych.

(akta kontroli str. 520-530, 536-538, 603, 613, wydruki z systemów)

W celu ciągłości działania systemów informatycznych wykonywano ich kopie zapasowe, które przechowywane były w jednym z budynków Urzędu w osobnym pomieszczeniu niż bazy, z których je tworzono. Kopii całościowych nie przechowywano dodatkowo w innym budynku Urzędu, pomimo wskazania takiego wymogu w pkt. 5.1. ppkt 4 Instrukcji Zarządzania Systemami Informatycznymi, co zostało opisane szerzej w Sekcji *Stwierdzone Nieprawidłowości*.

Zgodne z pkt. 5.2 Instrukcji Zarządzania Systemami Informatycznymi kopie zapasowe zbiorów danych, oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych oraz dyski z serwerów wycofanych z użycia umieszczono w zamykanym sejfie.

---

[107] Na podstawie dwóch umów zawartych ze spółką z o.o.: 7 grudnia 2015 r. z okresem obowiązywania od 1 stycznia 2016 r. do 31 grudnia 2018 r. oraz 17 grudnia 2018 r. z okresem obowiązywania od 1 stycznia do 31 grudnia 2019 r.

[108] Na podstawie umowy zawartej ze spółką z o.o. 2 grudnia 2016 r. z okresem obowiązywania od 1 stycznia 2017 r. do 31 grudnia 2019 r.

[109] Na podstawie dwóch umów zawartych ze spółką jawną: 24 kwietnia 2018 r. z okresem obowiązywania od 1 maja 2018 r. do 30 kwietnia 2019 r. oraz 16 kwietnia 2019 r. z okresem obowiązywania od 1 maja 2019 r. do 30 kwietnia 2021 r.

[110] Załącznik Nr 1 - Polityka Ochrony Danych (§ 10 ust. 4).

[111] W tym § 10 ust. 3 Polityki Ochrony Danych (Załącznik Nr 1) oraz pkt 7.1.-7.2 Instrukcji Zarządzania Systemami informatycznymi w zakresie przetwarzania danych osobowych (Załącznik nr 2).

Czas przechowywania wykonanej w danym dniu kopii przyrostowej wynosił sześć miesięcy, cztery tygodnie i siedem dni, pomimo że zgodnie z pkt. 5.1. ppkt 4 Instrukcji Zarządzania Systemami informatycznymi w zakresie przetwarzania danych osobowych, wskazane kopie należało przechowywać przez okres dwóch miesięcy.

W sprawie przechowywania kopii zapasowych przez okres dłuższy niż wymagany procedurami wewnętrznymi Prezydent wyjaśnił, że *Okres przechowywania niektórych kopii zapasowych wynosi czasem więcej niż dwa miesiące. Wynika to ze specyfiki danych poszczególnych kopii np. zamknięcia roku obrachunkowego, stan danych na określony dzień, dane instalacyjne systemów itp.*

(akta kontroli str. 520-530, 532-535, 561-564, 610)

2.13 Zgodnie z *Instrukcją Zarządzenia Systemami Informatycznymi w zakresie przetwarzania danych osobowych* [112] w celu zapewnienia zabezpieczenia dostępu do sieci lokalnej przyjęto użycie identyfikatora oraz hasła[113]. Proces ten wymagał uwierzytelnienia uprawnionego użytkownika za pomocą identyfikatora i hasła dostępu[114]. Przyjęto również m.in., że zmiana haseł następuje m.in. niezwłocznie w przypadku podejrzenia jego ujawnienia[115]. Przy każdorazowym opuszczeniu stanowiska komputerowego pracownicy zobowiązani byli m.in. do ręcznego ustawienia blokady ekranu[116].

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. 478-479, 608-609)

Stwierdzone nieprawidłowości

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

1. Zabezpieczenie fizyczne pomieszczenia serwerowni nie gwarantowało w sposób dostateczny ochrony danych osobowych przed ich utratą, w szczególności ze względu na:
   - możliwość nieautoryzowanego dostępu do pomieszczenia przez osoby postronne poprzez: usytuowanie serwerowni w sąsiedztwie innych pomieszczeń ogólnodostępnych i łatwą jej lokalizację[117], brak zabezpieczenia wejścia do pomieszczenia systemami alarmowymi włamania, monitoringu wizyjnego oraz elektronicznej weryfikacji dostępu, a także wyposażenie w drzwi wejściowe nieposiadające atestu antywłamaniowego;
   - niedostateczne zminimalizowanie ryzyka zagrożenia pożarowego w serwerowni, w tym: wyposażenie pomieszczenia w nieposiadające atestu przeciwpożarowego[118] drzwi drewniane oraz pokrycie podłogowe niespełniające wymagań przeciwpożarowych[119], a także brak w pomieszczeniu odpowiedniego dla sprzętu informatycznego systemu gaszenia.

Powyższy stan nie gwarantował odpowiedniego bezpieczeństwa danych osobowych, o którym mowa w art. 5 ust. 1 lit f RODO. Na podstawie wskazanego przepisu dane osobowe muszą być przetwarzane w sposób zapewniający

[112] Załącznik nr 2 do Zarządzenia Nr 179/2018.
[113] Załącznik nr 2 do Zarządzenia Nr 179/2018, rozdział 3 pkt 3.1, ppkt 2.
[114] Załącznik nr 2 do Zarządzenia Nr 179/2018, rozdział 3 pkt 3.1, ppkt 4.
[115] Załącznik nr 2 do Zarządzenia Nr 179/2018, rozdział 3 pkt 3.1, ppkt 5 oraz ppkt 7.
[116] Załącznik nr 2 do Zarządzenia Nr 179/2018, rozdział 4, pkt 4.2., ppkt 2.
[117] Wejście do serwerowni usytuowane w holu użytkowanym przez petentów Urzędu.
[118] O zapewnieniu ognioodporności.
[119] Wykładzina podłogowa nie posiadała atestu p.poż.

odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (integralność i poufność). Ponadto, zgodnie z art. 32 ust. 1 pkt b administrator zobowiązany jest wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, w tym zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.

Prezydent wyjaśnił, m.in. że: *Realizacja obowiązków (tj. zabezpieczenie fizyczne pomieszczenia serwerowni w postaci antywłamaniowych, ognioodpornych drzwi wraz z elektroniczną weryfikacją dostępu) została rozłożona w czasie ze względu na ograniczone możliwości finansowe budżetu miasta. Zakup takich drzwi planowany jest w budżecie na 2020 r. Odpowiednie pokrycie podłogowe oraz gaśnica również zostanie zakupiona w 2020 r. Aktualnie serwerownia zabezpieczona jest poprzez kraty w oknie, ochronę fizyczną budynku, czujniki dymowe, temperatury i wilgotności, klimatyzatory.*

Dane gromadzone w serwerowni stanowią informacje dotyczące najważniejszych sfer działalności Urzędu. Ich utrata lub brak dostępności może doprowadzić do sytuacji kryzysowej, w tym strat finansowych. Urządzenia informatyczne w serwerowni pobierają moc energetyczną na stałym, bardzo wysokim poziomie, co stwarza ryzyko zwarcia elektrycznego, a w konsekwencji wywołanie pożaru. Tym samym koniecznym jest, ognioodporne wyposażenie serwerowni. Gwarancją bezpieczeństwa informacji oraz zapewnienia optymalnych warunków pracy dla sprzętu sieciowo-serwerowego stanowią w szczególności zabezpieczenia fizyczne minimalizujące wszelkie potencjalne ryzyka zagrożenia pożarowego oraz nieautoryzowanego dostępu do danych.

(akta kontroli str. 520-531, 533-535, 561-563)

2. Wykonywane w Urzędzie całościowe kopie bezpieczeństwa przechowywane były tylko w jednym z budynków Urzędu, zamiast również w jego drugiej lokalizacji, co było niezgodne z pkt. 5.1. ppkt 4 Instrukcji Zarządzania Systemami Informatycznymi.
   Na podstawie wskazanej regulacji, kopie całościowe należało przechowywać również w zamykanym na klucz metalowym sejfie dodatkowej serwerowni w innej lokalizacji.

   Środowisko pracy komputerów pełniących rolę serwerów, wydzielano tylko w jednym z budynków Urzędu. W żadnym z pomieszczeń innego budynku Urzędu nie zorganizowano pomieszczenia serwerowni oraz nie wykonywano i nie przechowywano kopii zapasowych.

   Prezydent wyjaśnił, że: *Całościowe kopie bezpieczeństwa baz danych oraz kopie przyrostowe serwera plików przechowywane będą dodatkowo w serwerze backupowym w drugiej lokalizacji Urzędu (...), po zakupie odpowiedniego urządzenia. Planowane jest to w IV kwartale 2019 r.*

   (akta kontroli str. 520-531, 533-535, 561-563)

3. W okresie od 25 maja do 6 września 2018 r. 19 spośród 21 kontrolowanych pracowników Urzędu (tj. ponad 90%), przetwarzało dane osobowe bez upoważnienia Administratora[120].
   Upoważnienia ośmiu pracowników ME[121] oraz 11 TG[122], wydano dopiero 6 września 2018 r., zamiast z dniem 25 maja 2018 r., tj. w którym powstał obowiązek

[120] Wśród pozostałych dwóch pracowników ME: jedna osoba ze względu na usprawiedliwioną nieobecność od 1 sierpnia 2016 r. do dnia zakończenia czynności kontrolnych nie przetwarzała danych w tym okresie, a drugą upoważniono w dniu zatrudnienia, tj. 10 czerwca 2019 r.
[121] W tym do działań w zakresie podatków lokalnych.

stosowania rozporządzenia RODO[123] lub z dniem powrotu pracownika po długotrwałej usprawiedliwionej nieobecności[124].

Od czterech do 104 dni wskazani pracownicy przetwarzali dane osobowe bez upoważnienia Administratora, co było niezgodne z art. 29 oraz 32 ust. 4 RODO.

Zgodnie z art. 29 RODO każda osoba działająca z upoważnienia administratora i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Ponadto, na podstawie art. 32 ust. 4 tego rozporządzenia administrator podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.
W sprawie wydania wskazanych upoważnień ponad trzy miesiące po wejściu w życie RODO Prezydent wyjaśnił, że: *W związku z opóźnieniem wdrożenia dokumentacji przystosowującej Urząd do wymagań RODO, proces wydawania upoważnień został przesunięty na dalszy termin. Na tą sytuację złożył się również okres urlopowy oraz natłok innych obowiązków. Po okresie 6 września 2018 r, żaden z pracowników nie przetwarzał danych osobowych bez posiadania pisemnego upoważnienia Administratora. Obecnie dzięki wdrożonym procedurom każdy pracownik posiada stosowane upoważnienie zgodne z zakresem obowiązków i wykonywanych zadań.*

(akta kontroli str. 4, 209-230, 467-475, 561, 563, 621-643)

4. W okresie od 1 do 11 czerwca 2019 r. nie odebrano dostępu do systemu informatycznego zawierającego dane osobowe, pracownikowi, który w związku ze zmianą komórki organizacyjnej Urzędu przestał być uprawniony do wykorzystywania tego systemu. Pracownikowi ME dostęp do systemu *Nieruchomości Osób Prawnych - Wymiar* odebrano dnia 11 czerwca 2019 r., zamiast z dniem zmiany komórki organizacyjnej, tj. 1 czerwca 2019 r, co było niezgodne z art. 5 ust. 1 pkt f RODO. Ponadto, stanowiło naruszenie art. 20 ust. 2 pkt 5 rozporządzenia KRI.
Na podstawie art. 5 ust. 1 pkt. 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. Zgodnie z art. 20 ust. 2 pkt 5 rozporządzenia KRI zapewnienie bezpieczeństwa informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4 tego przepisu[125].

Prezydent wyjaśnił, że: *Dostęp osoby do określonych zasobów jest blokowany niekiedy do kilku dni po dacie zmiany komórki organizacyjnej. Wiąże to się z czasem jaki jest potrzebny do przekazania obowiązków innej osobie lub innymi czynnościami natury organizacyjnej*.

(akta kontroli: 206-208, 467, 206-208, 562, 564, 644-645)

OCENA CZĄSTKOWA

Prowadzone rejestry czynności przetwarzania danych osobowych oraz wszystkich kategorii czynności przetwarzania określały zgodnie z art. 30 ust. 1 i 2 RODO wszystkie wymagane elementy. Również na podstawie art. 28 ust. 3 tego rozporządzenia, przy zawieraniu umów, którymi powierzono dane osobowe

[122] W tym do działań w obszarze nieruchomości.
[123] 17 przypadków.
[124] Dwa przypadki.
[125] W art. 20 ust. 2 pkt 4 rozporządzenia KRI mowa jest o osobach zaangażowanych w proces przetwarzania informacji posiadających stosowne uprawnienia i uczestniczące w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

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.

Nie wszystkie stosowane zabezpieczenia fizyczne zapewniały pełną ochronę danych osobowych przed ich utratą. W szczególności możliwość nieautoryzowanego dostępu do pomieszczenia serwerowni przez osoby postronne oraz niedostateczne zminimalizowanie ryzyka zagrożenia pożarowego nie gwarantowało bezpieczeństwa, o którym mowa w art. 5 ust. 1 pkt f RODO. Również, niezgodnie z regulacjami wewnętrznymi kopie bezpieczeństwa przechowywane były tylko w jednym pomieszczeniu Urzędu, zamiast także w dodatkowej serwerowni w innej lokalizacji. W okresie od 25 maja do 6 września 2018 r., ponad 90% objętych kontrolą pracowników, przetwarzało dane osobowe bez upoważnienia Administratora, co było niezgodne z art. 29 oraz 32 ust. 4 RODO. Ponadto, przez 11 dni nie odebrano dostępu do systemu informatycznego zawierającego dane osobowe, pracownikowi, który w związku ze zmianą komórki organizacyjnej Urzędu przestał być uprawniony do korzystania z tego systemu.

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. 132)

W dniu 15 maja 2019 r. złożono skargę na pracownika Urzędu w związku z zagrożeniem bezpieczeństwa ochrony danych osobowych. Zdaniem skarżącej, do naruszenia doszło w wyniku skierowania[126] do osoby fizycznej oraz jednocześnie do wiadomości skarżącej pisma[127], którym w sposób nieuprawniony udostępniono adresatowi głównemu oraz odbiorcy do wiadomości[128] ich dane osobowe, w tym: imię, nazwisko oraz adres kontaktowy. Według pracowników Urzędu[129], przed skierowaniem pisma, skarżąca oraz główny adresat dobrowolnie podały swoje dane osobowe podczas jednoczesnej wizyty interesantów u Zastępcy Prezydenta Miasta. Tym samym w ocenie pracowników Urzędu[130] nie doszło do wskazanego naruszenia.

Na podstawie obowiązującej w Urzędzie Procedury postępowania w przypadku naruszenia ochrony danych osobowych[131] w związku z podejrzeniem naruszenia ochrony danych osobowych, IOD m.in.: sporządziła notatkę ze zdarzenia, odebrała pisemne wyjaśnienia od osób, które ujawniły naruszenie oraz zidentyfikowała rodzaj i skalę zdarzenia. W ocenie IOD, ryzyko naruszenia praw i wolności osób fizycznych których dane naruszono, nie skutkowało fizyczną, materialną lub niematerialną

[126] Przez Dyrektora Wydziału Edukacji Urzędu.
[127] Pismo nr SE.4456.44.2019.2 z 30 kwietnia 2019 r. dotyczące wyników rekrutacji dzieci do przedszkola.
[128] Tj. osobie skarżącej.
[129] W tym: Dyrektora Wydziału Edukacji oraz Inspektora z Biura Prezydenta Miasta.
[130] W tym: Dyrektora Wydziału Edukacji oraz Inspektora z Biura Prezydenta Miasta.
[131] § 5 pkt 1-4 Załącznika nr 3 do Zarządzenia Nr 179/2018 Prezydenta Miasta Stargard z 20 czerwca 2018 r.

szkodą. W konsekwencji, informacja o naruszeniu ochrony danych osobowych nie została przekazana organowi nadzorczemu.

W sprawie braku zawiadomienia UODO Prezydent wyjaśnił, że: *Skarga została przyjęta i rozpatrzona zgodnie z obowiązującą procedurą postępowania w przypadku naruszenia ochrony danych osobowych. Zebrane dowody wskazywały, iż dane które zostały przekazane do wiadomości drugiej stronie to imię, nazwisko i adres kontaktowy. Dokonano oceny skali wielkości naruszenia na podstawie metody Enisa (ENIS-Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji) - narzędzia pozwalającego na ocenę wagi naruszenia danych i ułatwienia podjęcia decyzji zarówno o powiadomieniu organu, jak i osób, których dane zostały naruszone. Na podstawie dokonanych wyliczeń stwierdzono niską wagę naruszenia - osoby nie zostały dotknięte naruszeniem i fakt ten nie podlegał zgłoszeniu do Urzędu Ochrony Danych Osobowych- incydent został zarejestrowany w rejestrze naruszeń (również zgodnie z zaleceniem przedstawiciela UODO, z którym IOD odbył rozmowę telefoniczną w dniu 16 maja 2018 r.).*

Ponadto, pismem z 20 maja 2019 r. Prezydent m.in.: przeprosił skarżącą za zaistniałą sytuację, przedstawił okoliczności zdarzenia oraz zapewnił o podjęciu starań zapobiegających podobnym incydentom.

Działania Prezydenta były zgodne z art. 33 ust. 1 oraz art. 34 ust. 1 RODO.

(akta kontroli str. 132, 135-144, 464-466 ,484-485, 617-619)

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

(akta kontroli str. 11, 133-134. 244-245)

3.3 Na stronie BIP Urzędu[132] oraz w pomieszczeniach ogólnodostępnych w budynkach zajmowanych przez Urząd[133] umieszczano m.in.: informacje o organizacji imprez kulturalno-rozrywkowych, zasady przetwarzania danych osobowych, wzory wniosków i formularzy urzędowych, ogłoszenia oraz wyniki dotyczące naboru na wolne stanowiska pracy, zasady wynajmowania lokali komunalnych, postanowienia sądów o podjęciu zawieszonych postępowań, zarządzenia o ustanowieniu kuratora, ogłoszenia o nabyciu spadku, informacje o sesji Rady Miejskiej, ogłoszenia o zamianie lokali komunalnych, decyzje w sprawach usunięcia drzew oraz obwieszczenia komornicze o licytacji nieruchomości. Wymienione publikacje nie zawierały informacji mogących naruszać ochronę danych osobowych. Nie upubliczniano również zbędnych i nieadekwatnych do celu, informacji o osobach fizycznych.

(akta kontroli str.39-55, 145-163)

3.4 W regulacjach wewnętrznych odniesienie do usuwania i niszczenia zbędnej dokumentacji zawarto w szczególności w:

- Polityce Ochrony Danych[134], poprzez wskazanie, że dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści;
- Instrukcji Zarządzania Systemami Informatycznymi w zakresie przetwarzania danych osobowych poprzez wskazanie, że: dane osobowe w postaci elektronicznej należy usunąć z nośnika informacji w sposób uniemożliwiający ich odtworzenie, nie później niż po upływie trzech dni po wykorzystaniu tych danych[135], a nośniki z danymi osobowymi należy niszczyć zgodnie z przepisami

[132] http://bipstargard.pl/BIP.aspx?Sel=7870&ident=23724
[133] Tj. w Stargardzie przy ul. Hetmana Stefana Czarnieckiego oraz Rynku Staromiejskim.
[134] Załącznik Nr 1 do Zarządzenia Nr 179/2018 (§ 10 ust. 2 pkt 12).
[135] Z zastrzeżeniem ich przechowywania, gdy obowiązek taki wynika z przepisów odrębnych.

dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi i prawnymi; niszczenie dokumentów i tymczasowych wydruków następuje w niszczarkach niezwłocznie po ustaniu celu ich przewarzania; sposobami usuwania danych z urządzeń lub nośników elektronicznych są programowe i sprzętowe kasowanie danych[136].

W okresie objętym kontrolą w związku z usuwaniem zbędnej dokumentacji zawarto jedną umowę[137] z podmiotem zewnętrznym. Wykonawcę zobowiązano do jednorazowego i całkowitego zniszczenia nośników danych w zabezpieczonej przed dostępem osób trzecich i wglądem do treści danych, przemysłowej instalacji niszczącej. W związku z realizacją postanowień wskazanej umowy zleceniobiorcy powierzono przetwarzanie danych osobowych, co zostało szerzej opisane w pkt 2.9 wystąpienia. Wykonanie usługi potwierdzono certyfikatem zniszczenia odebranych danych[138]. Dokumentacja została przeznaczona do usunięcia po uzyskaniu 7 maja oraz 26 października 2018 r. zgody Kierownika Oddziału w Stargardzie Archiwum Państwowego w Szczecinie na brakowanie dokumentacji niearchiwalnej.

Ponadto, w dniach: 19 listopada 2018 r., 17 maja oraz 4 i 24 czerwca 2019 r. pracownicy Urzędu protokolarnie zniszczyli dokumentację z procedury rekrutacyjnej.

W sprawie sposobu uregulowania zasad usuwania i niszczenia zbędnej dokumentacji oraz zbędnych nośników danych Prezydent wyjaśnił, m.in. że: *(...) Archiwum Zakładowe Urzędu Miejskiego niszczy dokumentację, w zakresie której znajdują się dane osobowe, w oparciu o przepisy (...) Instrukcji archiwalnej stanowiącej załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych, rzeczowych wykazów akt oraz instrukcji w sprawie działania archiwów zakładowych. Po uzyskaniu stosownych zgód Dyrektorów Wydziałów, dokumentacja jest niszczona protokolarnie na niszczarce Urzędu Miejskiego lub przez profesjonalną firmę, która gwarantuje wszelkie zabezpieczenia techniczne i organizacyjne zgodne z art. 28 RODO.*

(akta kontroli str. 11, 245, 486-515, 603, 611-612)

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 ME oraz TG 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 1 czerwca 2018 r. do 10 czerwca 2019 r. informację o przetwarzaniu danych osobowych przyjęło do wiadomości 12 pracowników z 13 zatrudnionych w ME oraz 11 z 12 zatrudnionych w TG;
- ze względu na długotrwałą usprawiedliwioną nieobecność informacji o przetwarzaniu danych osobowych nie przyjęło dwóch pracowników[139].

[136] Załącznik Nr 2 do Zarządzenia Nr 179/2018 (ppkt 4 oraz 6 pkt 6.1, ppkt 2 pkt 6.3, pkt 6.5).
[137] Umowa z 10 lipca 2019 r.
[138] Certyfikat z 31 lipca 2019 r.
[139] W tym ze względu na nieobecność: od 1 sierpnia 2016 r. do zakończenia czynności kontrolnych pracownicy ME oraz od 11 kwietnia 2018 r. do 20 października 2019 r. pracownicy TG.

Prezydent wyjaśnił również m.in, że wskazana *(...) klauzula informacyjna umieszczona jest w miejscu widocznym w pokoju pracownika prowadzącego akta osobowe (...)*.

Działania Administratora w zakresie informowania pracowników o przetwarzaniu ich danych osobowych były zgodne z art. 13 RODO.

(akta kontroli str.11, 209-210, 236, 238,245, 467-475)

3.6 W okresie od 1 października 2018 r. do 10 maja 2019 r. zawarto z osobami fizycznymi 69 umów zlecenia na obsługę informatyczną obwodowych komisji wyborczych powołanych do przeprowadzenia wyborów posłów do Parlamentu Europejskiego. 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. 4, 516-519,565)

3.7 W okresie objętym kontrolą przeprowadzono w Urzędzie 11 zewnętrznych naborów na stanowiska urzędnicze. Zgodnie z art. 13 ust. 1 i 2 RODO publikowane na stronie BIP Urzędu ogłoszenia o naborze pracowników zawierały m.in.: dane kontaktowe Administratora oraz IOD, cel[140], podstawę prawną i okres[141] 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. 150-152, 480-483)

3.8 Zgodnie z rejestrem czynności przetwarzania danych osobowych, dla przechowywania informacji o kandydatach przyjęto trzymiesięczny okres.

Odnośnie uzasadnienia do wskazanego terminu Prezydent wyjaśnił, że: *(...) W tym czasie osoby, z którymi nie została podpisana umowa mogą odbierać swoje dokumenty, a po upływie tego terminu pozostałe oferty kandydatów zostają komisyjnie zniszczone. Zasada przechowywania dokumentacji przez wskazany okres sugerowana jest zapisem art. 15 ust 3. ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych. Ze względu na możliwość wycofania swojej kandydatury i rezygnacji z pracy każdego z kandydatów pracodawca pozostawia sobie możliwość wyłonienia pracownika spośród kolejnych ofert.*

(akta kontroli str. 423, 439, 464, 466)

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.

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

[141] 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.

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

1. Zapewnienie w regulacjach wewnętrznych podległości służbowej Inspektora Ochrony Danych jedynie Prezydentowi.
2. Zabezpieczenie pomieszczenia serwerowni przed utratą danych poprzez zminimalizowanie ryzyka nieautoryzowanego dostępu oraz zagrożenia pożarowego.
3. Przechowywanie kopii bezpieczeństwa zgodnie z regulacjami wewnętrznymi, tj. w dwóch różnych lokalizacjach Urzędu.
4. Upoważnianie pracowników do przetwarzania danych osobowych z chwilą powstania stosownego obowiązku.
5. Odbieranie bez zbędnej zwłoki uprawnień w systemach informatycznych pracownikom, którzy zmienili miejsce pracy w Urzędzie.

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.

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.

Szczecin, 13 listopada 2019 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie
Dyrektor

Kontroler
Katarzyna Kozłowska
starszy inspektor kontroli państwowej

..... podpis

..... podpis