



NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej



RPLI/474300/2019 P
Data: 2019-12-16

KAP.410.006.02.2019

MAZOWIECKI URZĄD WOJEWÓDZKI W WARSZAWIE ODDZIAŁ ZARZĄDZANIA OBSŁUGĄ KLIENTA I DOKUMENTACJA		
wzrost Gina	2019 -12- 16	wzrost dnia
Za: <i>bz</i>		

Pan
Konstanty Radziwiłł
Wojewoda Mazowiecki
Mazowiecki Urząd Wojewódzki w Warszawie
Ul. Plac Bankowy 3/5
00 – 950 Warszawa

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Mazowiecki Urząd Wojewódzki w Warszawie, ul. Plac Bankowy 3/5,00 - 950 Warszawa (dalej MUW lub Urząd)
Kierownik jednostki kontrolowanej	Konstanty Radziwiłł (poprzednio, tj. do dnia 10 listopada 2019 r. Zdzisław Sipiera)
Zakres przedmiotowy kontroli	1. Organizacja ochrony danych osobowych w jednostce. 2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych. 3. Zarządzanie danymi osobowymi przetwarzanymi, w tym gromadzonymi w jednostce.
Okres objęty kontrolą	Od 25 maja 2018 r. do czasu zakończenia kontroli oraz dla zdarzeń wcześniejszych, jeśli mają wpływ na kontrolowaną działalność.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 w związku z art. 5 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli ¹
Kontroler	Paweł Łukasiewicz, doradca ekonomiczny, upoważnienie do kontroli nr KAP/72/2019 z dnia 11 września 2019 r. Dorota Paszkiewicz, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/71/2019 z dnia 11 września 2019 r.
	(akta kontroli str. 1-2)
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej

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

II. Ocena ogólna¹ kontrolowanej działalności

Najwyższa Izba Kontroli nie stwierdziła w MUW nieprawidłowości dotyczących przygotowania Urzędu do wdrożenia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)² - dalej RODO.

W Urzędzie opracowano system przetwarzania i zabezpieczania danych osobowych zgodny z wymogami RODO. Pracownicy Urzędu zostali przeszkoleni w związku z wejściem w życie nowych przepisów prawa oraz zapoznani ze zaktualizowanymi procedurami dotyczącymi bezpieczeństwa informacji. Realizując obowiązki określone w RODO, Wojewoda powołał Inspektora Ochrony Danych (IOD) oraz jego zastępcę i umożliwił im realizację zadań w sposób niezależny. Osoby pełniące te funkcje posiadały odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. W kontrolowanym okresie NIK nie stwierdziła zaniedbań w realizacji obowiązków IOD. Ochrona danych osobowych, z wyjątkiem niewielkich odstępstw, prowadzona była zgodnie z wytycznymi określonymi w RODO i w uregulowaniach wewnętrznych.

W MUW stosowano techniczne, fizyczne i informatyczne środki bezpieczeństwa, służące utrzymaniu poufności, integralności i odporności systemów oraz usług przetwarzania.

Zawiadomienie o naruszeniu ochrony danych osobowych sporządzono zgodnie z przepisami RODO oraz z przyjętymi uregulowaniami wewnętrznymi i terminowo przekazano je do Prezesa Urzędu Ochrony Danych Osobowych (dalej Prezes UODO).

Pracodawca, jako Administrator, prawidłowo informował kandydatów do pracy, pracowników, zleceniobiorców i petentów o przetwarzaniu ich danych osobowych. Stwierdzone nieprawidłowości dotyczyły niedotrzymania przez dziewięciu pracowników terminu dostarczenia oświadczeń o zapoznaniu się z Polityką ochrony danych osobowych MUW do Biura Kadr i Obsługi prawnej oraz trzech przypadków przetwarzania przez pracowników MUW danych osobowych bez upoważnień adekwatnych do zajmowanego stanowiska i zakresu przetwarzanych danych osobowych.

III. Opis ustalonego stanu faktycznego kontrolowanej działalności

OBSZAR
Opis stanu
faktycznego

1. jednostce

Organizacja ochrony danych osobowych w

1.1. Przygotowanie dokumentacji wymaganej przepisami RODO

W związku z wejściem w życie przepisów RODO, Inspektor Ochrony Danych w MUW oraz jego zastępca przeprowadzili i sporządzili ogólną analizę ryzyka związanego z przetwarzaniem danych osobowych. W dokumencie tym zidentyfikowano m.in. zagrożenia związane z przetwarzaniem danych osobowych w urzędzie oraz mechanizmy im zapobiegające.

¹ Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną ocenę negatywną albo ocenę w formie opisowej.

² Dz. U UE L119 z 4 maja 2016 r., str. 1. ze zm.

(akta kontroli str. 9-53)

W MUW opracowano dokumentację ochrony danych osobowych uwzględniającą wymogi RODO w dwóch dokumentach:

- *Procedura oceny i zgłaszania naruszeń ochrony danych osobowych w Mazowieckim Urzędzie Wojewódzkim w Warszawie* (zatwierdzona przez Wojewodę Mazowieckiego w dniu 25 maja 2018 r. i obowiązująca do czasu opracowania niżej wymienionego dokumentu),
- *Polityka ochrony danych osobowych Mazowieckiego Urzędu Wojewódzkiego w Warszawie* (zatwierdzona przez Wojewodę Mazowieckiego w dniu 12 września 2019 r.).

(akta kontroli str. 9-13,226-458)

Procedura oceny i zgłaszania naruszeń ochrony danych osobowych w Mazowieckim Urzędzie Wojewódzkim w Warszawie została przekazana pracownikom MUW do zapoznania się (za pośrednictwem poczty elektronicznej), a ponadto jej treść zamieszczono w intranecie MUW w zakładce „RODO”.

W przypadku *Polityki ochrony danych osobowych Mazowieckiego Urzędu Wojewódzkiego w Warszawie*, IOD MUW poinformował dyrektorów wydziałów/biur MUW, aby zobowiązali wszystkich pracowników do podpisania oświadczeń o zapoznaniu się z treścią ww. dokumentu oraz przekazali oświadczenia do Biura Kadr i Obsługi Prawnej (BKOP) w terminie do 18 września 2019 r. Szczegółowa kontrola 70 losowo wybranych oświadczeń pracowników wykazała, że dziewięciu pracowników nie sporządziło oświadczeń i nie przekazało ich w ww. terminie do BKOP (szczegółowy opis w punkcie *stwierdzone nieprawidłowości*).

(akta kontroli str. 243-244,294-295,1583-1607)

1.2. Wyznaczenie i działanie Inspektora Ochrony Danych

Zgodnie z art. 37 ust. 1 lit. a RODO, Wojewoda Mazowiecki z dniem 1 stycznia 2019 r. wyznaczył Inspektora Ochrony Danych w MUW (poprzedni IOD pełnił funkcję do 30 listopada 2018 r., i z tym dniem rozwiązał umowę o pracę³). Ponadto w dniu 16 sierpnia 2019 r., Wojewoda Mazowiecki wyznaczył Zastępcę IOD w MUW.

O wyznaczeniu IOD i jego zastępcy terminowo poinformowano Prezesa Urzędu Ochrony Danych Osobowych.

(akta kontroli str. 16-18,527-584,982-1024)

IOD i jego zastępca byli etatowymi pracownikami Urzędu zatrudnionymi w Biurze Ochrony Urzędu. W zakresach czynności ww. osób wskazano, że IOD podlega bezpośrednio administratorowi danych osobowych, tj. Wojewodzie Mazowieckiemu, natomiast zastępca IOD podlega bezpośrednio IOD. IOD oraz jego zastępca nie wykonywali innych zadań niezwiązanych z ochroną danych osobowych i tym samym nie zachodziło ryzyko konfliktu interesów, o których mowa w art. 38 ust. 6 RODO.

(akta kontroli str. 18,542-543,555-556,567-568,1761-1765)

Zgodnie z art. 37 ust. 7 RODO w ogólnodostępnych miejscach - m.in. na stronie internetowej Urzędu oraz na tablicach informacyjnych w skontrolowanych punktach obsługi klienta MUW podany był aktualny kontakt do IOD.

(akta kontroli str. 1384-1385,1699,1704-1705,1709,1720,1738,1747,1749)

Zarówno poprzedni IOD jak i obecny, a także zastępca IOD posiadali niezbędne kwalifikacje, o których mowa w art. 37 ust. 5 RODO, poparte wykształceniem, praktyką zawodową, kursami i szkoleniami związanymi z problematyką RODO.

(akta kontroli str. 1682-1687)

³ W okresie od 1 do 31 grudnia 2018 r. osoba z którą rozwiązano umowę o pracę, w ramach umowy zlecenia wykonywała na rzecz MUW zadania określone w art. 39 RODO.

IOD realizował zadania określone w art. 39 RODO, tj. m.in.:

- informował administratora, podmiot przetwarzający i pracowników o ich obowiązkach związanych z ochroną danych, w szczególności poprzez przeprowadzanie szkoleń i instruktarzy (np. w intranecie),
- monitorował przestrzeganie przepisów w zakresie ochrony danych osobowych, w szczególności poprzez przekazywanie pracownikom informacji o zmianach w przepisach związanych z ochroną danych osobowych,
- współpracował z organem nadzorczym i pełnił funkcję punktu kontaktowego dla organu nadzorczego, w szczególności poprzez uczestnictwo w szkoleniach organizowanych dla IOD przez organ nadzorczy, a także przy zgłaszaniu przypadków naruszeń ochrony danych do UODO.

(akta kontroli str. 1046-1375)

1.3. Inne działania jednostki związane z wdrażaniem RODO

Przeprowadzone oględziny w miejscach, wybranych przez kontrolera przeznaczonych do obsługi interesantów, tj. w Punkcie Obsługi Klienta, w Wydziale Polityki Społecznej w MUW, w Wydziale Spraw Cudzoziemców w MUW oraz w Wydziale Spraw Obywatelskich w MUW wykazały, że w każdym z ww. miejsc znajdowały się informacje, o których mowa w art. 13 ust. 1 i 2 RODO, tj. o przetwarzaniu danych osobowych petentów.

(akta kontroli str. 1699-1760)

W okresie objętym kontrolą w Urzędzie nie były prowadzone kontrole zewnętrzne dotyczące przygotowania do wdrożenia RODO.

(akta kontroli str. 9,19, 978-981)

W okresie od maja 2018 r. do września 2019 r. w MUW został przeprowadzony jeden audyt wewnętrzny⁴ pn. *Ocena dostosowania zasad przetwarzania, wykorzystywania i przechowywania danych osobowych w jednostce do wymagań rozporządzenia unijnego w sprawie ochrony danych osobowych*. W sprawozdaniu z audytu wskazano m.in., że system ochrony przetwarzania danych osobowych w urzędzie wymaga dalszych działań rozwojowych lub doskonalących. Sporządzono dokument pn. *Program działań korygujących i zapobiegawczych*, w którym wskazano m.in. planowane działania korygujące, osobę odpowiedzialną za ich realizację oraz termin realizacji. W przekazanych kontrolerom NIK w dniu 1 października 2019 r. wyjaśnieniach Wojewody Mazowieckiego wskazano, że czynności sprawdzające stan wdrożenia zaleceń audytu oceniającego dostosowanie zasad ochrony danych osobowych do wymagań rozporządzenia unijnego RODO miały zostać przeprowadzone w IV kwartale 2019 r. Na dzień zakończenia czynności kontrolnych w jednostce⁵ czynności te nie zostały przeprowadzone.

(akta kontroli str. 314-407,1046-1056)

⁴ Sprawozdanie z audytu sporządzono 17 lipca 2018 r.

⁵Tj. 15 listopada 2019 r.

Szkolenia dla pracowników Urzędu związane z ochroną danych osobowych i przetwarzaniem danych w związku z wejściem w życie RODO, prowadzone były zarówno przez podmioty zewnętrzne, a także przez Inspektora Ochrony Danych w MUW i jego zastępcę. Szkoleniami objęto zarówno osoby nowo zatrudnione, jak i pozostałych pracowników, w tym kadrę kierowniczą, m.in. w ramach cyklu szkoleń *Praktyczne aspekty ochrony danych osobowych w kontekście RODO*.

Szczegółowa kontrola pracowników Wydziału Zdrowia oraz Biura Kadr i Obsługi Prawnej wykazała, że po wejściu w życie przepisów RODO wszyscy pracownicy tych komórek organizacyjnych Urzędu uczestniczyli w szkoleniach związanych z ochroną danych osobowych.

(akta kontroli str. 657-660,1777-1783)

Na przygotowanie i realizację zadań dotyczących ochrony danych osobowych, w związku z wejściem przepisów RODO, w latach 2018-2019 wydatkowano w Urzędzie kwotę ok. 121,4 tys. zł. Środki zostały przeznaczone na zatrudnienie IOD oraz jego zastępcy (ok. 114 tys. zł), szkolenia dla pracowników (6 tys. zł) oraz zakup prenumerat, czasopism i książek tematycznych dla IOD (1,4 tys. zł).

(akta kontroli str. 9,19,1626-1676)

W kontrolowanym okresie Prezes Urzędu Ochrony Danych Osobowych nie nakładał na MUW kar pieniężnych, innych sankcji lub obowiązków naprawczych w związku z niewłaściwym stosowaniem RODO.

(akta kontroli str. 9-19)

**Stwierdzone
nieprawidłowości**

W działalności Urzędu w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Dziewięciu z 70 pracowników, których dokumentację objęto kontrolą, nie sporządziło i nie przekazało do 18 września 2019 r. do Biura Kadr i Obsługi Prawnej (BKOP) oświadczeń o zapoznaniu się z treścią *Polityki ochrony danych osobowych Mazowieckiego Urzędu Wojewódzkiego w Warszawie* mimo, że IOD MUW poinformował dyrektorów wydziałów/biur MUW, aby zobowiązali wszystkich pracowników do dopełnienia ww. obowiązków.

(akta kontroli str. 245-295,1583-1607,1614)

Wojewoda Mazowiecki wyjaśnił, że (...) *Pojedyncze przypadki osób, które były w tym terminie obecne w pracy, ale przekazały oświadczenia później, wynikały-na podstawie informacji uzyskanych bezpośrednio od nich - z natłoku obowiązków i braku czasu, który pozwoliłby zapoznać się z dokumentem (Polityką) wcześniej. Należy podkreślić, iż ostatecznie wszystkie oświadczenia zostały złożone. Ustalony pierwotnie termin złożenia oświadczeń miał charakter instrukcyjny, porządkujący tryb i czas zbierania oświadczeń, natomiast termin ten nie był obciążony żadnym rygorem prawnym, w szczególności takim, który dyskwalifikowałby skuteczność, ważność i legalność złożonych po terminie oświadczeń o zapoznaniu się z ww. dokumentem.*

NIK nie kwestionuje faktu, że termin określony w dokumencie wewnętrznym był terminem instrukcyjnym. Jednakże, z uwagi na charakter oświadczeń, które potwierdzały zapoznanie się z przyjętą w Urzędzie polityką ochrony danych, dla właściwego postępowania z danymi osobowymi, wewnętrznie określony termin winien być przestrzegany.

(akta kontroli str. 1608-1614)

Ocena cząstkowa

Urząd zrealizował zadania związane z przygotowaniem się do wdrożenia rozporządzenia RODO. Opracowano dokumentację ochrony danych osobowych

Mazowieckiego Urzędu Wojewódzkiego w Warszawie. Prawidłowo wyznaczono IOD. Pracownicy Urzędu zostali przeszkoleni w zakresie dotyczącym RODO.

OBSZAR

2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych

Opis stanu faktycznego

2.1. Prowadzenie rejestrów wymaganych przepisami RODO.

Prowadzone w Urzędzie *Rejestr czynności przetwarzania danych osobowych* oraz *Rejestr kategorii czynności przetwarzania*⁶, zawierały wszystkie wymagane informacje, wymienione w art. 30 ust. 1 RODO. Rejestry określały kategorie danych wyłącznie w zakresie niezbędnym dla celów ich przetwarzania i były na bieżąco aktualizowane przez IOD.

Zgodne z art. 5 ust. 1 pkt c) RODO w prowadzonych rejestrach, nie zawierano danych zbędnych lub niewspółmiernych do danej kategorii czynności przetwarzania. Zbierane dane były adekwatne, stosowne oraz ograniczone do tego, co było niezbędne do celów, w których były przetwarzane.

(akta kontroli str. 34,273-299, 2306-2308)

2.2. Upoważnienia do przetwarzania danych

W Urzędzie prowadzono ewidencję wszystkich pracowników upoważnionych do przetwarzania danych osobowych⁷. W ewidencji wskazano imię i nazwisko pracownika, komórkę organizacyjną podstawę zatrudnienia, zakres przetwarzania danych osobowych, datę udzielenia upoważnienia przez Administratora Danych Osobowych (dalej: ADO), datę otrzymania upoważnienia, datę ustania upoważnienia, określenie ADO, wskazanie systemów informatycznych, do których upoważniony ma dostęp oraz znak sprawy.

Na podstawie badania ewidencji wydanych upoważnień stwierdzono, że wszyscy pracownicy badanych dwóch komórek organizacyjnych⁸, przetwarzający dane osobowe, zostali upoważnieni do przetwarzania danych osobowych.

(akta kontroli str. 1615-1619,1625,2225, 2071-2091)

Badanie wybranych losowo 40 teczek z dokumentacją osobową pracowników Wydziału Zdrowia oraz Biura Kadr i Obsługi Prawnej, pod kątem prawidłowości posiadanych upoważnień do przetwarzania danych osobowych wykazało, że 37 spośród 40 pracowników posiadało upoważnienia do przetwarzania danych osobowych, zgodne z zakresem obowiązków znajdującym się w poszczególnych teczkach poddanych kontroli. W upoważnieniach m.in. wskazano podstawę prawną imię i nazwisko osoby upoważnionej, jej stanowisko, jednostkę organizacyjną. Dokument ten upoważniał do przetwarzania danych osobowych stosownie do powierzonych obowiązków służbowych, odpowiedzialności oraz poleceń wynikających z zakresu czynności na zajmowanym stanowisku. Na upoważnieniu widniał podpis pracownika i data przyjęcia upoważnienia oraz zobowiązanie

⁶ Oba rejestry funkcjonowały w Urzędzie zgodnie z art. 30 ust.1 i 2 RODO. Procedowanie w sprawie powstania obu rejestrów rozpoczęło w Urzędzie przed wejściem w życie przepisów RODO. Rejestr czynności przetwarzania danych osobowych był prowadzony od 13.04.2018 r., a podstawą jego prowadzenia były przepisy prawa oraz pismo Inspektora Ochrony Danych z 10.04.2018 r. nr BO-1.132.589.2018 w sprawie prowadzenia Rejestru Czynności, skierowane do dyrektorów wszystkich komórek organizacyjnych w Urzędzie. Oba Rejestry prowadzone były w formie plików Excel.

⁷ Ewidencję osób upoważnionych do przetwarzania danych osobowych w Urzędzie prowadził kierujący komórką organizacyjną do spraw ochrony danych osobowych i informacji niejawnych w MUW, ewidencja prowadzona była w systemie Excel, była na bieżąco aktualizowana. System umożliwiał filtrowanie w każdej z kategorii, w tym również informacji o pracownikach z danej komórki organizacyjnej pod kątem posiadanych upoważnień. Próba objęła dwa spośród Wydziałów Urzędu: Biuro Kadr i obsługi Prawnej oraz Wydział Zdrowia.

⁸ Na podstawie badania przeprowadzonego w oparciu o listę wszystkich pracowników zatrudnionych (na dzień przeprowadzenia badania, tj. 17.10.2019 r.) w Wydziale Zdrowia (60 pracowników) oraz Biurze Kadr i Obsługi Prawnej (116 pracowników).

pracownika do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.

W przypadku trzech pracowników kontrola wykazała, że dwóch z nich posiadało upoważnienie do przetwarzania danych osobowych nieadekwatne do zajmowanego stanowiska i zakresu przetwarzanych danych osobowych, zaś w przypadku jednej osoby upoważnienie wydano po dwóch miesiącach od zatrudnienia pracownika w urzędzie. Było to niezgodne z wymogami określonymi w art. 29 oraz art. 32 ust. 4 RODO (szczegółowy opis w punkcie *stwierdzone nieprawidłowości*).

(akta kontroli str. 1622-1626, 2225, 2251-2261, 2234-2250, 2262-2268)

Na podstawie losowo wybranych 10 umów zlecenia dotyczących osób zatrudnionych przez Urząd, przeprowadzono kontrolę upoważnień do przetwarzania danych osobowych przez te osoby. Ustalono, że zgodnie z art. 29 oraz 32 ust. 4 RODO, wszystkie osoby zatrudnione na podstawie umów poddanych badaniu, przetwarzały dane osobowe wyłącznie na polecenie Administratora⁹.

(akta kontroli str. 1803-1876, 2282-2283)

W okresie objętym kontrolą rozwiązano stosunek pracy łącznie z 416 pracownikami Urzędu, w tym z 14 pracownikami Wydziału Zdrowia oraz 39 pracownikami Biura Kadr i Obsługi Prawnej¹⁰. Kontrola 15 losowo wybranych kont dostępu do systemów teleinformatycznych wszystkich pracowników Urzędu, z którymi rozwiązano stosunek pracy lub którzy zmienili miejsce pracy w ramach Urzędu wykazała, że w/w osobom najpóźniej w dniu rozwiązania umowy o pracę, odebrano uprawnienia do dostępu do systemów informatycznych Urzędu lub danej komórki w strukturze Urzędu, zawierających dane osobowe¹¹.

(akta kontroli str. 2276-2277)

W okresie objętym kontrolą Wojewoda Mazowiecki, jako administrator danych osobowych powierzył, na podstawie 118 umów i porozumień przetwarzanie danych osobowych innym podmiotom.

(akta kontroli str. 2286-2295)

Analiza pięciu losowo wybranych umów powierzenia przetwarzania danych osobowych zawartych z podmiotami zewnętrznymi wykazała, że zgodnie z art. 28 ust. 3 RODO w ww. umowach określono ich przedmiot, czas trwania, charakter i cel przetwarzania danych, rodzaj danych osobowych oraz kategorie osób, których dotyczą jak również obowiązki i prawa administratora. Zbadane umowy były ujęte w *Rejestrze umów powierzenia przetwarzania danych osobowych*¹².

(akta kontroli str. 1877-1954, 2284)

W okresie objętym kontrolą Urząd nie przeprowadzał kontroli sposobu wykonania umów powierzenia przez podmiot przetwarzający dane osobowe. Jak wyjaśnił Wojewoda Mazowiecki, administrator przygotowuje się do przeprowadzenia kontroli w tym zakresie, czego potwierdzeniem jest m.in. wstępnie opracowany plan audytu. W Urzędzie został także stworzony nowy wzór umowy powierzenia danych (załącznik nr 25 do pisma Wojewody mazowieckiego z 18 września 2019 r.), gdzie w § 4 określono prawo kontroli danych osobowych przez administratora¹³.

⁹ Na podstawie odpowiednich upoważnień lub umów.

¹⁰ Wg danych na dzień 19.09.2019 r.

¹¹ Ustalono w dniu 09.10.2019 r. na podstawie oględzin systemów informatycznych.

¹² Umowa z 8 grudnia 2018 r. podpisana z przedsiębiorstwem OPTeam S.A. dotycząca rozbudowy elektronicznego systemu kluczy Optipass Portiernia wraz z oprogramowaniem, umowa z 22 sierpnia 2018 r. zawarta z Powiatem Otwockim w związku z wykonywaniem postanowień Porozumienia z 27 stycznia 2009 r. dot. utworzenia Terenowego Punktu Paszportowego w związku z przekazaniem Zarządowi Powiatu spraw z zakresu działania Wojewody, umowa z 3 grudnia 2018 r. zawarta z firmą ArchiDoc SA dot. usługi polegającej na uporządkowaniu i przygotowaniu do przekazania do Archiwum Zakładowego Mazowieckiego Urzędu Wojewódzkiego w Warszawie dokumentacji kat. A, umowa zawarta 31 lipca 2018 r. z Panem H.H.w związku z pełnieniem funkcji Inspektora Danych przy Wojewódzkim Zespole ds. Orzekania o Niepełnosprawności w Warszawie, umowa z 31 stycznia 2019 r. podpisana z firmą EMIKS INFO-ARCH dotycząca świadczenia usług opieki serwisowej oprogramowania.

¹³ Administrator lub upoważniony przez niego audytor zewnętrzny ma prawo do przeprowadzenia kontroli przestrzegania przez podmiot

Wojewoda Mazowiecki wyjaśnił ponadto, że pomimo braku kontroli przeprowadzonych w powyższym zakresie przez administratora danych w rozumieniu art. 28 RODO, istnieją sytuacje w ramach których kierujący komórkami organizacyjnymi po zakończeniu trwania umowy, odbierając jej przedmiot, stwierdzają prawidłowość w zakresie przetwarzania danych osobowych (np. umowa nr 146/2017/BA z 19 czerwca 2017 r. na dezynfekcję gazową mat. archiwalnych - przekazywanie dokumentów zawierających dane osobowe odbywa się na podstawie protokołów zdawczo-odbiorczych przygotowywanych i podpisywanych przez pracowników Biura Kadr i Obsługi Prawnej lub umowa 42/2018/BOU na niszczenie zbędnej dokumentacji oraz umowa powierzenia przetwarzania danych osobowych i certyfikaty zniszczenia dokumentacji). Innym przykładem wskazanym przez Wojewodę jest obsługa kontrahentów zewnętrznych, którzy otrzymują zdalny dostęp do systemów przez nich serwisowanych z wykorzystaniem połączenia VPN realizowanego przez urządzenia klasy UTM, a każdy z pracowników otrzymuje imienne konto z tylko sobie znanym hasłem (zmieniane po pierwszym logowaniu). Kontrahenci w ramach realizowanych umów uzyskują również dostęp zdalny do systemów, które serwisują w trybie nadzorowanym, a na serwerze lub komputerze administratora systemu (pracownika MUW) uruchamiana jest aplikacja dostępowa i zestawiane połączenie z serwisantem, który wykonuje prace serwisowe pod stałym nadzorem administratora systemu. Konta dostępne dla firm zewnętrznych są wyłączane po przekazaniu informacji o nieprzedłużeniu umowy serwisowej.

(akta kontroli str. 664-665, 1877-1954, 2284)

W okresie objętym kontrolą Wojewoda Mazowiecki wykonywał zadania podmiotu przetwarzającego. Zgodnie z art. 28 ust. 3 RODO przetwarzanie odbywało się na podstawie porozumień i umów powierzenia przetwarzania danych osobowych¹⁴. Analiza postanowień wszystkich obowiązujących porozumień i umów powierzenia wykazała, że w Urzędzie wywiązano się z obowiązków nałożonych na podmiot przetwarzający.

(akta kontroli str. 2190-2233)

2.3. Monitoring wizyjny

Monitoring wizyjny Urzędu został opisany w zarządzeniu nr 37 Dyrektora Generalnego Mazowieckiego Urzędu Wojewódzkiego w Warszawie z dnia 25 października 2018 r. w sprawie ustalenia regulaminu pracy w MUW, w rozdziale 13 pn. „Monitoring obiektu”. Dostęp do systemu monitoringu wizyjnego, poza administratorem obiektu, którym jest Biuro Obsługi Urzędu, posiada jedynie firma wykonująca usługi stałej ochrony osób i mienia w obiektach MUW, zgodnie z umową nr 46/2019/BOU z dnia 31 stycznia 2019 r. oraz powiązaną umową powierzenia przetwarzania danych zawartą również 31 stycznia 2019 r. Wykonawca usługi ochrony korzysta z urządzeń monitoringu, jako systemu wspomagającego obserwację ochranianego obiektu w celu realizacji umowy oraz wykonania opisanych w umowie prac technicznych (konserwacja, serwisowanie). Teren monitorowany został oznaczony w sposób widoczny i czytelny. Monitoringiem wizyjnym objęto ciągi korytarzowe, wejścia do Urzędu, wjazdy, dziedzińce oraz miejsce ewakuacji Urzędu. W miejscach ogólnodostępnych, tj. na zewnątrz budynku oraz na jego terenie, w szczególności przy wejściach do budynku, umieszczone były piktogramy (rysunki

przetwarzający zasad przetwarzania danych osobowych, o których mowa w umowie powierzenia oraz w obowiązujących przepisach prawa, w szczególności poprzez żądanie udzielenia wszelkich informacji dotyczących przetwarzania przez podmiot przetwarzający powierzonych danych osobowych, stosowanych środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z prawem lub dokonywania kontroli w miejscach, w których są przetwarzane powierzone dane osobowe.

¹⁵ Umowy dot. wdrożenia i utrzymania oraz rozwoju systemu elektronicznego EKD, porozumienie w sprawie określenia warunków realizacji przez Wojewodę Mazowieckiego zadań w zakresie desygncji w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020, umowa dot. prowadzenia ewidencji gruntów i budynków dla powiatu płońskiego, umowa dotycząca korzystania przez pracowników Urzędu z usług sportowo-rekreacyjnych na podstawie indywidualnych kart w ramach programu Multisport oraz związana z nią umowa powierzenia przetwarzania danych z 05.10.2018 r.

kamery) z napisem „obiekt monitorowany”, a także klauzule informacyjne. Stosownie do art. 22² § 2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy¹⁶, monitoring nie obejmował pomieszczeń sanitarnych, szatni, czy innych obiektów socjalnych.

(akta kontroli str. 530-538,555-560)

2.4. Ochrona systemów informatycznych

Przyjęte w Urzędzie rozwiązania dotyczące zabezpieczeń przetwarzanych danych osobowych oraz minimalizujące ryzyko przed nieuprawnionym uzyskaniem danych osobowych, ich kradzieżą lub utratą opisano m. in. w *Polityce Ochrony danych osobowych Mazowieckiego Urzędu Wojewódzkiego w Warszawie, Instrukcji zarządzania systemem informatycznym w Mazowieckim Urzędzie Wojewódzkim w Warszawie*. W ramach systemu zabezpieczeń danych osobowych w Urzędzie stosowano następujące formy ochrony danych: ochronę fizyczną¹⁷, ochronę techniczną budynku, m. in. system wydawania kluczy oraz dodatkowe wewnętrzne systemy kontroli wejścia do serwerowni i centrali telefonicznej, systemy przeciwpożarowe, systemy sygnalizacji włamania i napadu.

W strefie bezpieczeństwa serwerowni głównej w Urzędzie, stosowane były instalacje alarmowe przeciwwłamaniowe, autoryzacja wejść przy pomocy kart inteligentnych, haseł dostępu oraz dozór fizyczny¹⁸.

Zarówno w serwerowni głównej jak i zapasowej zastosowano również systemy klimatyzacji (klimatyzację precyzyjną w serwerowni głównej, klimatyzatory ściennie w serwerowni zapasowej)¹⁹.

(akta kontroli str. 1975-1976,2272-2275,2279-2280)

Podstawowym sposobem²⁰ zabezpieczenia danych i dostępu do nich w trybie Online był system definiowania użytkowników, grup użytkowników oraz haseł poprzez zabezpieczenia programowe wmontowane w system zarządzania siecią oraz w eksploatowane systemy użytkowe uniemożliwiające dostęp do systemu osobom nieupoważnionym.

Badanie stosowania przez pracowników Urzędu przyjętych rozwiązań minimalizujących ryzyko przed nieuprawnionym uzyskaniem danych osobowych, ich kradzieżą lub utratą, przeprowadzono na próbie 10 stanowisk komputerowych²¹. Każdy z użytkowników stanowiska posiadał indywidualne hasło zgodnie z *Instrukcją zarządzania systemem informatycznym w Mazowieckim Urzędzie Wojewódzkim w Warszawie*, przy użyciu którego rozpoczynał pracę w systemie. Praca

¹⁶ Dz.U. z 2019 r. poz. 1040. ze zm.

¹⁷ Kontrola wejść, kontrola osób wchodzących poprzez okazanie identyfikatora, wykonawców i usługodawców.

¹⁸ M. in. w serwerowni głównej zastosowano system monitoringu z zastosowaniem kamer przemysłowych, bezpieczny system przeciwpożarowy (z czynnikiem niepowodującym uszkodzeń sprzętu elektronicznego) oraz wzmocnione drzwi przeciwpożarowe.

¹⁹ Kopie zapasowe były tworzone w Urzędzie według potrzeb określonych przez przełożonych w formie kopii dziennych, tygodniowych oraz miesięcznych. Wykonują je użytkownicy na indywidualnych stanowiskach komputerowych, w sieciach wewnętrznych oraz kopie programów i systemów. Elektroniczne nośniki przechowywane były w zamkniętych meblach biurowych, kopie zapasoweienne - na stanowiskach pracy, a tygodniowe i miesięczne, zabezpieczone - w szafach metalowych w pomieszczeniach zapewniających ochronę danych przed nieuprawnionym dostępem.

²⁰ Zgodnie z Instrukcją Zarządzania Systemem Informatycznym.

²¹ W Wydziale Zdrowia oraz Biurze Kadr i Obsługi Prawnej.

wykonywana była przy wykorzystaniu wyłącznie własnego indywidualnego konta w systemach informatycznych. We wszystkich stanowiskach zostało zainstalowanie aktywne oprogramowanie antywirusowe. Korzystanie z poczty odbywało się przy pomocy konta pocztowego przydzielonego Użytkownikowi. Podczas badania przeprowadzonego w obecności kontrolera, wszyscy pracownicy poddani próbie, zablokowali i odblokowali ekrany zgodnie z procedurą. Rozwiązania minimalizujące ryzyko przed nieuprawnionym uzyskaniem danych osobowych, ich kradzieżą lub utratą pracownicy stosowali zgodnie z Instrukcją Zarządzania Systemem Informatycznym.

(akta kontroli str. 2279-2281)

**Stwierdzone
nieprawidłowości**

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

1. Trzech pracowników Urzędu (na 40 skontrolowanych) nie posiadało upoważnienia adekwatnego do zajmowanego stanowiska i zakresu przetwarzanych danych osobowych, tj.:

- w przypadku dwóch osób nie zmieniono posiadanego przez pracowników upoważnień do przetwarzania danych w związku ze zmianą miejsc zatrudnienia pracowników,
- w przypadku jednej osoby - upoważnienie wydano po dwóch miesiącach od zatrudnienia pracownika w urzędzie.

Było to niezgodne art. 29 oraz art. 32 ust. 4 RODO.

Wojewoda Mazowiecki wyjaśnił m.in., że w przypadku nieaktualnego upoważnienia pracownika Wydziału Zdrowia, wykonywał on te same obowiązki, które realizował w Wydziale Kontroli, w którym był wcześniej zatrudniony, tzn. przeprowadzał kontrole w podmiotach leczniczych i posiadał upoważnienie do przetwarzania danych wydane w dniu 11 kwietnia 2014 r. Wydział Zdrowia nie wystąpił do Biura Ochrony o wystawienie nowego upoważnienia do przetwarzania danych osobowych, co wynikało z przeoczenia, uwarunkowanego spiętrzeniem zadań, w związku ze zmianą w strukturze organizacyjnej MUW i zmianą lokalizacji siedziby. W związku z tym w trakcie trwania kontroli NIK sporządzono wnioski o udzielenie upoważnienia do przetwarzania danych osobowych dla ww. pracownika i w dniu 15 października 2019 r. otrzymał on stosowne upoważnienie. W przypadku pracownika, który w terminie od 5 kwietnia do 4 lipca 2018 r. został oddelegowany z Wydziału Zdrowia do Wydziału Spraw Cudzoziemców, nie otrzymał on upoważnienia do przetwarzania danych osobowych, gdyż nie wystąpiono z takim wnioskiem do Biura Ochrony z powodu niedopatrzenia.

Natomiast w przypadku pracownika, któremu upoważnienie wydano z dwu - miesięcznym opóźnieniem, wynikało to głównie ze zbyt późnego złożenia wniosku w tej sprawie przez pracownika odpowiedzialnego za jego złożenie, z powodu spiętrzenia zadań w związku ze zmianą w strukturze organizacyjnej.

(akta kontroli str. 1622-1626, 2225, 2251-2261, 2234-2250, 2262-2268)

Ocena częściowa

Administrator danych osobowych prawidłowo prowadził wymagane na podstawie RODO rejestry, tj. *Rejestr czynności przetwarzania danych osobowych i Rejestr kategorii czynności przetwarzania*. W Urzędzie wdrożono środki techniczne, fizyczne i organizacyjne dla zapewnienia zdolności do szybkiego przywrócenia dostępności danych osobowych oraz do utrzymania poufności, integralności i odporności systemów i usług przetwarzania. Właściwie zorganizowano monitoring wizyjny, a pracownicy oraz petenci posiadali możliwość powzięcia informacji o jego stosowaniu. Wdrożone zabezpieczenia techniczne i organizacyjne wynikały

z obowiązujących procedur bezpieczeństwa. W wyniku kontroli stwierdzono jednak przypadki przetwarzania danych osobowych bez stosownych upoważnień Administratora.

OBSZAR

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

Opis stanu faktycznego

3.1. osobowych

Postępowanie w przypadku naruszenia ochrony danych

Na podstawie prowadzonych w Urzędzie *Rejestrów naruszeń* za 2018 i 2019 r. ustalono, że do dnia 19 września 2019 r. zarejestrowano łącznie siedem przypadków naruszenia ochrony danych osobowych, z tego jeden w 2018 r. i sześć w 2019 r. W przypadku sześciu naruszeń, po przeprowadzeniu oceny skutków naruszenia stwierdzono, że nie było zasadne przesyłanie zawiadomień do Prezesa UODO, a także nie było potrzeby informowania osób, których to dotyczyło. W jednym przypadku (z 2019 r.) dokonano zgłoszenia do Prezesa UODO, zgodnie z terminem określonym w art. 33 ust. 1 RODO (do 72 godzin), wskazując jednocześnie, że nie wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o których mowa w art. 34 ust. 1 RODO. Prawidłowość takiej oceny postępowania została potwierdzona pismem z UODO¹⁵, w którym organ nadzorczy zgodził się z oceną administratora, nie wskazując na konieczność podejmowania dodatkowych działań, bądź przeprowadzania ponownej oceny naruszenia.

(akta kontroli str. 1386-1582,1620-1623)

3.2. Postępowanie z danymi osobowymi

W okresie objętym kontrolą do Urzędu pięciokrotnie zgłoszono żądanie usunięcia danych osobowych. We wszystkich przypadkach usunięto dane, a następnie w terminach określonych w art. 12 ust. 3 RODO, poinformowano o tym wnioskodawcę¹⁶.

(akta kontroli str. 9-11,585-630,1608-1612)

W okresie objętym kontrolą do Urzędu zgłoszono jedno żądanie uaktualnienia danych osobowych. Urząd, w terminie określonym w art. 12 ust. 3 RODO, poinformował wnioskodawcę o podjętych działaniach w tej sprawie, wskazując jednocześnie organ państwowy, który jest właściwy do sprostowania danych objętych żądaniem wnioskodawcy.

(akta kontroli str. 9-10,21-22,631-651)

W wyniku przeprowadzonych oględzin w ogólnodostępnych miejscach znajdujących się w Punkcie Obsługi Klienta, w Wydziale Polityki Społecznej w MUW, w Wydziale Spraw Cudzoziemców w MUW oraz w Wydziale Spraw Obywatelskich w MUW ustalono, że w ww. miejscach nie znajdowały się informacje, które mogły naruszać ochronę danych osobowych osób fizycznych.

(akta kontroli str. 1699-1760)

Zasady niszczenia dokumentów papierowych, a także usuwania informacji znajdujących się na sprzętach i nośnikach zewnętrznych uregulowane były w *Polityce ochrony danych osobowych Mazowieckiego Urzędu Wojewódzkiego w Warszawie*. Wskazano w niej, że do zadań kierującego komórką organizacyjną właściwą do spraw obsługi urzędu należy w szczególności podejmowanie czynności technicznych służących bezpieczeństwu i skutecznej ochronie przetwarzania danych osobowych w MUW, a także wyposażenie pomieszczeń m.in. w niszcarki. Ponadto Urząd zawarł w 2018 r. umowę z firmą zewnętrzną której przedmiotem

¹⁵ Pismo z 24 kwietnia 2019 r.

¹⁶ W jednym przypadku (sprawa Pani M. P.) usunięto dane objęte wnioskiem, jednakże nie doręczono pisma w tej sprawie, z uwagi na nieaktywny już adres email wnioskodawcy.

było niszczenie zbędnej dokumentacji oraz wystawianie z tego tytułu certyfikatów zniszczenia dokumentacji. Z ww. firmą zawarto także umowę powierzenia przetwarzania danych. Kontrola wykazała, że po każdorazowym niszczeniu dokumentacji, firma, zgodnie z umową wystawiała stosowny certyfikat.

(akta kontroli str. 932-977,1056)

3.3. Ochrona danych osobowych pracowników

Na podstawie oględzin 10 teczek akt osobowych pracowników Urzędu ustalono, że pracownicy zostali poinformowani o przetwarzaniu ich danych osobowych¹⁷ potwierdzając podpisem „klauzulę informacyjną dla pracownika Urzędu”¹⁸. Zgodnie ze sposobem prowadzenia dokumentacji pracowniczej określonej w rozporządzeniu Ministra Rodziny, Pracy i Polityki Społecznej z 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej¹⁹, klauzule informacyjne zostały wymienione w wykazie dokumentów zamieszczonych w aktach.

(akta kontroli str. 738-742)

Badanie dochowania przez Urząd obowiązku informacyjnego żart. 13RODO w przypadku zawierania umów zleceń, przeprowadzone na próbie 10 takich umów²⁰, wykazało, że zleceniobiorcy zostali poinformowani o przetwarzaniu ich danych osobowych²¹. Informacje przekazane przez Urząd zleceniobiorcom zawierały wszystkie dane wskazane w art. 13 ust. 1 i ust. 2 RODO.

(akta kontroli str.2282)

W okresie objętym kontrolą podczas rekrutacji pracowników, w ogłoszeniach Wojewody Mazowieckiego o naborach na wolne stanowiska urzędnicze, informowano kandydatów o warunkach przetwarzania ich danych osobowych²². W ogłoszeniach o naborze zawarto informacje o przetwarzaniu danych osobowych, o celu oraz sposobie przetwarzania tych danych. Jako dopuszczalny termin przechowywania informacji o kandydatach w Urzędzie przyjęto okres do trzech miesięcy od zakończenia procesu rekrutacji. Przyjęty termin był zgodny z rozporządzeniem Prezesa Rady Ministrów z 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych²³.

Oferty kandydatów, którzy nie zostali wyłonieni w drodze naboru przechowywane były w Biurze Kadr i Obsługi Prawnej w Oddziale Zarządzania Kadrami w opisanych teczkach w szafie zamykanej na klucz przez okres trzech miesięcy od daty zatrudnienia, a następnie były komisyjnie niszczone (zgodnie z § 19 ust. 2 Regulaminu naboru kandydatów na wolne stanowiska pracy niebędące wyższymi stanowiskami w służbie cywilnej oraz regulaminu naboru kandydatów na wolne stanowiska pracy niebędące stanowiskami w służbie cywilnej w Mazowieckim Urzędzie Wojewódzkim w Warszawie wprowadzonym Zarządzeniem nr 33 Dyrektora Generalnego Mazowieckiego Urzędu Wojewódzkiego w Warszawie z dnia 24 września 2018 r.). Oferta kandydata, który został wyłoniony w drodze naboru,

¹⁷ Oględziny przeprowadzono przez kontrolera 17.10.2019 r., do próby wybrano losowo 5 teczek osobowych z dokumentacją pracowników Wydziału Zdrowia oraz 5 teczek pracowników Biura Kadr i Obsługi Prawnej.

¹⁸ W klauzuli wskazano m.in. administratora - jego tożsamość, IOD - jego dane kontaktowe, cel przetwarzania danych i podstawę prawną przetwarzania, informacje o odbiorcach danych osobowych, informację o okresie przechowywania danych, informację o prawie do żądania dostępu do danych osobowych, prawie do ich sprostowania, usunięcia, ograniczenia przetwarzania, prawie do wniesienia sprzeciwu wobec przetwarzania, informację o prawie wniesienia skargi do organu nadzorczego.

¹⁹ Dz. U. poz. 2369.

²⁰ Zawartych od 25.05.2018 r.

²¹ We wszystkich 10 przypadkach zleceniobiorców poinformowano o przetwarzaniu ich danych osobowych w załączniku do umowy zlecenia.

²² Ustalono na podstawie badania 10 ogłoszeń Wojewody Mazowieckiego o naborach na wolne stanowiska urzędnicze opublikowane od dnia 25.05.2018 r.

²³ Dz.U. 2011 Nr 14 poz. 67.

była przekazywana do Oddziału Spraw Pracowniczych w Biurze Kadr i Obsługi Prawnej.

(akta kontroli str. 1622-1627, 2136-2187)

Stwierdzone
nieprawidłowości

OCENA CZĄSTKOWA

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

W Urzędzie prawidłowo zarządzano danymi osobowymi przetwarzanymi w jednostce. W przypadku stwierdzenia naruszenia ochrony danych osobowych terminowo przekazywano je Prezesowi UODO. Pracownicy oraz kandydaci na stanowiska urzędnicze byli informowani, zgodnie z przepisami RODO, o przetwarzaniu ich danych oraz o przyjętych rozwiązaniach dotyczących ochrony danych osobowych. W Urzędzie uregulowano i przestrzegano procedur niszczenia dokumentów i nośników zawierających dane osobowe.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny wynikające z ustaleń kontroli, Najwyższa Izba Kontroli odstępuje od formułowania wniosków pokontrolnych, z uwagi na fakt, iż stwierdzone nieprawidłowości miały charakter incydentalny lub zostały usunięte w trakcie kontroli.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia
zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Departamentu Administracji Publicznej Najwyższej Izby Kontroli. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61 b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Warszawa, dnia 41 grudnia 2019 r.

Kontrolerzy:
Paweł Łukasiewicz
Doradca ekonomiczny

Najwyższa Izba Kontroli
Departament Administracji Publicznej
Dyrektor
Bogdan Skwarka

i Q e^A JL

podpis
Dorota Paszkiewicz

B. Skwarka (A)
podpis

Główny specjalista kontroli państwowej

Dorota Paszkiewicz
podpis