NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.018.01.2019

Pan
Tobiasz Bocheński
Wojewoda Łódzki
Łódzki Urząd Wojewódzki w Łodzi,
ul. Piotrkowska 104, 90-926 Łódź

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi
ul. Kilińskiego 210, 90-980 Łódź
T +48 42 239 32 00, F +48 42 239 32 90
llo@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Łódzki Urząd Wojewódzki w Łodzi[1], ul. Piotrkowska 104, 90-926 Łódź
Kierownik jednostki kontrolowanej	Tobiasz Bocheński, Wojewoda Łódzki, od 25 listopada 2019 r. Karol Młynarczyk, I Wicewojewoda, od 12 listopada 2019 r. do 24 listopada 2019 r. Zbigniew Rau, Wojewoda Łódzki[2], od 9 grudnia 2015 r. do 11 listopada 2019 r.
Zakres przedmiotowy kontroli	1. Organizacja ochrony danych osobowych w jednostce. 2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych. 3. Zarządzanie danymi osobowymi przetwarzanymi, w tym gromadzonymi, w jednostce.
Okres objęty kontrolą	Od 25 maja 2018 r. do 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[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Łodzi
Kontroler	Magdalena Łysek, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LLO/173/2019 z 2 września 2019 r.

(akta kontroli str.1-2, 836)

[1] Dalej ŁUW lub Urząd.
[2] Dalej także Wojewoda.
[3] Dz. U. z 2019 r. poz. 489 ze zm., dalej ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

W ŁUW prawidłowo przygotowano się 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)[5] – dalej RODO. Ochrona danych osobowych, z wyjątkiem niewielkich odstępstw, prowadzona była zgodnie z wytycznymi określonymi w RODO i uregulowaniach wewnętrznych.

Uzasadnienie oceny ogólnej

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 i zapoznani ze zaktualizowanymi procedurami w zakresie bezpieczeństwa informacji. Realizując obowiązki określone w RODO, Wojewoda powołał Inspektora Ochrony Danych (IOD) i umożliwił mu realizację zadań w sposób niezależny. Osoba pełniąca tę funkcję posiadała odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. W kontrolowanym okresie IOD wywiązywał się z nałożonych na niego obowiązków, z wyjątkiem aktualizacji *Rejestru kategorii czynności przetwarzania*. W trakcie kontroli rejestr ten został zaktualizowany. Pozostałe rejestry, wymagane na podstawie RODO oraz uregulowań wewnętrznych, prowadzone były prawidłowo.

Wdrożone w ŁUW techniczne, fizyczne i informatyczne środki bezpieczeństwa, służące utrzymaniu poufności, integralności i odporności systemów i usług przetwarzania, były zgodne z regulacjami wewnętrznymi. W wyniku kontroli stwierdzono jednak przypadki niestosowania procedur wewnętrznych w zakresie przerywania pracy w systemach informatycznych oraz przetwarzania przez pracowników ŁUW danych osobowych bez stosownych upoważnień Administratora, co wynikało z opóźnień w ich wydawaniu. W kontrolowanym okresie doszło także do naruszeń ochrony danych osobowych. Stosowne zawiadomienia w tym zakresie, w przypadku wystąpienia przesłanek, przekazano do Prezesa Urzędu Ochrony Danych Osobowych, przy czym jedno (na trzy) po upływie ustalonego w RODO terminu.

Pracodawca, jako Administrator, prawidłowo informował kandydatów do pracy, pracowników, zleceniobiorców i petentów o przetwarzaniu ich danych osobowych.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[6] kontrolowanej działalności

OBSZAR

1. Organizacja ochrony danych osobowych w jednostce

Opis stanu faktycznego

1.1. Przygotowanie dokumentacji wymaganej przepisami RODO

W związku z wejściem w życie przepisów RODO, w ramach działań związanych z wdrożeniem systemu zarządzania bezpieczeństwem informacji, w Urzędzie dokonano szacowania ryzyka utraty bezpieczeństwa informacji, o której mowa w art. 32 RODO. Szacowanie to zostało przeprowadzone przez członków utworzonego w ŁUW *Zespołu do spraw wdrożenia RODO*. Wyniki szacowania

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

[5] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1. Tekst rozporządzenia dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1527242776060&uri=CELEX:32016R0679.

[6] 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.

przedstawiono w raporcie z dnia 10 lipca 2018 r., zawierającym m.in. opis postępowania z ryzykiem oraz zalecenia i wnioski.
We wnioskach wskazano m.in.: konieczność przebudowy sieci elektroenergetycznej oraz prowadzenia polityki informacyjnej, dotyczącej prawidłowego sposobu używania urządzeń przenośnych.
Zalecone w raporcie działania korygujące zostały wprowadzone poprzez zdublowanie i skonfigurowanie krytycznych elementów systemu, wprowadzenie procedury zapewnienia ciągłości działania ŁUW, a także przeprowadzenie polityki informacyjnej o prawidłowym sposobie używania i zabezpieczania nośników danych i urządzeń przenośnych oraz o zagrożeniach złośliwym oprogramowaniem,

(akta kontroli str. 3-70,77-133)

W ŁUW wprowadzono nową dokumentację dotyczącą ochrony danych osobowych, a także zaktualizowano dotychczasową, dostosowując ją do wymogów RODO:

- zarządzeniem nr 87/2018 Wojewody Łódzkiego z 25 maja 2018 r. wdrożono *Politykę Ochrony Danych Osobowych dla ŁUW* (dalej PODO). W kontrolowanym okresie PODO została poddana przeglądowi i zaktualizowana[7], m.in. poprzez wprowadzenie obowiązku współdziałania IOD z audytorami wewnętrznymi ŁUW w zakresie ochrony danych osobowych oraz obowiązku zgłaszania do IOD zamiaru wprowadzenia nowych rozwiązań lub zmian regulacji wewnętrznych, technologicznych, procesowych, które mogłyby mieć wpływ na przetwarzanie danych osobowych.
- zarządzeniem nr 128/2018 Wojewody Łódzkiego z 26 lipca 2018 r. w sprawie przyjęcia i wdrożenia *Systemu Zarządzania Bezpieczeństwem Informacji dla Łódzkiego Urzędu Wojewódzkiego w Łodzi* dokonano zmian obowiązującej *Polityki Bezpieczeństwa Informacji* (PBI) i *Instrukcji zarządzania systemami informatycznymi* (IZSI).

Ww. dokumentacja po zatwierdzeniu przez Wojewodę została podana do wiadomości pracownikom Urzędu poprzez powszechną informację na stronie intranetowej jednostki oraz przekazanie w poczcie elektronicznej informacji o takich dokumentach.

(akta kontroli str.134-351)

W Urzędzie prowadzono wymagane na podstawie art. 30 ust. 1 i 2 RODO rejestry - *Rejestr czynności przetwarzania danych osobowych* oraz *Rejestr kategorii czynności przetwarzania*, przy czym *Rejestr kategorii czynności przetwarzania* nie został zaktualizowany (opisano w punkcie 3 niniejszego wystąpienia). Ponadto utworzono *Rejestr naruszeń ochrony danych osobowych,* uwzględniający dane określone w art. 33 ust. 5 RODO.

(akta kontroli str. 483-490, 822-835 folder 2 i 3)

1.2. Wyznaczenie i działanie Inspektora Ochrony Danych

Zgodnie z art. 37 ust. 1 lit. a RODO, zarządzeniem z dnia 19 czerwca 2018 r. Wojewoda Łódzki wyznaczył Inspektora Ochrony Danych (IOD) i jego zastępcę.
Ponadto, zarządzeniem z dnia 16 marca 2018 r. Wojewoda powołał *Zespół do spraw wdrożenia RODO*, którego zadaniem było przygotowanie ŁUW do wdrożenia i stosowania RODO. W skład zespołu weszli: IOD, jako przewodniczący, zastępca IOD, administrator systemu informatycznego (ASI), inspektor wojewódzki w Biurze Administracji i Logistyki oraz radca prawny w Wydziale Prawnym, Nadzoru i Kontroli.
Na mocy zarządzenia Wojewody z 10 czerwca 2019 r. rozwiązano *Zespół do spraw wdrożenia RODO* i powołano *Zespół Inspektora Ochrony Danych w ŁUW*, w skład którego weszli Lokalni Inspektorzy Ochrony Danych, umiejscowieni w poszczególnych biurach, wydziałach i zespołach Urzędu. Do kierowania pracami Zespołu został wskazany IOD, a w przypadku jego nieobecności zastępca IOD

[7] Zarządzeniem Wojewody Łódzkiego z dnia 26 czerwca 2019 r. nr 173/2019.

lub inna wyznaczona osoba. Lokalni Inspektorzy Ichrony Danych byli pracownikami poszczególnych komórek organizacyjnych ŁUW. Do ich zadań należało koordynowanie spraw związanych z ochroną danych osobowych w poszczególnych wydziałach, wspieranie IOD w informowaniu pracowników o obowiązkach związanych z ochroną danych osobowych, czy w monitorowaniu przestrzegania przepisów o ochronie danych osobowych.

(dowód: akta kontroli str. 354-363)

IOD i jego zastępca byli etatowymi pracownikami Urzędu. IOD zatrudniony był na samodzielnym stanowisku do spraw funkcjonowania systemów teleinformatycznych i realizacji polityki bezpieczeństwa informacji, a od 20 maja 2019 r. wyłącznie na samodzielnym stanowisku do spraw funkcjonowania systemów teleinformatycznych. Zadania wykonywane w ramach umowy o pracę nie powodowały konfliktu interesów, o których mowa w art. 38 ust. 6 RODO. Zgodnie z art. 38 ust. 3 RODO, IOD podlegał bezpośrednio najwyższemu kierownictwu Administratora danych osobowych (ADO), tj. Wojewodzie.

(akta kontroli str. 368-376)

Zgodnie z art. 37 ust. 7 RODO w ogólnodostępnych informacjach – m.in. na stronie internetowej Urzędu oraz na tablicach informacyjnych, podany był aktualny kontakt do IOD i zastępcy IOD.

(dowód: akta kontroli str. 352-353, 769)

IOD posiadał niezbędne kwalifikacje, o których mowa w art. 37 ust. 5 RODO, poparte wykształceniem, wieloletnią praktyką zawodową, szkoleniami i kursami obejmującymi problematykę RODO. Poprzednio pełnił w Urzędzie funkcję Administratora Bezpieczeństwa Informacji.

(dowód: akta kontroli str. 364, 377-389)

O wyznaczeniu IOD i jego zastępcy terminowo poinformowano Prezesa Urzędu Ochrony Danych Osobowych. W okresie objętym kontrolą nie było zmian na stanowiskach IOD i jego zastępcy.

(dowód: akta kontroli str. 365-367, 390-393)

IOD realizował zadania określone w art. 39 RODO. W celu zwiększenia świadomości nt. ochrony danych osobowych m.in. szkolił pracowników Urzędu i prowadził instruktaże. W zakresie monitorowania przestrzegania RODO, innych przepisów prawa o ochronie danych osobowych oraz PODO prowadził audyty danych osobowych i wydawał stosowne zalecenia oraz nadzorował aktualizację PODO. Informował także ADO oraz pracowników o obowiązkach, jakie w zakresie ochrony danych nakładają na nich przepisy prawa oraz polityki wewnętrzne, a także doradzał w sprawie ich stosowania. Pełnił również funkcję punktu kontaktowego dla organu nadzorczego oraz osób, których dane były przetwarzane.

(dowód: akta kontroli str. 66-78, 394-401, 491-495, 822-835 folder 1)

1.3. Inne działania jednostki związane z wdrażaniem RODO

Zgodnie z art. 13 ust. 1 i 2 RODO, ADO informował petentów o przetwarzaniu ich danych osobowych. Stosowne powiadomienia w tym zakresie zawarte były m.in. na tablicy informacyjnej Urzędu, w Kancelarii Urzędu oraz w Biuletynie Informacji Publicznej, a także w stopkach pism oraz e-maili.

(dowód: akta kontroli str. 352-353, 769)

Od 14 listopada 2018 r. do 28 lutego 2019 r. w Urzędzie przeprowadzono audyt wewnętrzny dotyczący *Oceny wdrażania w Łódzkim Urzędzie Wojewódzkim w Łodzi polityki bezpieczeństwa informacji w związku z nowymi regulacjami prawnymi*. Audyt ten obejmował okres od 25 maja 2018 r. do 11 stycznia 2019 r. Celami zadania zapewniającego było dostarczenie kierownictwu obiektywnej oceny w zakresie przeciwdziałania w ŁUW stwierdzonym incydentom w zakresie bezpieczeństwa informacji oraz dostarczenie racjonalnego zapewnienia o skuteczności, efektywności

oraz adekwatności funkcjonowania systemu kontroli zarządczej w audytowanym obszarze. Audytorzy sformułowali zalecenia dotyczące m.in.:

- aktualizacji PBI poprzez dodanie zapisu o konieczności bezwzględnego informowania Dyrektora Biura sprawującego nadzór nad *Oddziałem informatyzacji i monitoringu* o rozwiązaniu z pracownikiem umowy o pracę,
- aktualizacji PODO oraz PBI w zakresie konieczności okresowego dostarczania przez *Oddział ds. kadr* informacji o osobach, które zakończyły pracę,
- aktualizacji PODO, PBI i IZSI w zakresie ustalenia odpowiedzialności za aktualizowanie przedmiotowych polityk.

W wyniku przeprowadzonych czynności sprawdzających w dniu 23 maja 2019 r. oraz 17-23 września 2019 r. audytorzy odnotowali, że wnioski dotyczące aktualizacji *PBI i IZSI* nie zostały wprowadzone. Według wyjaśnień ASI, który był odpowiedzialny za ich realizację, opóźnienia wynikały z nadmiaru obowiązków. Do dnia zakończenia niniejszej kontroli NIK wszystkie zalecenia zostały wdrożone.
W Urzędzie nie były prowadzone inne kontrole i audyty zewnętrzne dotyczące przygotowania do RODO.

(dowód: akta kontroli str. 402-464, 516-517, 520-523)

Szkolenia pracowników ŁUW związane z bezpieczeństwem przetwarzania danych osobowych oraz wejściem nowych przepisów prawa w tym zakresie prowadzone były przez firmy zewnętrzne, IOD, a także przez *Zespół do spraw bezpieczeństwa systemu teleinformatycznego*.
Kontrolę stanu przeszkolenia pracowników przeprowadzono na podstawie próby 338 osób zatrudnionych w dwóch wydziałach[8]. W wyniku badania ustalono, że na dzień 13 września 2019 r. przeszkolono 314 pracowników tych wydziałów, tj. 92,9%. Pozostali nie uczestniczyli w szkoleniu, m.in. z uwagi na nieobecność.

(dowód: akta kontroli str. 491-495, 822-835 folder 5 plik 1, folder 6)

Na przygotowanie i realizację zadań dotyczących ochrony danych osobowych wydatkowano w latach 2017 – 2019 kwotę 96 tys. zł. Środki te zostały wykorzystane na: zakupy informatyczne (37,2 tys. zł), szkolenia pracowników Urzędu (34,1 tys. zł), wydatki osobowe (18 tys. zł)[9], prenumeratę prasy fachowej i dostęp do serwisów tematycznych (4,1 tys. zł) oraz koszty podróży służbowych związanych z RODO i udziału w konferencjach (2,6 tys. zł).

(dowód: akta kontroli str. 465-481)

W kontrolowanym okresie na Urząd nie zostały nałożone żadne kary pieniężne, inne sankcje lub obowiązki, zasadne w przypadku niewłaściwego stosowania przepisów RODO.

(dowód: akta kontroli str. 482)

Stwierdzone nieprawidłowości

W działalności Urzędu w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działania Wojewody w zakresie organizacji bezpieczeństwa informacji.

OBSZAR

2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych

Opis stanu faktycznego

2.1. Prowadzenie rejestrów wymaganych przepisami RODO.
Prowadzony w Urzędzie *Rejestr czynności przetwarzania danych osobowych* zawierał wszystkie wymagane informacje, wymienione w art. 30 ust. 1 RODO.

[8] Wydział Spraw Obywatelskich i Cudzoziemców oraz Wydział Zdrowia, Rodziny i Polityki Społecznej.
[9] Dodatki zadaniowe wyplacane w ramach wynagrodzeń.

Ustalał kategorie danych wyłącznie w zakresie niezbędnym dla celów przetwarzania i był na bieżąco aktualizowany przez IOD.

(dowód: akta kontroli str. 486-490, 822-835 folder 2)

W prowadzonym na podstawie art. 30 ust. 2 RODO *Rejestrze kategorii czynności przetwarzania* ujęto według stanu na dzień 4 września 2019 r. cztery z pięciu kategorii przetwarzania dokonywanych w imieniu innych administratorów (szerzej opisano w sekcji *Stwierdzone nieprawidłowości*).

(dowód: akta kontroli str.486-488, 782-786, 802-804, 822-835 folder 3)

2.2. Upoważnienia do przetwarzania danych

W Urzędzie prowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych. W ewidencji tej ujęto aktualnych pracowników Urzędu oraz stażystów i praktykantów. Kontrola zgodności zakresu upoważnień do przetwarzania danych osobowych wydanych 290 pracownikom[10], z danymi przetwarzanymi przez nich w ramach wykonywanych obowiązków służbowych, w 285 przypadkach nie wykazała rozbieżności. Pozostałych pięciu pracowników przetwarzało dane osobowe bez stosownego upoważnienia (szerzej opisano w sekcji *Stwierdzone nieprawidłowości*).

(dowód: akta kontroli str. 491-501, 822-835 folder 5 plik 2)

W wyniku badania dziewięciu umów zleceń[11] ustalono, że we wszystkich przypadkach ADO udzielił zleceniobiorcy stosownego upoważnienia do przetwarzania danych osobowych.

(dowód: akta kontroli str. 502-513)

Kontrola 10 losowo wybranych kont dostępu do systemów teleinformatycznych byłych pracowników ŁUW wykazała, że wszystkie konta zostały zablokowane w terminach określonych w procedurach wewnętrznych.

W dniu 23 października 2019 r. w ŁUW wprowadzono *Procedurę dodatkowego mechanizmu blokowania dostępu do systemów teleinformatycznych ŁUW*, opracowaną przez *Zespół do spraw bezpieczeństwa systemu teleinformatycznego*. Procedura ta miała na celu zagwarantowanie niezawodności blokowania dostępu do systemów dla: byłych pracowników, pracowników długotrwale nieobecnych, byłych stażystów i praktykantów.

(dowód: akta kontroli str. 514-519, 524-529)

Analiza 10 losowo wybranych umów powierzenia[12] (z 41) zawartych z podmiotami zewnętrznymi wykazała, że:

- w każdym przypadku ADO zawarł z podmiotem przetwarzającym umowę powierzenia przetwarzania danych osobowych, zawierającą wszystkie elementy wymagane na podstawie art. 28 ust. 3 RODO oraz PODO,
- w każdej z umów zawarto zapis, iż ADO jest uprawniony do kontroli sposobu wykonania umowy przez przetwarzającego,
- wszystkie umowy zostały ujęte w *Rejestrze podmiotów przetwarzających*.

(dowód: akta kontroli str. 483-484, 822-835 folder 4 plik 1)

W kontrolowanym okresie nie przeprowadzono żadnej kontroli sposobu wykonania umowy powierzenia przez przetwarzającego dane osobowe. Jak wyjaśnił Wojewoda, kontrola była fakultatywna, na wypadek pojawienia się problemów we współpracy. Niemniej do niektórych podmiotów zewnętrznych, które miały

---

[10] Do kontroli wybrano w sposób celowy wszystkich pracowników *Wydziału Spraw Obywatelskich i Cudzoziemców* oraz *Wydziału Zdrowia, Rodziny i Polityki Społecznej*.

[11] Wszystkie umowy cywilnoprawne obowiązujące na dzień 31 października 2019 r., związane z przetwarzaniem danych osobowych.

[12] Umowy: z 10 listopada 2015 r. w sprawie przeprowadzania badań potrzeb pracowników oraz ewaluacji, z 2 listopada 2018 r. w sprawie asysty technicznej jednego z systemów, z 28 grudnia 2018 r. w sprawie hostingu strony www, z 17 kwietnia i 27 maja 2019 r. dotyczące zapewnienia nadzoru autorskiego nad systemami informatycznymi, z 17 lipca 2018 r. i 26 kwietnia 2019 r. w sprawie ochrony fizycznej budynków, z 1 lipca 2019 r. w sprawie usług serwisowych rejestratora rozmów telefonicznych, z 16 sierpnia 2018 r. i 1 września 2018 r. w sprawie badań okresowych i wstępnych.

dostęp do istotnych danych, przed podpisaniem umowy powierzenia przetwarzania wysyłana była ankieta weryfikująca, czy dany podmiot spełnia wymagania związane z ochroną danych osobowych.

(dowód: akta kontroli str. 782-797)

W kontrolowanym okresie Wojewoda Łódzki wykonywał zadania podmiotu przetwarzającego. Zgodnie z art. 28 ust. 3 RODO przetwarzanie odbywało się na podstawie porozumień i umów powierzenia przetwarzania danych osobowych[13], a także na podstawie ustawy z dnia 13 lipca 2006 r. o dokumentach paszportowych[14]. Analiza postanowień wszystkich obowiązujących porozumień i umów powierzenia (5) wykazała, że w Urzędzie wywiązano się z obowiązków nałożonych na podmiot przetwarzający.

(dowód: akta kontroli str. 782-786, 798-801, 822-835 folder 4 plik 2)

2.3. Monitoring wizyjny

Monitoring wizyjny prowadzony był w Urzędzie na podstawie *Regulaminu funkcjonowania systemu nadzoru telewizyjnego (CCTV) w Łódzkim Urzędzie Wojewódzkim w Łodzi* z dnia 16 grudnia 2016 r. oraz § 11 PBI. Teren monitorowany został oznaczony w sposób widoczny i czytelny. W miejscach ogólnodostępnych umieszczone były piktogramy (rysunek kamery) z napisem „obiekt monitorowany", a także klauzule informacyjne. Stosownie do postanowień zawartych w art. 22^2 ustawy z dnia 26 czerwca 1974 r. - kodeks pracy[15], monitoring nie obejmował pomieszczeń sanitarnych, szatni, czy innych obiektów socjalnych. Dostęp do nagrań z monitoringu miały wyłącznie osoby uprawnione, a nagrania przechowywane były przez okres nieprzekraczający jednego miesiąca.

(dowód: akta kontroli str. 530-538)

2.4. Ochrona systemów informatycznych

W PBI ustalono zasady zapewnienia bezpieczeństwa obejmujące m.in. politykę kluczy, ochronę infrastruktury energetycznej, teleinformatycznej i telekomunikacyjnej, a także zabezpieczenie przewożonych dokumentów paszportowych i kart pobytu cudzoziemców. W celu zwiększenia efektywności ochrony danych osobowych w ŁUW stosowano różnego rodzaju zabezpieczenia lub ich kombinacje, w tym: zabezpieczenia fizyczne, logiczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje.

(dowód: akta kontroli str. 219-264, 539-563.)

W serwerowni i punktach dystrybucyjnych zapewniono podtrzymanie zasilania oraz sprzyjające warunki środowiskowe pracy serwerów i urządzeń sieciowych. Zastosowane rozwiązania zabezpieczające te pomieszczenia minimalizowały ryzyko nieuprawnionego ujawnienienia informacji będących w posiadaniu Urzędu, modyfikacji, usunięcia lub ich zniszczenia. Znajdujące się w serwerowni materiały łatwopalne zostały usunięte z tego pomieszczenia w trakcie kontroli.

(dowód: akta kontroli str. 516-519, 564-566)

Zasady tworzenia i przechowywania kopii bezpieczeństwa danych określono w § 16 IZSI. Kopiami bezpieczeństwa objęte były wszystkie bazy danych przetwarzanych przez serwery Urzędu. W ŁUW ostatnie kopie wykonano i przechowywano zgodnie z tymi procedurami. System realizujący kopie bezpieczeństwa umieszczony był w pomieszczeniu zabezpieczonym przed dostępem osób nieupoważnionych, w innej strefie pożarowej, co minimalizowało ryzyko utraty tych kopii.

(dowód: akta kontroli str.249-264, 567-575)

---

[13] Umowa z 17 lipca 2018 r. dotycząca świadczenie usług ochrony, umowa z 20 lipca 2018 r. dotycząca realizacji staży zawodowych, porozumienie z 3 września 2018 r. dotyczące przetwarzania danych osobowych w ramach zbioru *Centralny system teleinformatyczny wspierający realizację programów operacyjnych*, porozumienie z 9 lipca 2018 r. w sprawie odbywania praktyk wakacyjnych i praktyk zawodowych przez studentów Uniwersytetu Medycznego w Łodzi, umowa z 24 czerwca 2019 r. dotycząca świadczenia usług w ramach Programów FitProfit lub FitSport.

[14] Dz. U. 2018 r., poz. 1919 ze zm.

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

W systemach informatycznych Urzędu, w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem, wprowadzono zabezpieczenia polegające na wdrożeniu nowego urządzenia brzegowego oraz aktualnego programu antywirusowego na każdej stacji roboczej. Urządzenie brzegowe umożliwia monitoring sieci i zdarzeń poprzez system logów, raportów oraz podgląd w czasie rzeczywistym. Mechanizm ten zapewnia bieżącą kontrolę ruchu sieciowego poprzez klasyfikację, blokowanie szkodliwego ruchu i anomalii.
W IZSI ustalono także obowiązek logowania się do systemu poprzez identyfikator i hasło (§ 10 pkt 7) oraz zasadę rozpoczęcia, przerw i zakończenia pracy w systemach informatycznych (§ 14 pkt 2).
W dniu 8 marca 2017 r. Wojewoda Łódzki powołał *Zespół do spraw bezpieczeństwa systemu teleinformatycznego*. Do zadań tego zespołu należał m.in. przeprowadzanie testów bezpieczeństwa.

(dowód: akta kontroli str. 249-264, 540-542, 578-600)

W wyniku kontroli 10 losowo wybranych stanowisk komputerowych pod kątem stosowanych przez użytkowników haseł dostępu oraz procedury zawieszania pracy ustalono, że:

- celem uruchomienia komputerów i kolejnych systemów, wykorzystywanych na danym stanowisku pracy, wszyscy pracownicy wprowadzali hasła spełniające wymogi w zakresie liczby znaków,
- trzech z dziesięciu pracowników potrafiło blokować stację roboczą. Pozostali nie znali kombinacji klawiszy służącej zawieszeniu pracy komputera, wskazanej do stosowania w IZSI (szerzej opisno w sekcji *Stwierdzone nieprawidłowości*).

(dowód: akta kontroli str. 516-519, 576-577)

W IZSI ustanowiono także zasady umożliwiające bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Użytkowany w Urzędzie sprzęt mobilny (m.in. laptopy), służący do przetwarzania informacji wymagających ochrony, był zabezpieczony zgodnie z IZSI.

(dowód: akta kontroli str. 249-264, 601-611)

Stwierdzone nieprawidłowości

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

1. *Rejestr kategorii czynności przetwarzania* prowadzony był nierzetelnie. Według stanu na dzień 4 września 2019 r. nie ujęto w nim jednej pozycji (z pięciu), dotyczącej realizacji programów FitProfit i FitSport, na podstawie umowy z dnia 24 czerwca 2019 r.
Wojewoda Łódzki i IOD wyjaśnili, iż było to spowodowane omyłkowym odznaczeniem pola checkboxa w systemie, w którym prowadzony jest rejestr.
Według stanu na dzień zakończenia kontroli *Rejestr kategorii czynności przetwarzania* został zaktualizowany.

(dowód: akta kontroli str. 486-488, 782-786, 802-804, 822-835 folder 3)

2. Siedmiu na 10 skontrolowanych pracowników (70%) nie potrafiło blokować stacji roboczej, a tym samym nie stosowało procedur przerywania pracy w systemach informatycznych, określonych w § 14 pkt 2 IZSI. Zgodnie z tymi procedurami, odchodząc od stanowiska pracy, pracownik ma obowiązek zablokowania stacji roboczej poprzez kombinację odpowiednich klawiszy.
Dyrektor Generalny ŁUW wyjaśnił m.in., że w celu zminimalizowania ryzyka dostępu do danych osobowych przez osoby nieuprawnione, system teleinformatyczny Urządu został skonfigurowany w taki sposób, aby wymuszał automatyczne blokowanie dostępu do kont użytkowników po 10 minutach nieaktywności. Ponadto wskazał, że pracownicy wychodząc z pokoju są zobowiązani do zamykania drzwi na klucz.

Zdaniem NIK tego rodzaju zabezpieczeń nie można uznać za wystarczające i spełniające wymogi określone w IZSI.

(dowód: akta kontroli str. 516-519, 576-577)

3. Wbrew wymogom określonym w art. 29 oraz art. 32 ust. 4 RODO, pięciu pracowników Urzędu (na 290 skontrolowanych) nie posiadało stosownego upoważnienia do przetwarzania danych wydanego przez ADO. Osoby te były nowymi pracownikami ŁUW, zatrudnionymi między 15 lipca do 11 września 2019 r. w *Wydziale Spraw Obywatelskich i Cudzoziemców* (3) oraz *Wydziale Zdrowia, Rodziny i Polityki Społecznej* (2).
Według stanu na dzień zakończenia niniejszej kontroli NIK ww. pracownicy otrzymali stosowne upoważnienia do przetwarzania danych osobowych.
IOD wyjaśnił m.in., że przyczyną braku wystawienia upoważnienia niezwłocznie mogło być nieprzekazanie z wydziałów odpowiedniego wniosku w EZD.

(dowód: akta kontroli str. 491-501, 822-835 folder 5 plik 2)

OCENA CZĄSTKOWA

Administrator danych osobowych prowadził wymagane na podstawie RODO rejestry, tj. *Rejestr czynności przetwarzania danych osobowych i Rejestr kategorii czynności przetwarzania*, przy czym *Rejestr kategorii czynności przetwarzania* był prowadzony nierzetelnie. W ŁUW techniczne, fizyczne i informatyczne środki bezpieczeństwa, służące utrzymaniu poufności, integralności i odporności systemów i usług przetwarzania, były zgodne z regulacjami wewnętrznymi. W wyniku kontroli stwierdzono jednak przypadki niestosowania procedur wewnętrznych w zakresie przerywania pracy w systemach informatycznych oraz przetwarzania danych osobowych bez stosownych upoważnień Administratora, wskutek opóźnień w ich wydaniu.

OBSZAR

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

Opis stanu faktycznego

3. 1. Postępowanie w przypadku naruszenia ochrony danych osobowych
W okresie objętym kontrolą w Urzędzie pięciokrotnie odnotowano naruszenie ochrony danych osobowych. W przypadku dwóch naruszeń, po przeprowadzeniu oceny skutków naruszenia, nie było zasadne przesyłanie zawiadomień do Prezesa Urzędu Ochrony Danych Osobowych (UODO). Pozostałe trzy przypadki naruszenia[16] zostały zgłoszone do Prezesa UODO. Dwa z nich przesłano w terminie określonym w art. 33 ust. 1 RODO (do 72 godzin), jedno - ósmego dnia od momentu stwierdzenia naruszenia (szerzej opisano w sekcji *Stwierdzone nieprawidłowości*).
Każdorazowo o naruszeniu zawiadomiono osoby, których dane dotyczyły. Zawiadomienia spełniały wymogi określone w art. 34 ust. 2 RODO.

(dowód: akta kontroli str. 612-753)

3.2. Postępowanie z danymi osobowymi
W okresie objętym kontrolą do Urzędu wpłynęły dwa wnioski dotyczące usunięcia i sprostowania danych osobowych. W pierwszym przypadku, zgodnie z żądaniem skutecznie usunięto dane, a następnie bezzwłocznie poinformowano o tym wnioskodawcę. Drugi wniosek, dotyczący sprostowania danych, został wycofany przed podjęciem czynności w tym zakresie.

(dowód: akta kontroli str. 772-781)

W ogólnodostępnych miejscach w budynku Urzędu nie znajdowały się informacje, które mogły naruszać ochronę danych osobowych osób fizycznych.

(dowód: akta kontroli str.754-771)

[16] Naruszenia dotyczyły wysłania e-maila na temat organizacji spotkania informacyjnego dla organizacji pozarządowych bez opcji *do ukrytej wiadomości*, przekazania klientowi składającemu wniosek paszportowy potwierdzenia złożenia wniosku o paszport innej osoby, wysłania korespondencji omyłkowo do osoby o tym samym imieniu i nazwisku, jednak zamieszkałej pod innym adresem.

Administrator uregulował zasady niszczenia dokumentów papierowych, a także usuwania informacji znajdujących się na sprzętach i nośnikach zewnętrznych. W IZSI wskazano m.in., że niepotrzebne wydruki zawierające dane chronione należy niszczyć wyłącznie przy pomocy niszczarek (§ 17 pkt 4). Uszkodzone lub wymontowane z likwidowanego sprzętu dyski twarde i inne równoważne nośniki danych są niszczone mechanicznie, we właściwym oddziale ds. informatyzacji (§ 5 pkt 8).

Analiza 10 (ze 116) protokołów fizycznej likwidacji dysku twardego oraz protokołu likwidacji trzech elektronicznych nośników danych wykazała, że we wszystkich przypadkach likwidacji dokonano zgodnie z wewnętrznymi procedurami.

(dowód: akta kontroli str. 249-264, 805-806)

3.3. Ochrona danych osobowych pracowników

Po wejściu w życie RODO pracodawca, jako Administrator danych osobowych, powiadomił wszystkich pracowników Urzędu o przetwarzaniu ich danych osobowych. Informacje w tym zakresie, zawierające elementy wymagane na podstawie art. 13 ust. 1 i 2 RODO, zostały zamieszczone w intranecie, na stronie BIP Urzędu oraz w miejscach ogólnodostępnych.

(dowód: akta kontroli str. 352-353, 771, 822-835 folder 1)

Badanie 10 umów cywilnoprawnych wykazało, że w ośmiu przypadkach do umowy dołączono klauzulę informacyjną zawierającą elementy wskazane w art. 13 ust. 1 i 2 RODO. W dwóch pozostałych przypadkach dopełniono obowiązku informacyjnego poprzez zamieszczenie stosownych klauzul w miejscu kontaktu z podmiotem podpisującym umowę.

Na podstawie analizy wszystkich 19 udostępnionych na stronie internetowej BIP ŁUW na dzień 29 października 2019 r., informacji o naborze na wolne stanowiska stwierdzono, że we wszystkich przypadkach zamieszczono wymaganą klauzulę informacyjną.

(dowód: akta kontroli str. 807-813)

Oferty kandydatów były przechowywane przez okres sześciu miesięcy od zakończenia procesu rekrutacji, zgodnie z zarządzeniem nr 25/2017 Dyrektora Generalnego ŁUW z dnia 29 września 2017 r. w sprawie naborów na wolne stanowiska do korpusu służby cywilnej w ŁUW. Okres przechowywania ofert uzasadniony był czasem niezbędnym do przeprowadzenia naboru na stanowisko pracy w służbie cywilnej (z uwzględnieniem 3 miesięcy, w których Dyrektor Generalny ŁUW miał możliwość wyboru kolejnego kandydata, w przypadku, gdy ponownie zaistnieje konieczność obsadzenia tego samego stanowiska). Natomiast akta dotyczące naboru były przechowywane przez okres 5 lat, co było zgodne z *Rejestrem czynności przetwarzania danych osobowych* i wynikało z oznaczenia kategorii archiwalnej (B5 dla konkursów na stanowiska w urzędach).

(dowód: akta kontroli str. 814-821, 822-835 folder 2)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Jedno z trzech zgłoszeń naruszenia ochrony danych osobowych przesłano do Prezesa UODO z przekroczeniem terminu określonego w art. 33 ust. 1 RODO (do 72 godzin). Sytuacja ta dotyczyła naruszenia stwierdzonego 25 lutego 2019 r. o godzinie 14:20, zgłoszonego do Prezesa UODO 5 marca 2019 r. o godzinie 10:18. IOD wyjaśnił, iż opóźnienie to było wynikiem błędu w EZD i natychmiast po jego naprawieniu zgłoszenie zostało przesłane wraz ze stosownym wyjaśnieniem przyczyn opóźnienia.

(akta kontroli str. 612-641)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie zarządzania danymi osobowymi przetwarzanymi w jednostce. Stwierdzona nieprawidłowość, polegajaca na opóźnieniu w przekazaniu Prezesowi UODO zgłoszenia naruszenia ochrony danych osobowych, miała charakter formalny i nie wpłynęła na obniżenie oceny.

IV. Uwagi i wnioski

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

Wnioski

1. Stosowanie ustalonych procedur przerwania pracy w systemach informatycznych.
2. Niezwłoczne wystawianie upoważnień do przetwarzania danych osobowych.
3. Terminowe zawiadamianie Prezesa UODO o przypadkach naruszenia ochrony danych osobowych.

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Łódź, dnia listopada 2019 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi

Kontroler
Magdalena Łysek
starszy inspektor kontroli państwowej

.....
podpis

Dyrektor
Przemysław Szewczyk

.....
podpis

Administrator uregulował zasady niszczenia dokumentów papierowych, a także usuwania informacji znajdujących się na sprzętach i nośnikach zewnętrznych. W IZSI wskazano m.in., że niepotrzebne wydruki zawierające dane chronione należy niszczyć wyłącznie przy pomocy niszczarek (§ 17 pkt 4). Uszkodzone lub wymontowane z likwidowanego sprzętu dyski twarde i inne równoważne nośniki danych są niszczone mechanicznie, we właściwym oddziale ds. informatyzacji (§ 5 pkt 8).

Analiza 10 (ze 116) protokołów fizycznej likwidacji dysku twardego oraz protokołu likwidacji trzech elektronicznych nośników danych wykazała, że we wszystkich przypadkach likwidacji dokonano zgodnie z wewnętrznymi procedurami.

(dowód: akta kontroli str. 249-264, 805-806)

3.3. Ochrona danych osobowych pracowników

Po wejściu w życie RODO pracodawca, jako Administrator danych osobowych, powiadomił wszystkich pracowników Urzędu o przetwarzaniu ich danych osobowych. Informacje w tym zakresie, zawierające elementy wymagane na podstawie art. 13 ust. 1 i 2 RODO, zostały zamieszczone w intranecie, na stronie BIP Urzędu oraz w miejscach ogólnodostępnych.

(dowód: akta kontroli str. 352-353, 771, 822-835 folder 1)

Badanie 10 umów cywilnoprawnych wykazało, że w ośmiu przypadkach do umowy dołączono klauzulę informacyjną zawierającą elementy wskazane w art. 13 ust. 1 i 2 RODO. W dwóch pozostałych przypadkach dopełniono obowiązku informacyjnego poprzez zamieszczenie stosownych klauzul w miejscu kontaktu z podmiotem podpisującym umowę.

Na podstawie analizy wszystkich 19 udostępnionych na stronie internetowej BIP ŁUW na dzień 29 października 2019 r., informacji o naborze na wolne stanowiska stwierdzono, że we wszystkich przypadkach zamieszczono wymaganą klauzulę informacyjną.

(dowód: akta kontroli str. 807-813)

Oferty kandydatów były przechowywane przez okres sześciu miesięcy od zakończenia procesu rekrutacji, zgodnie z zarządzeniem nr 25/2017 Dyrektora Generalnego ŁUW z dnia 29 września 2017 r. w sprawie naborów na wolne stanowiska do korpusu służby cywilnej w ŁUW. Okres przechowywania ofert uzasadniony był czasem niezbędnym do przeprowadzenia naboru na stanowisko pracy w służbie cywilnej (z uwzględnieniem 3 miesięcy, w których Dyrektor Generalny ŁUW miał możliwość wyboru kolejnego kandydata, w przypadku, gdy ponownie zaistnieje konieczność obsadzenia tego samego stanowiska). Natomiast akta dotyczące naboru były przechowywane przez okres 5 lat, co było zgodne z *Rejestrem czynności przetwarzania danych osobowych* i wynikało z oznaczenia kategorii archiwalnej (B5 dla konkursów na stanowiska w urzędach).

(dowód: akta kontroli str. 814-821, 822-835 folder 2)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Jedno z trzech zgłoszeń naruszenia ochrony danych osobowych przesłano do Prezesa UODO z przekroczeniem terminu określonego w art. 33 ust. 1 RODO (do 72 godzin). Sytuacja ta dotyczyła naruszenia stwierdzonego 25 lutego 2019 r. o godzinie 14:20, zgłoszonego do Prezesa UODO 5 marca 2019 r. o godzinie 10:18. IOD wyjaśnił, iż opóźnienie to było wynikiem błędu w EZD i natychmiast po jego naprawieniu zgłoszenie zostało przesłane wraz ze stosownym wyjaśnieniem przyczyn opóźnienia.

(akta kontroli str. 612-641)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie zarządzania danymi osobowymi przetwarzanymi w jednostce. Stwierdzona nieprawidłowość, polegajaca na opóźnieniu w przekazaniu Prezesowi UODO zgłoszenia naruszenia ochrony danych osobowych, miała charakter formalny i nie wpłynęła na obniżenie oceny.

IV. Uwagi i wnioski

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

Wnioski

1. Stosowanie ustalonych procedur przerwania pracy w systemach informatycznych.
2. Niezwłoczne wystawianie upoważnień do przetwarzania danych osobowych.
3. Terminowe zawiadamianie Prezesa UODO o przypadkach naruszenia ochrony danych osobowych.

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Łódź, dnia 3 grudnia 2019 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi

Kontroler
Magdalena Łysek
starszy inspektor kontroli państwowej

.....
podpis

Dyrektor
Przemysław Szewczyk

.....
podpis