NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR.410.013.01.2019

Pan Piotr Ćwik
Wojewoda Małopolski
ul. Basztowa 22
31-156 Kraków

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie
ul. Łobzowska 67, 30-038 Kraków
T +48 12 342 34 00, F +48 12 342 34 44
lkr@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Małopolski Urząd Wojewódzki w Krakowie, ul. Basztowa 22, 31-156 Kraków *(MUW; Urząd)*
Kierownik jednostki kontrolowanej	Piotr Ćwik, Wojewoda Małopolski *(Wojewoda)* od 3 czerwca 2017 r. (akta kontroli str. 8, 11)
Zakres przedmiotowy kontroli	1. Organizacja ochrony danych osobowych w MUW. 2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych. 3. Zarządzanie danymi osobowymi przetwarzanymi, w tym gromadzonymi w MUW.
Okres objęty kontrolą	Od 25 maja 2018 r. do czasu zakończenia czynności kontrolnych, tj. do 30 grudnia 2019 r. oraz dla zdarzeń wcześniejszych, jeśli miały wpływ na kontrolowaną działalność.
Podstawa prawna podjęcia kontroli	art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Krakowie
Kontrolerzy	1. Małgorzata Korusiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/147/2019 z 4 września 2019 r.; 2. Paweł Lipowski, specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/148/2019 z 4 września 2019 r. (akta kontroli str. 1-2, 3-4)

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

II. Ocena ogólna kontrolowanej działalności[2]

OCENA OGÓLNA

W okresie objętym kontrolą Urząd został prawidłowo przygotowany do wdrożenia rozporządzenia RODO[3]. Ochrona danych osobowych w MUW była prowadzona zgodnie z wytycznymi określonymi w rozporządzeniu RODO.

W MUW opracowano dokumentację dotyczącą ochrony danych osobowych zgodną z wymogami RODO, w tym przeprowadzono analizę ryzyka w przetwarzaniu danych osobowych, prowadzono i aktualizowano rejestry: czynności przetwarzania danych oraz kategorii czynności przetwarzania danych i naruszeń bezpieczeństwa danych.

Wojewoda wyznaczył Inspektora Ochrony Danych (*IOD*) o odpowiednich kwalifikacjach i zagwarantował mu niezależność w wykonywaniu funkcji. MUW terminowo przesłał do Prezesa Urzędu Ochrony Danych Osobowych (UODO) informację o wyznaczeniu IOD. IOD wykonywał swoje zadania określone w przepisach o ochronie danych osobowych, w tym prowadził szkolenia dla pracowników Urzędu.

Osoby przetwarzające dane w MUW posiadały stosowne upoważnienia do ich przetwarzania. Dostęp do systemów informatycznych zawierających dane osobowe odbierano pracownikom, którzy przestawali pracować w MUW.

Powierzając podmiotom zewnętrznym przetwarzanie danych osobowych zawierano odpowiednie umowy powierzenia, a IOD kontrolował podmioty zewnętrzne przetwarzające te dane.

W Urzędzie wdrożono i przestrzegano zabezpieczeń wynikających z obowiązujących procedur bezpieczeństwa. Poinformowano pracowników i gości o stosowaniu monitoringu wizyjnego.

W przypadkach stwierdzenia naruszenia ochrony danych osobowych, zgodnie z przyjętymi procedurami, informowano osoby, których to dotyczyło, oraz Prezesa UODO. Rozpatrywano prośby o usunięcie danych, zgodnie z oczekiwaniem wnioskujących. O przetwarzaniu danych osobowych i o przyjętych rozwiązaniach dotyczących ich ochrony informowano również pracowników i kandydatów do pracy. W MUW uregulowano proces niszczenia dokumentów zawierających dane osobowe.

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

OBSZAR

1. Organizacja ochrony danych osobowych w MUW

Opis stanu faktycznego

Zarządzeniem z dnia 7 czerwca 2019 r.[5] Wojewoda zatwierdził Politykę ochrony danych osobowych w MUW (*Polityka ODO*) i zobowiązał m.in. Dyrektora Generalnego do zapewnienia zatwierdzenia „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych" (*Instrukcja ZSI*) (lub zatwierdzenia procedur określających sposób zarządzania systemami

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej. W niniejszym wystąpieniu zastosowano ocenę opisową.

[3] 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 i Dz. Urz. UE L 127 z 23 maja 2018 r., str. 2).

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

[5] Zarządzenie Wojewody Małopolskiego z dnia 7 czerwca 2019 r. w sprawie Polityki ochrony danych osobowych w Małopolskim Urzędzie Wojewódzkim w Krakowie. Zarządzenie uchylało „Politykę Bezpieczeństwa w Małopolskim Urzędzie Wojewódzkim w Krakowie" zatwierdzoną w dniu 5 listopada 2015 r.

informatycznymi, przy pomocy których przetwarza się w MUW informacje, w tym również dane osobowe, a której obowiązek opracowania spoczywa na Dyrektorze Wydziału Administracji i Logistyki).

Polityka ODO została wprowadzona w celu zapewnienia zgodności przetwarzania danych osobowych w szczególności z wymogami RODO i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[6]. Uzupełnieniem jej zapisów były przede wszystkim: Instrukcja ZSI, Polityka bezpieczeństwa monitoringu wizyjnego, Polityka Bezpieczeństwa Informacji (*PBI*), której celem było wdrożenie w MUW Systemu Zarządzania Bezpieczeństwem Informacji (*SZBI*).

Wojewoda będący Administratorem danych oraz działający w jego imieniu Dyrektor Generalny MUW mieli realizować obowiązki związane z zabezpieczeniem informacji podlegających ochronie za pośrednictwem m.in.: dyrektorów wydziałów MUW, IOD, Wydziałowych Koordynatorów Bezpieczeństwa Informacji (*WKBI*) oraz osób wyznaczonych spośród pracowników na: Administratora Systemu Informatycznego, Administratora Bezpieczeństwa Systemu Informatycznego, Lokalnych Administratorów Systemów Informatycznych, Administratora Kopii Zapasowych, Administratora Sieci. Na dzień 6 grudnia 2019 r. nie wyznaczono Pełnomocnika do Spraw Bezpieczeństwa i Cyberprzestrzeni. Dyrektor Generalny wyjaśnił, że funkcje te powierzono pracownikom wydziału IT.

W Polityce ODO opisano m.in.: zasady dotyczące przetwarzania danych osobowych; zapewnienia zgodności ich przetwarzania z przepisami prawa (m.in.: prawo do sprostowania danych, prawo do usunięcia danych); rejestrację czynności przetwarzania; zarządzanie ryzykiem przy przetwarzaniu danych osobowych; obowiązek ochrony danych w fazie projektowania oraz domyślnej ochrony danych; organizacyjne środki przetwarzania danych osobowych (w tym szkolenia, upoważnienia do przetwarzania danych osobowych); fizyczne i techniczne środki przetwarzania danych osobowych; audyty prowadzone przez IOD; ocenę skutków przetwarzania dla ochrony danych osobowych; sankcje za naruszenie zasad ochrony danych osobowych; procedurę załatwiania skarg (skargi złożone do Prezesa UODO); procedurę postępowania w przypadku zastosowania przeciwko Wojewodzie lub podmiotowi przetwarzającemu środka ochrony prawnej przed sądem; zasady przeglądów Polityki ODO.

Załącznikami do Polityki ODO były m.in.: Ewidencja osób przeszkolonych w zakresie ochrony danych osobowych; Rejestr czynności przetwarzania danych; Rejestr kategorii czynności przetwarzania danych; klauzule informacyjne (m.in. dla pracowników, odnoszące się do art. 13 i art. 14 RODO i monitoringu); Zasady bezpieczeństwa użytkowania systemu informatycznego; wzór umowy powierzenia przetwarzania danych; procedurę postępowania w przypadku wystąpienia naruszenia ochrony danych.

W Polityce ODO wskazano, że była ona dokumentem niepodlegającym udostępnieniu w trybie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej[7].

Na dzień 28 listopada 2019 r. prace nad nowelizacją Instrukcji ZSI (z 2015 r.) nie zostały zakończone. Dyrektor Generalny wyjaśnił, że planowane zakończenie tych prac to I kwartał 2020 r.

Celem Instrukcji ZSI było określenie zasad właściwego zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych.

---

[6] Dz. U. z 2019 r. poz. 1781; dalej: *ustawa o ochronie danych osobowych.*

[7] Dz. U. z 2019 r. poz. 1429.

W Instrukcji ZSI wskazano m.in.: procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie teleinformatycznym oraz wskazanie osób odpowiedzialnych za te czynności; sposób odnotowywania informacji o udostępnieniu danych osobowych odbiorcom oraz o operacjach wykonywanych na danych osobowych w systemie informatycznym, a także procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

(akta kontroli str. 35-36, 37-41)

1.1. Przygotowanie dokumentacji wymaganej przepisami RODO

Opis stanu faktycznego

Analiza ryzyka związanego z przetwarzaniem danych osobowych odbywała się w MUW na podstawie dokumentu „Proces zarządzania ryzykiem w zakresie ochrony danych osobowych", będącego załącznikiem nr 17 do Polityki ODO.

Szacowanie ryzyka dokonywano w MUW w oparciu o:

- kartę oceny ryzyka naruszenia praw i obowiązków osób fizycznych oraz bezpieczeństwa przetwarzania danych osobowych (w poszczególnych wydziałach);
- „Zasady wykonywania oceny ryzyka związanego z przetwarzaniem danych osobowych".

Karta oceny ryzyka przewidywała ocenę (maksymalnego) poziomu ryzyka pod względem: poufności, integralności i dostępności danych osobowych. W dokonywanej ocenie ryzyka przewidywano:

- 27 zagrożeń dla danych osobowych przetwarzanych w sposób tradycyjny i z wykorzystaniem informatycznych nośników danych;
- 42 zagrożenia dla danych osobowych przetwarzanych w systemach informatycznych.

Zasady oceny ryzyka związanego z przetwarzaniem danych osobowych przewidywały m.in. 46 przykładowych zagrożeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych oraz ocenę ich wpływu na: poufność, integralność i dostępność.

Obliczana wartość ryzyka służyła ocenie i hierarchizacji ryzyka. Dla oceny istotności ryzyka stosowano czterostopniową skalę obejmującą cztery jego poziomy. Poszczególnym poziomom przyporządkowano opis sposobów postępowania z ryzykiem.

Wydziałowe oraz zbiorczy rejestr oceny ryzyka związanego z przetwarzaniem danych osobowych obejmowały: wskazanie czynności przetwarzania, kolejny numer karty oceny ryzyka, wartości ryzyka dla danych osobowych przetwarzanych: w sposób tradycyjny, z wykorzystaniem informatycznych nośników danych oraz w systemie informatycznym wraz z określeniem wartości ryzyka z punktu widzenia – odpowiednio: poufności, integralności i dostępności oraz wartości ryzyka dla czynności przetwarzania.

(akta kontroli str. 24, 42-45, 46-81)

Proces zarządzania ryzykiem w MUW w zakresie ochrony danych osobowych został podzielony na fazy:

- ustanowienie kontekstu;
- szacowanie ryzyka;
- postępowanie z ryzykiem w celu jego zredukowania;
- informowanie o ryzyku;
- monitorowanie i przegląd ryzyka oraz procesu zarządzania ryzykiem.

(akta kontroli str. 24, 25, 42-45)

Przed opracowaniem analizy ryzyka, w kwietniu 2018 r., IOD zwrócił się do kierujących wydziałami MUW o dokonanie analizy ryzyka dla bezpieczeństwa przetwarzania danych osobowych odnośnie do wszystkich realizowanych czynności.

W maju 2018 r. IOD poinformował Administratora o przeprowadzeniu w MUW oceny poziomu ryzyka dla bezpieczeństwa przetwarzania danych osobowych. Administrator przyjął ten dokument.

Informacja o wynikach analizy ryzyka w MUW sporządzona przez IOD (9 maja 2019 r.) zawierała m.in.:

- zidentyfikowane zabezpieczenia organizacyjne, techniczne oraz informatyczne wprowadzone i funkcjonujące w MUW;
- zidentyfikowane zagrożenia i propozycje rozwiązań z punktu widzenia skutków urzeczywistnienia ryzyka naruszenia praw lub wolności osób fizycznych oraz prawdopodobieństwa ich wystąpienia. Zgodnie z raportem z 158 czynności przetwarzania danych osobowych (dla danych przetwarzanych w formie tradycyjnej i na informatycznych nośnikach danych oraz danych przetwarzanych w systemach informatycznych) w 151 przypadkach wartość ryzyka mieściła się na poziomie ryzyka akceptowalnego, w sześciu przypadkach ryzyko było na poziomie wysokim, a dla jednej czynności przetwarzania jego wartość była na poziomie bardzo wysokim;
- zalecenia i wnioski dla kierujących dwoma wydziałami MUW (Spraw Obywatelskich i Cudzoziemców oraz Bezpieczeństwa i Zarządzania Kryzysowego).

Zbiorczy rejestr oceny ryzyka związanego z przetwarzaniem danych osobowych w MUW został podpisany przez Dyrektora Wydziału Prawnego i Nadzoru w czerwcu 2019 r. (w zastępstwie Dyrektora Generalnego). Zawierał on 158 czynności przetwarzania.

Wydziałowe rejestry ryzyka tworzone były od kwietnia do maja 2018 r. w 14 wydziałach MUW, w Wojewódzkiej Inspekcji Geodezyjnej i Kartograficznej oraz Państwowej Straży Rybackiej. Zawierały od dwóch (Wydział Prawny i Nadzoru) do 65 (Wydział Polityki Społecznej) kategorii czynności przetwarzania.

(akta kontroli str. 24, 25, 42-45)

W załączniku Nr 17 do Polityki ODO („Proces zarządzania ryzykiem w zakresie ochrony danych osobowych") wyróżniono cztery sposoby postępowania z ryzykiem. W przypadkach, gdy w wyniku procesu oceny wartości ryzyka dyrektor wydziału MUW stwierdzi, że występują ryzyka, których wartość oceniono na poziomie wysokim lub bardzo wysokim (w „Informacji o wynikach analizy ryzyka"), powinien opracować, a następnie wdrożyć „Plan postępowania z ryzykiem". Informację w tym zakresie powinien przekazać IOD oraz Dyrektorowi Generalnemu. Na dzień 6 grudnia 2019 r. takich planów postępowania z ryzykiem, ze względu na niestwierdzenie ryzyka na poziomie wysokim lub bardzo wysokim, nie opracowano.

(akta kontroli str. 24, 42-45, 46-81)

W okresie objętym kontrolą w MUW prowadzono trzy postępowania wyjaśniające w związku ze skargami dotyczącymi ochrony danych osobowych. Dwie z nich wpłynęły od Generalnego Inspektora Ochrony Danych Osobowych w latach 2015-2017 i dotyczyły przetwarzania danych osobowych w celu realizacji szczepień dzieci osób skarżących. W żadnej ze spraw w MUW nie stwierdzono naruszeń przepisów odnoszących się do ochrony danych osobowych.

(akta kontroli str. 8, 9, 23, 26-27)

W MUW opracowano rejestr czynności przetwarzania danych osobowych, rejestr kategorii przetwarzania danych osobowych oraz rejestr naruszeń danych

osobowych. Opis w tym zakresie znajduje się w Obszarze 2 pkt 1 niniejszego wystąpienia.

(akta kontroli str. 24, 25, 42-45, 164-165)

W rejestrze naruszeń danych osobowych na 20 grudnia 2019 r. ujęto pięć incydentów. Opis w tym zakresie znajduje się w Obszarze 3 wystąpienia.

(akta kontroli str. 24, 25, 42-45)

W dniu 13 czerwca 2019 r. IOD przesłał do dyrektorów komórek organizacyjnych MUW pismo dotyczące zatwierdzenia Polityki ODO wraz z prośbą o przeanalizowanie tego dokumentu, zapoznanie podległych pracowników z zawartymi w nim procedurami, zapewnienie przestrzegania tych procedur oraz realizację szczegółowych zadań, które ww. Polityka nakładała na kierujących wydziałami (w terminie do 15 lipca 2019 r.). Treść ww. dokumentu umieszczono na stronie intranetowej MUW.

Analogicznie postąpiono po wdrożeniu procedur dotyczących przetwarzania danych osobowych obowiązujących przed 13 czerwca 2019 r., zatwierdzonych przez Wojewodę 5 listopada 2015 r. („Polityka bezpieczeństwa w MUW" oraz „Instrukcja ZSI służącym do przetwarzania danych osobowych"). Informacja o powyższym została przekazana pismem z 16 listopada 2015 r.

Dokumentacja obowiązująca od czerwca 2019 r. została wprowadzona do stosowania w formie zarządzenia Wojewody w trybie wskazanym w § 67, 69, 78 Regulaminu organizacyjnego MUW[8].

Opracował ją IOD, konsultując jej treść ze wszystkimi dyrektorami wydziałów MUW. Ponadto współpracował w tym zakresie z wybranymi pracownikami Wydziału Administracji i Logistyki oraz Wydziału Prawnego i Nadzoru. Dokumentację zatwierdzał Wojewoda.

W skład udostępnianej wewnętrznie dokumentacji wchodziły: zarządzenie Wojewody z dnia 7 czerwca 2019 r., Polityka ODO wraz z załącznikami (od nr 1 do nr 29). Na podstawie ww. zarządzenia uchylono „Politykę bezpieczeństwa w MUW".

(akta kontroli str. 25, 104-105, 106-113)

1.2. Wyznaczenie i działanie Inspektora Ochrony Danych

Opis stanu faktycznego

Działając na podstawie art. 158 ust. 2 ustawy o ochronie danych osobowych, Wojewoda poinformował elektronicznie (ePUAP) Prezesa UODO o wyznaczeniu IOD w dniu 2 sierpnia 2018 r. Wyznaczenie IOD odbyło się na podstawie wniosku Pełnomocnika Wojewody ds. Ochrony Informacji Niejawnych z dnia 31 lipca 2018 r.

(akta kontroli str. 8, 9, 23)

IOD wyznaczono spośród pracowników MUW. Pełnił on przed powołaniem na to stanowisko funkcję Administratora Bezpieczeństwa Informacji (ABI). Na podstawie § 20 ust. 3 regulaminu organizacyjnego, funkcję IOD pełnił Pełnomocnik Wojewody ds. Ochrony Informacji Niejawnych (w pełnym wymiarze czasu pracy; IOD nie miał formalnie wyznaczonego podziału czasu pracy pomiędzy tymi funkcjami). W okresie objętym kontrolą nie było zmian na stanowisku IOD.

(akta kontroli str. 8, 9, 23)

W regulaminie organizacyjnym ustalono bezpośrednią podległość IOD Wojewodzie oraz określono m.in. następujące zadania IOD:

- informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej i Rzeczypospolitej Polskiej o ochronie danych i doradzanie im w tej sprawie;

[8] Ustalonego zarządzeniem Wojewody Małopolskiego z dnia 18 kwietnia 2016 r. (ze zm.); dalej: *regulamin organizacyjny*.

- monitorowanie przestrzegania RODO, innych przepisów UE i Rzeczypospolitej Polskiej o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- prowadzenie, na podstawie danych przekazywanych przez wydziały, rejestru czynności przetwarzania danych osobowych, za które odpowiadał Administrator;
- koordynowanie spraw związanych z wykonywaniem analizy ryzyka związanego z operacjami przetwarzania danych osobowych, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

W trakcie kontroli NIK (23 września 2019 r.) w MUW powołano Zastępcę IOD (na podstawie wniosku IOD z 29 lipca 2019 r.)[9]. Zawiadomienie w tym zakresie złożono do Prezesa UODO w dniu 23 września 2019 r. Wydziały MUW powiadomiono o tym fakcie 25 września 2019 r.

(akta kontroli str. 8, 9, 23, 35-36, 37-41)

Wojewoda jako Administrator wyjaśnił, że każda przedstawiana przez IOD procedura mająca na celu wdrożenie w MUW zasad, o których mowa w RODO, była przed podpisaniem analizowana, a działalność IOD w ramach Urzędu (kierowane do komórek organizacyjnych pisma) była aprobowana przez Wojewodę. Dodał, że działalność IOD podlegała nadzorowi Dyrektora Generalnego. (wskazał przy tym na korespondencję z IOD z lutego 2018 r. związaną z przygotowaniem MUW do wdrożenia RODO). Wybrane aspekty działalności IOD podlegały audytowi wewnętrznemu, m.in. w 2018 r. przeprowadzono audyt systemu Elektronicznego Zarządzania Dokumentacją (*EZD*) związany z działalnością IOD, który wskazywał m.in. na konieczność aktualizacji dokumentów związanych z RODO, a działalność IOD została ujęta w planie audytu na 2019 r. („ochrona danych osobowych – koordynacja działalności oraz obsługa administracyjno-techniczna”[10]).

(akta kontroli str. 182-183, 184-191)

Na stronie internetowej MUW[11] podano (według stanu na 16 września 2019 r.) kontakt do IOD (adresy: skrzynki ePUAP i email oraz dane adresowe). Ponadto dane IOD znajdowały się w każdej klauzuli informacyjnej stosowanej w MUW. Na ww. stronie internetowej również znajdowały się: klauzula informacyjna, informacja o utrwalaniu i rozpowszechnianiu wizerunku osób uczestniczących w spotkaniach i uroczystościach organizowanych przez MUW oraz szczegółowe klauzule informacyjne. Informacje te dostępne były także na stronie BIP MUW (dostęp: *pozostałe informacje – ochrona danych osobowych*).

(akta kontroli str. 8, 9, 23)

IOD posiadał wykształcenie wyższe […][12]. W latach 2010-2019 (do sierpnia) uczestniczył w 11 szkoleniach, kursach i konferencjach z zakresu ochrony danych osobowych. Zastępca IOD w latach 2017-2018 m.in. ukończył szkolenie z zakresu RODO oraz posiadał uprawnienia audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji według normy ISO 27001:2013, ukończył również studia podyplomowe w zakresie systemów zarządzania bezpieczeństwem informacji.

(akta kontroli str. 8, 12-25, 160-163)

[9] Funkcję tę pełnił pracownik zatrudniony na samodzielnym stanowisku ds. bezpieczeństwa teleinformatycznego i kontroli w Zespole do Spraw Ochrony Informacji Niejawnych MUW.

[10] Z uwagi na kontrolę NIK audyt przeniesiono na 2020 r.

[11] www.malopolska.uw.gov.pl (zakładka: *Ochrona danych osobowych*).

[12] Na podstawie pisma Wojewody Małopolskiego z 14 lutego 2020 r. znak ZI-II.1610.2.2019 NIK wyłączyła jawność informacji zgodnie wnioskiem zawartym w ww. piśmie w zakresie szczegółowych danych dot. wykształcenia IOD.

Wojewoda jako Administrator wyjaśnił, że IOD miał zapewnioną niezależność w wykonywaniu obowiązków w regulaminie organizacyjnym MUW, podlegając bezpośrednio Wojewodzie. Sprawował również funkcję Pełnomocnika ds. Ochrony Informacji Niejawnych.

(akta kontroli str. 25, 104-105, 106-113)

Dyrektor Generalny wyjaśnił, że IOD informował o obowiązkach związanych z ochroną danych osobowych:

- Administratora – poprzez przekazywanie informacji na temat przygotowywanych procedur oraz wytycznych dotyczących ochrony danych osobowych jak również informacji o prawidłowym przetwarzaniu danych osobowych. IOD przygotował m.in.:
  - Politykę ODO;
  - Zasady bezpieczeństwa użytkowania systemu informatycznego;
  - Politykę ochrony danych osobowych w systemie monitoringu wizyjnego;
  - procedury zarządzania ryzykiem w zakresie ochrony danych osobowych, w tym w przypadku naruszenia ochrony danych osobowych (w tym rejestr czynności przetwarzania);
  - wzory: klauzul informacyjnych: (szczegółowej) dla klientów MUW (ze stycznia 2019 r.); w związku z przetwarzaniem danych osobowych w systemie monitoringu wizyjnego; w celu związanym z postępowaniem o udzielenie zamówienia publicznego; dla pracowników oraz osób, które wykonują zadania dla MUW na podstawie innych tytułów prawnych w przypadku monitoringu wizyjnego; umieszczenia danych w BIP; akt osobowych; Zakładowego Funduszu Świadczeń Socjalnych i Pracowniczej Kasy Zapomogowo-Pożyczkowej;
  - oświadczeń o zachowaniu w tajemnicy (w tym w związku z przepisami związanymi z nadawaniem orderów i odznaczeń), upoważnień do przetwarzania danych osobowych (w tym dla zbiorów danych osobowych przetwarzanych w MUW, wprowadzonych od 25 maja 2018 r., szkód w gospodarstwach rolnych), zgód na przetwarzanie danych osobowych, dokumentacji związanej z rejestrowaniem czynności przetwarzania danych osobowych;
- podmioty przetwarzające – poprzez umieszczenie zapisów o obowiązkach takich podmiotów w umowach powierzenia przetwarzania danych (opracowanie wzoru takiej umowy w maju 2018 r. z aktualizacją z sierpnia 2019 r.);
- pracowników MUW – poprzez szkolenia z zakresu ochrony danych osobowych oraz kierowanie wytycznych (m.in. w zakresie udostępniania danych dla celów kontroli NIK, autoryzacji osób podczas przekazywania informacji przez telefon, udzielania informacji klientom MUW o zgromadzonych danych osobowych), wyjaśnień (m.in. w sprawach treści decyzji administracyjnych, stosowania RODO w procedurach zamówień publicznych wraz z klauzulami do SIWZ), konsultowanie dokumentów, których celem było wdrożenie procedur umożliwiających zapewnienie rozliczalności w zakresie ochrony danych osobowych - m.in. analizy przepisów prawnych, aktualizację danych dotyczących WKBI (czerwiec 2018 r.).

(akta kontroli str. 25, 35-36, 37-41)

Dyrektor Generalny wskazał, że IOD monitorował przestrzeganie przepisów o ochronie danych osobowych poprzez bieżące prowadzenie dokumentacji niezbędnej do zapewnienia rozliczalności w tym zakresie (m.in. aktualizacji zakresów czynności w zakresie przetwarzania danych osobowych, nieumieszczania imion i nazwisk na kartach parkingowych MUW), zarządzanie naruszeniami ochrony danych osobowych, opiniowanie rozwiązań w zakresie ochrony danych osobowych

(m.in. stosowanie szyfrowania i pseudoanonimizacji w systemach informatycznych, regulaminy serwisów www) oraz kreowanie takich rozwiązań poprzez m.in. uzyskiwanie opinii prawnych (m.in. w zakresie stosowania RODO) oraz prowadzenie wewnętrznych audytów w zakresie ochrony danych osobowych (w lipcu 2019 r. zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych) oraz inicjowanie działań związanych z podpisywaniem umów powierzenia przetwarzania danych, a także ich opiniowanie.

(akta kontroli str. 25, 35-36, 37-41)

Do IOD nie kierowano żądań udzielenia zaleceń co do oceny skutków dla ochrony danych.

(akta kontroli str. 35-36, 37-41)

IOD współpracował z organem nadzorczym poprzez konsultacje telefoniczne, pisemne oraz w drodze wideokonferencji, w tym wysłał do UODO pismo dotyczące interpretacji związanej z powierzeniem przetwarzania danych osobowych przez podmiot oferujący usługi rekreacyjno-sportowe (z grudnia 2018 r.).

(akta kontroli str. 25, 35-36, 37-41)

IOD pełnił funkcję punktu kontaktowego dla organu nadzorczego np. poprzez przesyłanie do UODO podpisanych przez Wojewodę zgłoszeń o naruszeniu ochrony przetwarzanych danych osobowych.

(akta kontroli str. 35-36, 37-41)

Przed wejściem do pomieszczeń konferencyjnych IOD zamieścił klauzule informacyjne związane z ochroną wizerunku osób biorących udział w konferencjach i uroczystościach organizowanych na terenie MUW. Tą drogą zapewniano bezpośrednie przekazanie takiej informacji wszystkim osobom uczestniczącym w spotkaniach, w trakcie których utrwalano ich wizerunek.

(akta kontroli str. 8, 9, 23)

1.3. Inne działania MUW związane z wdrażaniem RODO

Opis stanu faktycznego

Na stronie internetowej MUW w zakładce *Ochrona danych osobowych* znajdowały się klauzule informacyjne dotyczące zasad przetwarzania danych osobowych w MUW: ogólna i szczegółowe oraz informacja dla uczestników spotkań i uroczystości organizowanych przez MUW[13].

W klauzulach wskazano m.in.: Administratora, kontakt do IOD i cele dla jakich dane osobowe były przetwarzane.

We wszystkich pomieszczeniach (korytarze), w których prowadzono obsługę klientów MUW, objętych oględzinami (po rozpoczęciu kontroli 11 września 2019 r.) znajdowały się klauzule informacyjne (klauzula ogólna sporządzona przez MUW oraz klauzule szczególne do danych czynności przekazane przez: Ministerstwo Cyfryzacji, Ministerstwo Spraw Wewnętrznych i Administracji oraz Urząd ds. Cudzoziemców).

(akta kontroli: 5-7, 23)

W lipcu 2019 r. IOD przeprowadził audyt w zakresie monitorowania przestrzegania RODO oraz ochrony danych osobowych, w ramach którego sprawdzono sposób realizacji wymagań nałożonych na dyrektorów wydziałów MUW w zakresie: powołania WKBI, prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz sposobu wydawania upoważnień, dostępu do systemów informatycznych, postępowania z: dokumentacją, wydrukami, hasłami oraz informatycznymi nośnikami danych zawierającymi dane osobowe po zakończeniu godzin pracy przez pracowników Urzędu.

[13] Dostęp w dniu 16 września 2019 r.

W wyniku audytu stwierdzono nieprawidłowości polegające na: umożliwieniu potencjalnego dostępu do dokumentów zawierających dane osobowe klientów MUW przez osoby nieuprawnione, tj. personel sprzątający; nieinformowaniu IOD w każdym przypadku o wydaniu osobie upoważnienia do przetwarzania danych osobowych; wykorzystywaniu niszczarek niegwarantujących zapewnienia poufności po zniszczeniu dokumentów; niewyłączaniu komputerów po zakończeniu pracy oraz korzystaniu z drukarek sieciowych w sposób, który nie zapewniał poufności danych osobowych.

Po przeprowadzeniu audytu IOD zalecił przeanalizowanie jego wyniku przez Dyrektora Generalnego i podjęcie działań naprawczych, w tym: wykonanie inwentaryzacji istniejących środków bezpieczeństwa fizycznego oraz zaplanowanie środków finansowych na wdrożenie programu: wymiany niszczarek na spełniające wymóg wynikający z § 65 ust. 16 Polityki ODO, zakup szaf uniemożliwiających dostęp osób nieuprawnionych do dokumentów zawierających dane osobowe; podjęcie działań dyscyplinujących w celu zapobieżenia naruszaniu poufności danych osobowych; uświadomieniu dyrektorom wydziałów, iż niedopuszczalne jest pozostawianie dokumentów zawierających dane osobowe bez odpowiedniego zabezpieczenia po godzinach pracy; polecenie dyrektorom: informowania IOD o wydanych upoważnieniach do dostępu do danych osobowych; sprawdzenia, czy wszystkie osoby realizujące zadania związane z czynnościami przetwarzania danych osobowych są do tego upoważnione; przeprowadzania rozmów z podległymi pracownikami w celu uświadomienia wagi stosowania środków bezpieczeństwa podczas przetwarzania danych osobowych oraz przypomnienia o konieczności przestrzegania „Zasad bezpieczeństwa użytkowania systemu teleinformatycznego", w tym o konieczności wyłączania komputerów; podjęcie działań zmierzających do ograniczenia przetwarzania dokumentów w formie papierowej, gdyż generuje to koszty związane z zakupem np. szaf i niszczarek; podjęcie działań zapobiegających pozostawianiu włączonych drukarek, w szczególności w sytuacji, gdy zadania drukowania znajdują się jeszcze w pamięci urządzeń; sugerował również powszechne wdrożenie tzw. druku podążającego[14].

(akta kontroli str. 8, 9, 23)

W 2018 r. Wydział Organizacji i Kontroli MUW nie prowadził kontroli zewnętrznych dotyczących ochrony danych osobowych. W 2019 r. Wydział ten przeprowadził dwie kontrole jednostek wojewódzkiej administracji zespolonej, uwzględniające tę tematykę, tj.:

- Wojewódzkiego Urzędu Ochrony Zabytków w Krakowie (doraźna) – czynności kontrolne zostały zakończone 19 lipca 2019 r.,
- Komendy Wojewódzkiej Państwowej Straży Pożarnej w Krakowie – czynności kontrolne zostały zakończone 26 lipca 2019 r.

W trakcie kontroli NIK oba ww. postępowania pokontrolne były w toku (opracowywane były projekty wystąpień pokontrolnych).

Na IV kwartał 2019 r. zaplanowano kontrolę Wojewódzkiego Inspektoratu Ochrony Roślin i Nasiennictwa w Krakowie, której zakres tematyczny miał obejmować m.in. ochronę danych osobowych.

Wydział Organizacji i Kontroli nie prowadził kontroli wewnętrznych w zakresie ochrony danych osobowych. W MUW nie było również zewnętrznych kontroli związanych z RODO (w okresie objętym kontrolą).

(akta kontroli str. 8, 9, 23)

Szkolenia pracowników uczestniczących w operacjach przetwarzania danych osobowych w związku z RODO prowadzone były przez IOD według przygotowanych

[14] Funkcjonalność pozwalająca na odbiór wydruków z drukarki dopiero po autoryzacji pracownika.

przez niego materiałów, których aktualna wersja zamieszczana była w intranecie MUW.

Ww. szkolenia odbywały się od stycznia 2018 r. do 16 października 2019 r. Zrealizowano 30 szkoleń, którymi objęto 1 440 osób (od 25 maja 2018 r.: 19 szkoleń dla 816 osób). Czas szkolenia wynosił ok. 3,5 godz., na każdym szkoleniu obowiązywało odnotowanie uczestnictwa w formie podpisu na liście obecności. IOD przeprowadzał również szkolenia z zakresu RODO dla nowo zatrudnionych pracowników w ramach służby przygotowawczej (od 25 maja 2018 r. odbyły się cztery szkolenia dla 107 osób).

Ponadto 22 maja 2018 r. pisemnie polecono pracownikom MUW udział w e-szkoleniu „Przygotowanie do wdrożenia RODO", organizowanym przez KPRM i dostępnym na platformie e-learningowej KPRM. Ukończenie szkolenia miało nastąpić do 30 czerwca 2018 r.

Zasady uczestnictwa w ww. szkoleniach określone były w:
- „Polityce bezpieczeństwa w MUW" (§ 9 ust. 4, § 22) oraz Instrukcji ZSI z 2015 r. (§ 4);
- Polityce ODO.

Do uczestnictwa w szkoleniach zobowiązane były wszystkie osoby, które otrzymały upoważnienie do przetwarzania danych osobnych. W szkoleniach uczestniczyli: kadra kierownicza wydziałów (i komórek równorzędnych), pracownicy oraz osoby zatrudnione na podstawie umów zlecenia i umów o dzieło oraz stażyści, praktykanci i wolontariusze.

Szkolenia dotyczyły m.in.: przepisów prawnych w zakresie ochrony danych osobowych, praktycznych zasad przetwarzania danych osobowych, obowiązków Administratora, IOD i pracowników, praw osób, których dane są przetwarzane, sytuacji szczególnych związanych z przetwarzaniem danych osobowych, środków ochrony prawnej, odpowiedzialności i sankcji, naruszeń ochrony danych osobowych, szacowania ryzyka dla danych osobowych oraz zasad bezpieczeństwa związanych z użytkowaniem systemów informatycznych.

(akta kontroli str. 25, 104-105, 106-113)

Według stanu na 15 października 2019 r. w MUW zatrudnionych było 1 243 pracowników. Analiza 63 akt osobowych[15] pracowników Wydziału Rewaloryzacji Zabytków Krakowa i Dziedzictwa Narodowego, Kancelarii Urzędu oraz Archiwum Zakładowego zlokalizowanych w Wydziale Organizacji i Kontroli wykazała, że:
- w aktach osobowych 52 pracowników znajdowały się upoważnienia do przetwarzania danych osobowych;
- w aktach osobowych ośmiu pracowników znajdowało się zaświadczenie o ukończeniu kursu e-learningowego związanego z wdrożeniem RODO (czerwiec 2018 r.);
- w aktach osobowych siedmiu pracowników znajdowały się ich oświadczenia o zapoznaniu się z m.in. z: RODO, zasadami bezpieczeństwa użytkowania systemu teleinformatycznego, „Klauzulą informacyjną dla pracowników oraz osób, które wykonują zadania dla MUW na podstawie innych tytułów prawnych".

Dyrektor Generalny wyjaśnił, że z uwagi na potrzeby i możliwości organizacyjne MUW szkolenia dla pracowników związane z RODO były prowadzone w ramach szkoleń wewnętrznych prowadzonych przez IOD; listy obecności, wykazy osób przeszkolonych i zaświadczenia potwierdzające przeszkolenie pracowników są

[15] Dokumenty tj. certyfikaty ze szkolenia dotyczącego ochrony danych osobowych i przetwarzania danych osobowych; upoważnienia do przetwarzania danych; Informacja pracodawcy o przetwarzaniu danych osobowych pracownika – jeżeli były w aktach, znajdowały się w części B akt osobowych i były zaewidencjonowane w wykazie dokumentów w tych aktach.

przechowywane w wersji tradycyjnej, jak i elektronicznej w zasobach akt właściwych w ramach spraw realizowanych przez IOD. Dodał, że zgodnie z przyjętym w Urzędzie rozwiązaniem, do akt osobowych dołączane były i są zaświadczenia lub poświadczenia ukończenia szkoleń dotyczących ochrony i przetwarzania danych osobowych, w sytuacji uczestnictwa pracownika w szkoleniu zewnętrznym, w tym również ukończenia szkolenia metodą e-learningową realizowanego na platformie KPRM.

(akta kontroli str. 114, 115, 121-139)

Dyrektor Generalny wyjaśnił, że *trudno jest określić faktycznie poniesione koszty* (związane z wdrożeniem RODO w MUW) *lub ich wartość szacunkową, gdyż nie były one odrębnie ewidencjonowane.* IOD brał udział w spotkaniach i szkoleniach zewnętrznych dla inspektorów ochrony danych, w tym w szkoleniu w sierpniu 2019 r., którego koszt wyniósł 1,8 tys. zł. Dodał, że zadania dotyczące ochrony danych osobowych w MUW *pełnione są w ramach obowiązków pracowników i nie jest możliwe wyodrębnienie kosztów wynagrodzeń związanych z zadaniami (…) z obszaru ochrony danych osobowych*.

(akta kontroli str. 35-36, 37-41)

Dyrektor Generalny wyjaśnił, że w okresie objętym kontrolą nie poniesiono wydatków, które były związane z niewłaściwym stosowaniem RODO. Na MUW nie nałożono również administracyjnych kar pieniężnych, innych sankcji lub obowiązków naprawczych, związanych z niewłaściwym stosowaniem RODO.

(akta kontroli str. 35-36, 37-41)

Stwierdzone nieprawidłowości

W działalności MUW w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK ocenia pozytywnie działania MUW w obszarze organizacji ochrony danych osobowych w Urzędzie.

OBSZAR

2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych

Opis stanu faktycznego

2.1. Prowadzenie rejestrów wymaganych przepisami RODO

Rejestr czynności przetwarzania danych osobowych w MUW zawierał wszystkie informacje wymagane art. 30 ust. 1 RODO, w tym opis technicznych i organizacyjnych środków bezpieczeństwa.

Przetwarzanie danych miało odbywać się wyłącznie w przypadkach, gdy spełniony był jeden z warunków określonych w art. 6 ust. 1 RODO.

Pierwszy rejestr czynności przetwarzania danych został utworzony w Urzędzie 16 maja 2018 r. Prowadzony był na serwerze (dysku systemowym) systemu informatycznego MUW w formie elektronicznej. W dniu 24 maja 2018 r. dokument ten został umieszczony w systemie EZD. W aktualizowanej wersji z 5 czerwca 2018 r. wyszczególniono 150 czynności przetwarzania w 22 komórkach organizacyjnych MUW.

W wyniku kolejnych aktualizacji (21 listopada i 18 grudnia 2018 r., 4 czerwca i 16 sierpnia 2019 r.) liczba czynności przetwarzania została zwiększona do 160. Dane Administratora były wskazane w aktualizacji rejestru z 18 grudnia 2018 r.

Aktualizacji rejestru czynności przetwarzania danych dokonywano w związku z:

- dopisywaniem nowo zgłoszonych przez komórki organizacyjne czynności przetwarzania danych, co wynikało z podejmowanych przez dyrektorów tych komórek działań dotyczących przeglądu zgłoszonych czynności przetwarzania,

analizy realizowanych zadań przez wydziały i podejmowania decyzji o wyodrębnieniu niektórych czynności i ich opisaniu;

- aktualizacjami danych zawartych w tym rejestrze, zgłaszanymi przez dyrektorów komórek organizacyjnych związanymi z: zmianami podstaw prawnych przetwarzania danych, zmianami zakresów przetwarzanych danych, aktualizacją (dopisaniem) podmiotów, którym powierzono przetwarzanie danych, uściśleniem okresu przetwarzanych (kategorii) danych oraz podmiotów, którym dane mogą być przekazywane (udostępniane);
- umieszczeniem w tym rejestrze dodatkowej kolumny z nazwą zbioru danych osobowych, do których odnosi się dana czynność przetwarzania, w celu ułatwienia identyfikacji czynności w połączeniu ze zbiorem danych;
- zmianą „właściciela" czynności przetwarzania danych (przeniesienie czynności między wydziałami);
- zaprzestaniem przetwarzania danych, w ramach określonego celu przetwarzania.

(akta kontroli str. 182-183, 184-191)

Rejestr kategorii czynności przetwarzania zawierał wszystkie informacje wymagane art. 30 ust. 2 RODO, tj. określał kategorię przetwarzań, wskazywał dokumentację odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 RODO oraz wskazywał opis technicznych i organizacyjnych środków bezpieczeństwa.

Pierwszy rejestr kategorii czynności przetwarzania danych został utworzony w MUW 16 maja 2018 r. Prowadzony był na serwerze (dysku systemowym) systemu informatycznego MUW w formie elektronicznej. W dniu 13 sierpnia 2018 r. dokument ten został umieszczony w systemie EZD. W aktualizacji z 13 sierpnia 2018 r. wyszczególniono 13 kategorii przetwarzań. Po aktualizacji (z 21 sierpnia 2019 r.) liczba kategorii przetwarzań zwiększyła się do 28.

Aktualizacji rejestru kategorii czynności przetwarzania danych dokonywano w związku z powierzaniem przetwarzania danych osobowych Wojewodzie przez podmioty zewnętrzne (organy administracji publicznej) i podpisywaniem nowych umów powierzenia przetwarzania danych.

Ww. rejestry nie zawierały informacji o nadmiernych kategoriach danych.

(akta kontroli str. 182-183, 184-191)

2.2. Upoważnienia do przetwarzania danych

Opis stanu faktycznego

Pracownicy MUW otrzymywali upoważnienia do przetwarzania danych osobowych, wydawane przez Wojewodę, Dyrektora Generalnego oraz dyrektorów wydziałów. Dyrektor Generalny oraz dyrektorzy wydziałów zostali upoważnieni przez Wojewodę do przetwarzania danych osobowych oraz do udzielania upoważnień pracownikom wydziałów do przetwarzania danych w podległych im wydziałach. Na podstawie badania dokumentacji odnoszącej się do pracowników dwóch komórek organizacyjnych Urzędu stwierdzono, że pracownicy zajmujący się przetwarzaniem danych osobowych posiadali stosowne upoważnienia, a ich zakres odpowiadał zakresowi ich czynności.

W MUW w imieniu Wojewody „Ewidencję osób upoważnionych do przetwarzania danych osobowych" prowadził IOD. Do ww. ewidencji wpisywane były te osoby, których upoważnienia zostały przekazane IOD przez dyrektorów wydziałów. W ewidencji tej według stanu na 29 października 2019 r. było ujętych 961 osób.

Ww. ewidencja była prowadzona alfabetycznie w formie elektronicznej (wszystkie wpisy były w jednym dokumencie z podziałem na okres do 24 maja 2018 r. włącznie oraz od 25 maja 2018 r.).

Dyrektor Generalny wyjaśnił, że zgodnie z przyjętą w Urzędzie praktyką, bieżące upoważnienia do przetwarzania danych osobowych dla pracowników przygotowywane są w wersji elektronicznej i nie dołączano ich dodatkowo do akt osobowych pracownika.

(akta kontroli str. 25, 104-105, 106-113, 114, 115, 121-139)

Według stanu na 15 października 2019 r. MUW był stroną 166 umów zleceń i umów o dzieło zawartych z osobami fizycznymi. Umowy te dotyczyły m.in. pełnienia funkcji IOD w Wojewódzkiej Komisji ds. Zdarzeń Medycznych, wydawania opinii medycznych i obsługi prawnej postępowań odwoławczych w tym zakresie, uczestnictwa w Wojewódzkim Zespole ds. Orzekania o Niepełnosprawności, pełnienia funkcji konsultantów wojewódzkich w poszczególnych dziedzinach medycyny.

W sześciu z analizowanych 11 umów zleceniobiorca oświadczył, że zapoznał się z przepisami RODO i zobowiązał się do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami, w granicach przyznanego upoważnienia. Zleceniobiorcy ci zostali upoważnieni do przetwarzania danych w stosownym zakresie. Podpisane przez zleceniobiorcę oświadczenie o zobowiązaniu do zachowania w tajemnicy wszelkich podlegających ochronie informacji, uzyskanych ustnie, pisemnie lub w jakiejkolwiek innej formie w czasie pracy lub realizacji umowy w MUW stanowiło załącznik do umowy.

W pięciu umowach zlecenia nie było zapisu wskazującego na upoważnienie zleceniobiorcy do wykonywania czynności przetwarzania danych osobowych:

- trzy analizowane umowy były umowami zlecenia na sprawowanie funkcji konsultanta wojewódzkiego w ochronie zdrowia. Zadania Wojewody w tym zakresie koncentrowały się na kwestiach organizacyjnych i obejmowały: powołanie do funkcji konsultanta wojewódzkiego w danej specjalności, zawarcie z konsultantem umowy na dany rok oraz finansowanie jego działalności. Dokumentacja wynikająca z realizacji zadań przez konsultanta jest jego własnością i jest przez niego przechowywana. Konsultanci nie mają dostępu do elektronicznego systemu zarządzania dokumentacją funkcjonującego w MUW. Wojewoda wyjaśnił, że *nie ma podstaw prawnych do wydania upoważnień dla konsultantów wojewódzkich, którzy wykonują zadania samodzielnie i niezależnie od Wojewody Małopolskiego*;
- lekarz pełniący funkcję Naczelnego Lekarza Uzdrowiska w województwie małopolskim posiadał upoważnienie do przetwarzania danych osobowych w ramach powierzonych obowiązków służbowych, w którym zapisano, że przetwarzanie tych danych musi być zgodne m.in. z RODO. Ponadto Naczelny Lekarz Uzdrowiska poświadczył zapoznanie się z Zasadami bezpieczeństwa użytkowania systemu teleinformatycznego MUW. Naczelny Lekarz Uzdrowiska odbył szkolenie z RODO zorganizowane przez IOD;
- osoba zajmująca stanowisko IOD w Wojewódzkiej Komisji do Spraw Medycznych posiadała upoważnienie do przetwarzania danych osobowych wydane 25 maja 2018 r. przez Przewodniczącego Komisji do Spraw Zdarzeń Medycznych jako odrębnego administratora danych.

(akta kontroli str. 114, 115, 140-151)

W okresie od 25 maja 2018 r. do 15 października 2019 r. MUW rozwiązał umowę o pracę z 202 osobami, a 27 osób zmieniło stanowisko pracy w ramach MUW.

Kontrolą objęto losowo wybraną grupę 10 osób spośród 202 pracowników MUW (tj. 5%), z którymi rozwiązano stosunek pracy po 25 maja 2018 r. oraz sześciu spośród 27 pracowników MUW (22%), którzy zmienili stanowisko w ramach MUW.

W wyniku oględzin wykorzystywanego w MUW systemu zarządzania użytkownikami i prawami dostępu w ramach usługi katalogowej ustalono, że:

- w ww. systemie konta byłych pracowników zostały zablokowane, co powodowało brak możliwości logowania do systemu informatycznego MUW;
- ww. system rejestrował datę ostatniej modyfikacji konta użytkownika, która była dokonywana przez administratora systemu;
- zarejestrowana w ww. systemie informatycznym data ostatniej modyfikacji konta danego użytkownika była tożsama lub późniejsza niż data rozwiązania stosunku pracy z daną osobą (ostatnia modyfikacja oznaczała blokowanie konta);
- dostęp do systemów informatycznych obecnych pracowników był adekwatny do zakresu aktualnie wykonywanych obowiązków zawodowych.

Blokowanie kont w domenie Urzędu dokonywane było przez pracowników Wydziału IT w momencie uzyskania informacji o rozwiązaniu stosunku pracy. IOD Urzędu wskazał, że blokowanie kont w terminie późniejszym niż ustanie stosunku pracy *wynikać mogło z problemów związanych z obiegiem dokumentacji w tak dużej organizacji, jaką jest MUW.* Dodał, że w fazie testów *znajduje się aplikacja informatyczna tworzona przez pracowników mająca zapewnić systemowe rozwiązanie, umożliwiające zautomatyzowane przekazywanie informacji administratorom systemów informatycznych, w związku z zaistnieniem zmian kadrowych, w tym sytuacji rozwiązania umów o pracę*.

Po ustaniu zatrudnienia danej osoby w MUW dokonywane były przez administratorów w ww. systemie czynności związane z wyłączeniem, przeniesieniem oraz modyfikacją danych na kontach użytkowników. IOD wskazał, że *modyfikacje te dotyczyły czynności porządkowych (np. usunięcie przełożonego, usunięcie konta z grup porządkowych).*

(akta kontroli str. 114, 115, 116-119, 120, 166-175)

Powierzanie przetwarzania danych osobowych odbywało się w MUW na podstawie umów powierzenia przetwarzania danych, zawieranych z podmiotami, którym powierzano takie przetwarzanie (stanowiły one załączniki do umów lub postanowienia o powierzeniu przetwarzania umieszczane były w umowie).

Za monitorowanie poprawności przetwarzania powierzonych danych przez podmioty zewnętrzne, jak i nadzór nad przestrzeganiem postanowień zawartych w umowach powierzenia przetwarzania, odpowiedzialni byli dyrektorzy poszczególnych wydziałów (komórek organizacyjnych), właściwi dla danej umowy. Mieli oni obowiązek współpracy z IOD, tj.: informowania IOD o zamiarze podpisania takiej umowy, uzyskania jego akceptacji, przesłania umowy po jej podpisaniu oraz powiadomienia IOD o występowaniu wszelkich naruszeń w tym zakresie.

IOD był m.in. odpowiedzialny za przygotowanie wzoru umowy powierzania przetwarzania danych, zatwierdzonego następnie przez Wojewodę jako załącznik do Polityki ODO.

Po wejściu w życie RODO zaktualizowanych zostało pięć umów powierzenia przetwarzania danych osobowych podmiotom zewnętrznym. Dotyczyły one:

- zapewnienia usług sprzątania, prac gospodarczych, usług portierskich i ochrony (umowa z podmiotem prywatnym z 24 maja 2018 r.);
- zapewnienia usługi sprzątania i ochrony zamiejscowego oddziału MUW w Nowym Sączu (podmiot prywatny; 24 maja 2018 r.);
- Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności (Ministerstwo Rodziny, Pracy i Polityki Społecznej; 25 maja 2018 r.);
- obsługa Systemu Informatycznego „enova" i Systemu Informatycznego „Płatnik" (podmiot prywatny; 1 stycznia 2019 r.);

- obsługa Systemu Informatycznego „Zatrudnienie Cudzoziemców” (Ministerstwo Rodziny, Pracy i Polityki Społecznej; 23 lipca 2018 r.).

Analiza pięciu umów powierzenia przekazania danych przez Wojewodę wykazała, że zawierały one elementy wskazane w art. 28 ust. 3 RODO.

Według stanu na 15 października 2019 r. prowadzony przez IOD:
- rejestr umów powierzenia przetwarzania danych osobowych przez Wojewodę innym podmiotom zawierał 56 pozycji;
- rejestr umów powierzenia przetwarzania danych osobowych Wojewodzie zawierał 27 pozycji;
- rejestr umów wzajemnego powierzenia przetwarzania danych osobowych pomiędzy Wojewodą a innymi podmiotami zawierał osiem pozycji.

W rejestrze umów powierzania przetwarzania danych przez Wojewodę znajdowały się umowy dotyczące przetwarzania danych m.in. w ramach: usług tłumacza przysięgłego; w zbiorze „Koordynacja systemów zabezpieczenia społecznego – świadczenia wychowawcze i świadczenia rodzinne”; uczestnictwa w kursach adaptacyjnych organizowanych w ramach ww. Projektu; dostawy i uruchomienia infrastruktury informatycznej; serwisu użytkowanych systemów informatycznych i oprogramowania; prowadzenia szkoleń przez firmy zewnętrzne; wykonywania operatów szacunkowych przez zewnętrznych rzeczoznawców majątkowych; obsługi klientów MUW przez inne instytucje zewnętrzne; obsługi logistycznej (zapewnienie usług przewozowych, wyrabianie pieczątek).

W okresie objętym kontrolą MUW powierzano przetwarzanie danych osobowych na podstawie umów powierzenia przetwarzania danych osobowych, które zawierano z administratorami tych danych. W okresie od maja 2015 r. do kwietnia 2019 r. MUW zawarł 34 takie umowy. Umowy wskazywały zakres i cel przetwarzania danych i były zawierane na czas określony, także w ramach realizacji wcześniej zawartych umów.

W rejestrze umów powierzania przetwarzania danych osobowych Wojewodzie wpisane były umowy:
- cztery zawarte z Ministrem Infrastruktury i Ministrem Inwestycji i Rozwoju, związane z realizacją programów operacyjnych;
- dwie dotyczące świadczenia usług rekreacyjno-sportowych;
- 19 ze stacjami sanitarno-epidemiologicznymi z terenu Małopolski (Wojewódzką i powiatowymi) dotyczące udostępnienia aplikacji do dokumentowania kontroli;
- po jednej z: Zakładem Karnym w Nowym Sączu (nieodpłatna praca skazanych na rzecz MUW) i Spółdzielnią Socjalną „S.” (aktywizacja zawodowa młodych Subregionu Tarnowskiego).

W rejestrze umów wzajemnego powierzenia przetwarzania danych pięć umów dotyczyło powierzenia przetwarzania danych w związku z zapewnieniem usług sprzątania, usług portierskich i ochrony MUW oraz zamiejscowego oddziału w Nowym Sączu, pozostałe trzy dotyczyły powierzenia przetwarzania danych w związku z: obsługą Systemu Automatycznej Identyfikacji Kluczy (*SAIK*), usługą ochronną w formie monitorowania i ochrony obiektu w systemie dyskretnego ostrzegania i obsługą systemu „Kolejkowicz” w Oddziale Paszportowym MUW.

(akta kontroli str. 25, 35-36, 37-41, 104-105, 106-113, 156, 157-159)

2.3. Monitoring wizyjny w MUW

Opis stanu faktycznego

Zarządzeniem z dnia 18 września 2019 r.[16] Wojewoda ustalił „Politykę ochrony danych osobowych w systemie monitoringu wizyjnego stosowanym w budynkach MUW" (*Polityka monitoringu*) i zobowiązał Dyrektora Generalnego do ustalenia „Instrukcji zarządzania systemem monitoringu wizyjnego stosowanym w budynkach Małopolskiego Urzędu Wojewódzkiego w Krakowie".

Zgodnie z zarządzeniem Dyrektora Generalnego MUW[17] „Instrukcja zarządzania systemem monitoringu wizyjnego stosowanym w budynkach MUW" (*Instrukcja monitoringu*) była dokumentem niepodlegającym udostępnieniu w trybie ustawy o dostępie do informacji publicznej.

Integralną część Instrukcji monitoringu stanowiły załączniki zawierające szczegółowy opis systemu (m.in.: obszar objęty monitoringiem, rozmieszczenie kamer, okres przechowywania obrazu, pomieszczenia, w których przechowywane były dane rejestrowane przez kamery); wzór oświadczenia podpisywanego przez pracowników o zapoznaniu się z Polityką monitoringu; procedura wykonywania i odtwarzania nagrań z kamer; wzór rejestru kopii nagrań z systemu oraz wykaz podmiotów zewnętrznych uprawnionych do uzyskania nagrań z kamer.

Ww. procedury w zakresie monitoringu wizyjnego zostały spisane razem z wejściem w życie Polityki monitoringu i Instrukcji monitoringu. Kamery w budynkach MUW działały już wcześniej, o czym pracownicy byli poinformowani (strona intranetowa).

Po wejściu w życie RODO, w czerwcu 2018 r. do dyrektorów wydziałów (komórek organizacyjnych) została przesłana (drogą elektroniczną) zaktualizowana klauzula informacyjna w zakresie sposobu przetwarzania danych osobowych osób zatrudnionych w MUW lub realizujących zadania na rzecz Urzędu na podstawie innych tytułów prawnych, która zawierała m.in. informacje o sposobie przetwarzania danych osobowych w przypadku stosowania monitoringu wizyjnego. Pismo to zawierało prośbę o udostępnienie klauzuli pracownikom.

W MUW funkcjonował system monitoringu wizyjnego. Polityka monitoringu zakazywała montowania kamer w sposób umożliwiający podgląd m.in. pomieszczeń sanitarnych, palarni, obrazów wyświetlanych na monitorach komputerów służbowych pracowników Urzędu. Wszystkie zarejestrowane dane były zapisywane na dyskach twardych serwerów lub rejestratorów danych i były dostępne przez okres do 60 dni, po tym terminie dane były automatycznie usuwane poprzez nadpisanie. Dane z systemu zapisywane były na serwerach niezależnych od systemu informatycznego MUW.

Oględziny przeprowadzone (11 września 2019 r.) w czterech lokalizacjach MUW wykazały, że we wszystkich ww. budynkach zainstalowany był monitoring wizyjny. Przy wejściach znajdowały się dobrze widoczne i czytelne informacje o zainstalowanych kamerach („obiekt monitorowany" i symbol kamery). Nie stosowano monitoringu w pomieszczeniach wyłączonych na podstawie art. 22^2 Kodeksu pracy[18].

(akta kontroli str. 5-6, 7, 24, 25, 42-45, 82-103)

[16] Zarządzenie Wojewody Małopolskiego z dnia 18 września 2019 r. w sprawie „Polityki ochrony danych osobowych w systemie monitoringu wizyjnego stosowanym w budynkach Małopolskiego Urzędu Wojewódzkiego w Krakowie".

[17] Zarządzenie Dyrektora Generalnego z dnia 19 września 2019 r. w sprawie „Instrukcji zarządzania systemem monitoringu wizyjnego stosowanym w budynkach Małopolskiego Urzędu Wojewódzkiego w Krakowie".

[18] Ustawa z dnia

2.4. Ochrona systemów informatycznych

Opis stanu faktycznego

W przypadku budynku MUW stosowano w ramach:

- zabezpieczenia serwerowni: system monitoringu wizyjnego, system kontroli dostępu, system sygnalizacji pożaru i gaszenia gazem oraz ochrona budynku w postaci całodobowego dozoru świadczonego przez firmę zewnętrzną;
- zabezpieczenia pomieszczeń, w których przechowywane były zbiory danych: system kontroli dostępu w części pomieszczeń, system monitoringu wizyjnego, SAIK i całodobowego dozoru portierskiego świadczonego przez firmę zewnętrzną;
- kontroli dostępu dla osób nieupoważnionych poprzez systemy: kontroli dostępu i monitoringu wizyjnego;
- sygnalizacji włamania, napadu i pożaru (na podstawie umów zawartych z dwoma firmami zewnętrznymi);
- ochrony budynków: system monitoringu wizyjnego oraz całodobowy dozór portierski świadczony przez dwie firmy zewnętrzne (w tym jedna dla lokalizacji przy pl. Na Stawach 3).

W przypadku budynków Delegatur MUW w: Nowym Sączu i Tarnowie stosowano m.in. elektroniczne systemy kontroli dostępu, systemy sygnalizacji pożaru, dozór fizyczny (realizowany przez zewnętrzne firmy), monitoring wizyjny oraz systemy sygnalizacji włamania i napadu.

Administrator wyjaśnił, że systemy zabezpieczeń były sprawne, konserwowane i sprawdzane w ustalonych umowami terminach.

(akta kontroli str. 182-183, 184-191)

W zakresie obowiązujących w MUW regulacji dotyczących tworzenia kopii bezpieczeństwa baz danych obowiązywały:

- Instrukcja ZSI;
- rejestr wykonywania i odtwarzania kopii zapasowych.

Instrukcja ZSI została przyjęta (5 listopada 2015 r.) na podstawie §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[19]. Zakładała, że administrator systemu teleinformatycznego miał konfigurować ustawienia systemu teleinformatycznego, tak aby hasło użytkownika było odpowiednio złożone. Załącznik nr 7 do Instrukcji ZSI („Rejestr wykonania i odtworzenia kopii zapasowych") przewidywał w szczególności wskazanie: rodzaju kopii zapasowej, informatycznego nośnika danych, na którym zapisano kopię zapasową, oraz rodzaj zdarzenia.

(akta kontroli str. 24, 25, 42-45)

W ramach kontroli przeprowadzono oględziny wdrożonych zabezpieczeń serwerowni w siedzibie MUW (17 września 2019 r.). Do pomieszczeń serwerowni prowadziło dwoje drzwi, a dostęp ograniczony był czytnikami kart elektronicznych.

Monitoring pomieszczenia serwerowni był prowadzony poprzez rejestrację obrazu. Ewidencjonowano przebywanie osób w serwerowni – wewnątrz pomieszczenia znajdował się zeszyt wejść/wyjść do/z serwerowni. Centralka klimatyzacji powiadamiała (automatycznie) SMS-owo odpowiedzialnych pracowników o zmianach granicznych zakresów temperatury wewnątrz serwerowni. W przypadku zaniku napięcia następowało również powiadomienie (automatycznie) SMS-owo pracowników MUW.

[19] Dz. U. Nr 100, poz. 1024.

Wewnątrz serwerowni znajdowały się czujki systemu przeciwpożarowego, sygnalizator alarmu przeciwpożarowego oraz sześć wolnostojących gaśnic (do gaszenia urządzeń pod napięciem). Zainstalowano również system automatycznego gaszenia pożaru. Wewnątrz serwerowni działał system klimatyzacji namiarowej. Urządzenia serwerowni podłączone były do układu podtrzymywania napięcia „UPS" oraz agregatu zapewniającego awaryjne zasilanie.

W pomieszczeniu znajdowały się serwery w specjalnych szafach typu „RACK" (na podwyższeniu nad podłogą). Zapewniały one m.in. tworzenie kopii bezpieczeństwa baz danych MUW, wymiennie z serwerownią zlokalizowaną w innym miejscu Krakowa. Stan okablowania był bez zastrzeżeń (nie występowały widoczne ślady mechanicznych uszkodzeń izolacji).

Przez pomieszczenie serwerowni nie przebiegały rury. W pomieszczeniu nie znajdowały się urządzenia komputerowe wycofane z użytku, materiały łatwopalne (meble, dokumentacja, papierowe/tekturowe opakowania).

(akta kontroli str. 7, 28-29)

W okresie od 25 maja 2018 r. do czasu kontroli NIK tworzone były kopie bezpieczeństwa dla baz danych dla wszystkich systemów Urzędu. Kopie bezpieczeństwa wykonywano według ustalonego planu z częstotliwością zależną od systemu. Kopie te przechowywane były na dedykowanych macierzach backupowych oraz na bibliotece taśmowej „L.". Kopie bezpieczeństwa baz danych dla wszystkich systemów MUW przechowywano w serwerowni zlokalizowanej w Krakowie. Dodatkowo bezpieczeństwo kopii zapasowych było zwiększane poprzez zastosowanie architektury redundantnej systemu backupowego.

(akta kontroli str. 182-183, 184-191)

W MUW do zabezpieczania przed nieuprawnionym dostępem z zewnątrz do danych osobowych przetwarzanych w systemie informatycznym wykorzystywano […][20]. Licencje dotyczące tego systemu były aktualne.

(akta kontroli str. 156, 157-159)

Podstawowym zabezpieczeniem dostępu do komputerów przyjętym w MUW było hasło i login. Badanie sposobów zabezpieczenia dostępu do komputerów przeprowadzono w ramach oględzin (25 września 2019 r.). Oględzinami objęto wybraną losowo (dobór przypadkowy) grupę 10 komputerów użytkowanych przez pracowników Oddziału Obywatelstwa i Nadzoru w Wydziale Spraw Obywatelskich i Cudzoziemców MUW, obsługujących wyłącznie wewnętrzne bazy danych i służących do przetwarzania danych osobowych (bez stanowisk mających dostęp do rejestrów centralnych, np. PESEL, dowody osobiste, paszporty).

Oględziny wykazały, że:

- pracownicy prawidłowo logowali się do systemu komputerowego, tzn. zgodnie z obowiązującymi w MUW procedurami;
- pracownicy byli w stanie zablokować ekran komputera na wypadek czasowego odejścia od komputera, a następnie go odblokować.

(akta kontroli str. 30-34)

Stwierdzone nieprawidłowości

W działalności MUW w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK ocenia pozytywnie działania MUW w obszarze stosowania wdrożonych rozwiązań organizacyjnych dotyczących ochrony danych osobowych.

[20] Na podstawie pisma Wojewody Małopolskiego z 14 lutego 2020 r. znak ZI-II.1610.2.2019 NIK wyłączyła jawność informacji zgodnie wnioskiem zawartym w ww. piśmie w zakresie szczegółowych danych dot. stosowanych technicznych środków bezpieczeństwa przetwarzanych danych osobowych..

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

3.1. Postępowanie w przypadku naruszenia ochrony danych osobowych

Opis stanu faktycznego

W okresie objętym kontrolą (do 1 października 2019 r.) w MUW wystąpiło pięć przypadków naruszenia ochrony danych osobowych (ujętych w aktualizowanym rejestrze naruszeń), tj.:

- stwierdzone 9 sierpnia 2018 r. (incydent z 2 sierpnia 2018 r.; zgłoszenie podpisane przez Administratora 10 września 2018 r.) w Wydziale Polityki Społecznej (Oddział Koordynacji Świadczeń Rodzinnych i Wychowawczych), polegało na wysłaniu danych osobowych (identyfikacyjnych i kontaktowych) klienta do niewłaściwego odbiorcy (wskutek złej nazwy skrzynki ePUAP w EZD)[21]. Podjęto pięć działań zaradczych, w tym m.in.: skierowano pismo do osoby fizycznej, do której mylnie wysłano pismo zawierające dane osobowe, informujące o konieczności niezwłocznego usunięcia danych osobowych, których nie ma ona prawa przetwarzać, ze swoich zasobów; podjęto działania w celu weryfikacji istniejącej bazy adresowej; skierowano do Ministra Cyfryzacji informację o błędzie krytycznym formularzy pism ogólnych do Urzędu[22];
- stwierdzone 16 lipca 2019 r. (incydent z 14 lipca 2019 r.; zgłoszenie podpisane 19 lipca 2019 r.), zgłoszone także do MSWiA przez IOD, polegało na ujawnieniu danych niewłaściwej osoby (imię i nazwiska, adres zamieszkania/pobytu) podczas rozmowy telefonicznej w Centrum Powiadamiania Ratunkowego Wydziału Bezpieczeństwa i Zarządzania Kryzysowego)[23]. Jako podjęte działania zaradcze wskazano m.in.: przesłanie wszystkim pracownikom Centrum Powiadamiania Ratunkowego (CPR) informacji o naruszeniu, celem zwrócenia uwagi na bezpieczeństwo przetwarzania danych osobowych; zaplanowanie dodatkowych szkoleń z personelem CPR w zakresie ochrony danych osobowych przetwarzanych w ww. Wydziale (na dzień 28 listopada 2019 r. szkoleń nie przeprowadzono; zaplanowano je na 20 stycznia 2020 r.);
- stwierdzone 12 lipca 2019 r. (zgłoszenie podpisane 23 lipca 2019 r.), w Wydziale Polityki Społecznej, polegało na wysłaniu danych osobowych (imię i nazwiska, adres zamieszkania klienta oraz imię i nazwisko dziecka) do niewłaściwego odbiorcy (stwierdzone na podstawie zgłoszenia telefonicznego osoby, która otrzymała korespondencję dotyczącą świadczeń socjalnych dla innej osoby (ze względu na zbieżność nazwisk)[24]. Wskazano podjęte działania zaradcze, w tym m.in.: wprowadzono obowiązek dodatkowej weryfikacji zgodności danych osobowych przez innego referenta, pomiędzy: danymi umieszczonymi na etykiecie/wkładce a danymi osoby, której korespondencja dotyczyła, przed fizycznym umieszczeniem korespondencji w kopercie; zaplanowano przeprowadzenie dodatkowych szkoleń w zakresie ochrony danych osobowych przetwarzanych w ww. Wydziale (na dzień 28 listopada 2019 r. szkoleń nie przeprowadzono, zaplanowano je na 20 grudnia 2019 r.);

[21] Incydent związany był z naruszeniem poufności danych osobowych poprzez wysłanie pisma skierowanego do Urzędu Miasta w Krakowie za pośrednictwem platformy ePUAP do niewłaściwego adresata (osoby prywatnej). Naruszenie wynikało z przypisania w systemie informatycznym nazwie instytucji, do której miało trafić pismo, błędnego adresu skrzynki ePUAP innej osoby fizycznej.

[22] E-mail do epuap-pomoc@coi.gov.pl z 13 września 2018 r.

[23] Incydent związany był z naruszeniem poufności danych: dane osobowe osoby fizycznej zostały ujawnione innej nieuprawnionej osobie fizycznej.

[24] Incydent związany był z naruszeniem poufności danych: dane osobowe zostały wysłane do niewłaściwego odbiorcy (nieuprawnionej osoby fizycznej).

- stwierdzone 4 września 2019 r. (incydent z 29 sierpnia 2019 r.; podpisane 6 września 2019 r.), w Wydziale Polityki Społecznej, polegające na wysłaniu danych osobowych (imię i nazwiska, adres zamieszkania, imiona rodziców, data urodzenia, nr PESEL, nr telefonu) do niewłaściwego odbiorcy oraz ujawnieniu danych szczególnej kategorii (stan zdrowia) klienta[25]. Jako podjęte działanie zaradcze wskazano ponownie wprowadzenie obowiązku dodatkowej weryfikacji danych adresata wygenerowanych z *EZD* (etykieta/wkładka) z danymi organu (instytucji) właściwego w danej sprawie;
- stwierdzone 4 września 2019 r., (incydent z 2 września 2019 r.; podpisane 6 września 2019 r.), w Wydziale Polityki Społecznej, polegające na wysłaniu danych osobowych (nazwiska i imiona, adres zamieszkania lub pobytu, informacja o ustaleniu prawa do świadczeń) w decyzji w sprawie ustalenia prawa do świadczeń rodzinnych do błędnego adresata[26]. Jako podjęte działanie zaradcze wskazano obowiązek dokładnej weryfikacji przez osobę zajmującą się kopertowaniem korespondencji pod kątem prawidłowego adresowania i umieszczania dokumentacji w kopertach oraz obowiązek dokładnej powtórnej weryfikacji dokumentacji pod kątem prawidłowości kopertowania.

Incydenty zbliżone czasowo, tj. z 29 sierpnia i 2 września 2019 r. dotyczyły różnych pracowników Wydziału Polityki Społecznej MUW.
We wskazanych czterech przypadkach, w których dane osobowe zostały ujawnione nieuprawnionej osobie fizycznej, jako skutki naruszenia dla osób fizycznych wskazano utratę kontroli nad własnymi danymi osobowymi. Wszystkie naruszenia ochrony danych osobowych zostały zgłoszone do Prezesa UODO.

Zgłoszenia do Prezesa UODO w imieniu Administratora dokonywał IOD, kwalifikując je w każdym przypadku jako kompletne i jednorazowe.

We wszystkich przypadkach:
- wskazywano na naruszenie poufności danych (podstawowych) klientów MUW;
- przyczynę naruszenia określano jako wewnętrzne działanie niezamierzone;
- określano możliwe konsekwencje jako utrata kontroli nad własnymi danymi osobowymi;
- przyjmowano, że nie wystąpiło wysokie ryzyko naruszenia praw i wolności osób fizycznych;
- podejmowano działania zaradcze – odpowiednio: weryfikacja bazy adresowej; szkolenie i rozmowa dyscyplinująca z pracownikiem; obowiązek dodatkowej weryfikacji danych adresowych; obowiązek dodatkowej weryfikacji dokumentacji;
- osoby, których dane dotyczyły, były powiadomione o naruszeniu indywidualnie (w pierwszych dwóch ww. przypadkach) lub nie były zawiadamiane ze względu na stwierdzony brak wysokiego ryzyka naruszenia praw i wolności (w trzech przypadkach).

Dyrektor Generalny MUW wyjaśnił, że każdy przypadek został szczegółowo przeanalizowany i wyjaśniono przyczyny wystąpienia naruszeń.

(akta kontroli str. 24, 25, 35-36, 37-41, 42-45)

[25] Incydent związany był z naruszeniem poufności danych: dane osobowe zostały wysłane do niewłaściwego odbiorcy – nieuprawnionego organu administracji państwowej (decyzję Wojewody wraz z aktami sprawy przesłano do Powiatowego Urzędu Pracy w Nowym Targu zamiast do takiego Urzędu w Tarnowie). Informacja o zdarzeniu przekazana została przez inną instytucję (PUP w Nowym Targu), do której omyłkowo skierowano decyzję w sprawie pozbawienia statusu bezrobotnego (dla PUP w Tarnowie) wraz z informacją o przekazaniu sprawy zgodnie z właściwością.

[26] Incydent naruszenie poufności danych: dane osobowe zostały wysłane do niewłaściwego odbiorcy – nieuprawnionej osoby fizycznej.

3.2. Postępowanie z danymi osobowymi

Opis stanu faktycznego

W okresie objętym kontrolą (do 1 października 2019 r.) do MUW wpłynęły trzy wnioski o usunięcie danych osobowych. W dwóch przypadkach przetwarzane dane osobowe zostały usunięte, tj.:

- poprzez usunięcie pliku protokołu z kontroli przeprowadzonej w podmiocie leczniczym w lutym 2013 r., zawierającym dane osobowe (m.in. adres i nr telefonu) z BIP MUW oraz zablokowanie możliwości wyświetlania w wynikach wyszukiwania adresu URL, pod którym znajdowała się kopia protokołu kontroli, tak aby podany adres (URL) nie był osiągalny dla „G.", wykorzystując narzędzie do usuwania takich adresów („G.S.C."), co spowodowało trwałe usunięcie jakichkolwiek powiązań ze stroną internetową, na której znajdował się protokół (elektroniczny wniosek klienta MUW z 14 sierpnia 2018 r., odpowiedź IOD z 20 września 2018 r., informująca o usunięciu danych);
- poprzez zanonimizowanie danych osobowych w zakresie obejmującym dane adresowe osoby wchodzącej w skład rady nadzorczej w przedsiębiorstwie państwowym, uwidocznionych na stronie BIP MUW (elektroniczny wniosek z 10 lipca 2018 r., odpowiedź z 17 lipca 2018 r.). Na podstawie tego przypadku dokonano anonimizacji zarządzenia Wojewody w zakresie danych adresowych.

W trzecim przypadku elektroniczny wniosek klienta MUW (z 24 stycznia 2019 r.) został przesłany do Urzędu Marszałkowskiego Województwa Małopolskiego (31 stycznia 2019 r.), gdyż Wojewoda Małopolski we wskazanym przez wnioskodawcę zakresie, nie był administratorem danych osobowych. O tym fakcie została poinformowana również osoba zainteresowana usunięciem danych osobowych (imię, nazwisko, adres e-mail).

W udzielanych odpowiedziach IOD przesyłał ogólną klauzulę informacyjną stosowaną w MUW.

(akta kontroli str. 25, 35-36, 37-41)

W okresie objętym kontrolą do MUW nie wpłynęły żądania sprostowania bądź uzupełnienia niekompletnych danych.

(akta kontroli str. 35-36, 37-41)

Oględziny przeprowadzone w czterech lokalizacjach MUW (11 września 2019 r.) wykazały, że tablice informacyjne znajdujące się w ogólnodostępnych pomieszczeniach, tj. w holach, na korytarzach i w salach, w których odbywała się rejestracja i obsługa klientów, nie zawierały danych osobowych.

(akta kontroli str. 5-7)

Dokumenty papierowe przeznaczone do zniszczenia pakowane były przez pracowników Urzędu do koszy transportowych osłoniętych folią nieprzeźroczystą oraz transportowane pojazdami służbowymi do firmy zewnętrznej, gdzie były w obecności pracowników MUW niszczone. MUW nie miał zawartej umowy powierzenia przetwarzania danych osobowych w tym zakresie (nie występowało ryzyko bezpośredniego wglądu i dostępu do przywiezionych dokumentów przez pracowników ww. firmy podczas realizacji usługi).

MUW zawarł umowę współpracy w zakresie odbioru i zagospodarowania odpadów z firmą zewnętrzną, w ramach, której przekazywano do utylizacji części komputerowe i AGD. Wojewoda wskazał, że ze względów bezpieczeństwa nie przekazywano w ramach tej umowy nośników zawierających dane osobowe. Z takich nośników usuwano informacje za pomocą m.in. urządzenia do kompletnego

kasowania danych ze wszystkich nośników magnetycznych […][27], a następnie składowano w zabezpieczonym pomieszczeniu.

(akta kontroli str. 156, 157-159)

3.3. Ochrona danych osobowych pracowników

Opis stanu faktycznego

W MUW opracowano klauzulę informacyjną dla pracowników oraz osób, które wykonują zadania dla Urzędu na podstawie innych tytułów prawnych (załącznik nr 13 do Polityki ODO)[28]. Klauzula została udostępniona pracownikom MUW w systemie obiegu dokumentów EZD (przekazanie do wiadomości pracowników nastąpiło przez dyrektora Wydziału Administracji i Logistyki 20 czerwca 2018 r.) oraz była udostępniana każdej nowo zatrudnianej osobie oraz osobie, która wykonywała prace na rzecz Urzędu na podstawie innych tytułów prawnych.

(akta kontroli str. 25, 35-36, 37-41)

Analiza 63 akt osobowych pracowników Wydziału Rewaloryzacji Zabytków Krakowa i Dziedzictwa Narodowego MUW, Kancelarii Urzędu oraz Archiwum Zakładowego zlokalizowanych w Wydziale Organizacji i Kontroli MUW wykazała, że w aktach osobowych siedmiu pracowników znajdowały się ich oświadczenia o zapoznaniu się z m.in. z: RODO, zasadami bezpieczeństwa użytkowania systemu teleinformatycznego, „Klauzulą informacyjną dla pracowników oraz osób, które wykonują zadania dla MUW na podstawie innych tytułów prawnych".

Dyrektor Generalny wyjaśnił, że informacja pracodawcy o przetwarzaniu danych osobowych pracownika pozostaje w pierwotnej, tj. elektronicznej wersji dokumentów, i jako taka nie jest dołączana do akt osobowych poszczególnych pracowników. Nowozatrudnieni pracownicy zapoznawani są ze stosownym dokumentem (tzw. klauzulą RODO dla pracownika), który to dokument dołączany jest do akt osobowych pracownika.

(akta kontroli str. 114, 115, 121-139)

Analiza wybranych 11 umów zlecenia i/lub umów o dzieło wykazała, że MUW informował zleceniobiorców o przetwarzaniu ich danych osobowych.

W okresie od 25 maja 2018 r. do 15 października 2019 r. przeprowadzono 131 postępowań rekrutacyjnych. Kontrolą objęto wybranych w sposób losowy 10 postępowań prowadzonych od 31 maja 2018 r. do 16 sierpnia 2019 r. (8% postępowań).

W ogłoszeniach o naborze we wszystkich badanych postępowaniach informowano kandydatów o warunkach przetwarzania ich danych osobowych. Ogłoszenia te zawierały klauzulę informacyjną wskazującą m.in. na: przepisy RODO, kontakt do IOD, cel przetwarzania danych, okres przechowywania danych i uprawnienia kandydatów. Wskazywano w nich, że każdy kandydat przystępując do naboru podawał swoje dane dobrowolnie, a bez podania wymaganych danych osobowych nie był możliwy udział w naborze.

(akta kontroli str. 114, 115, 152-155, 176-181)

W MUW przyjęto, że okres przechowywania danych to czas niezbędny do przeprowadzenia naboru na stanowisko pracy w służbie cywilnej, z uwzględnieniem trzech miesięcy, w których dyrektor generalny ma możliwość wyboru kolejnego wyłonionego kandydata, w przypadku, gdy ponownie zaistnieje konieczność obsadzenia tego samego stanowiska. Powyższe stanowisko przyjęto na podstawie

[27] Na podstawie pisma Wojewody Małopolskiego z 14 lutego 2020 r. znak ZI-II.1610.2.2019 NIK wyłączyła jawność informacji zgodnie wnioskiem zawartym w ww. piśmie w zakresie szczegółowych danych dot. typu urządzenia.

[28] Obejmowała ona informacje o przetwarzaniu danych osobowych w ramach: monitoringu wizyjnego, umieszczania danych w Internecie (BIP), akt osobowych i tzw. systemów wykorzystywanych do obsługi zatrudnienia, ZFŚS i PKZP oraz wystąpienia wypadku przy pracy oraz w drodze do pracy lub z pracy.

art. 33 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej[29]. O takim postępowaniu kandydaci informowani byli każdorazowo w ogłoszeniu o naborze w klauzuli informacyjnej dotyczącej danych osobowych.

(akta kontroli str. 182-183, 184-191)

Stwierdzone nieprawidłowości

W działalności MUW w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK ocenia pozytywnie działania Urzędu w obszarze zarządzania danymi osobowymi przetwarzanymi, w tym gromadzonymi, w MUW.

IV. Uwagi i wnioski

W związku z niestwierdzeniem nieprawidłowości NIK nie formułuje wniosków i uwag pokontrolnych.

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 Krakowie. 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.

Wobec niesformułowania wniosków i uwag NIK nie oczekuje odpowiedzi na niniejsze wystąpienie.

Kraków, stycznia 2020 r.

Kontrolerzy:

Małgorzata Korusiewicz
główny specjalista kontroli państwowej

Paweł Lipowski
specjalista kontroli państwowej

[29] Dz.U. poz. 1559 ze zm.