NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.16.2017
P/17/062
UNK.10576/18

00374318

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/17/062 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontroler	Wojciech Zambrzycki – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/169/2017 z 28 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Miejski w Suwałkach, ul. Mickiewicza 1, 16-400 Suwałki (dalej: *Urząd* lub *UM*)
Kierownik jednostki kontrolowanej	Czesław Renkiewicz – Prezydent Miasta Suwałki[2] (zwany dalej *Prezydentem*)

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości[3] zapewnienie ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem.

Uzasadnienie oceny ogólnej

Ocena pozytywna wynika między innymi z profesjonalnego wykonania zabezpieczeń odpowiedzialnych za autoryzację dostępu do komputerowej sieci wewnętrznej Urzędu, zapewnienia właściwej ochrony przed nieuprawnionym dostępem, kradzieżą lub utratą danych i systematycznym wykonywania kopii zapasowych.

Stwierdzono jednak m.in. następujące nieprawidłowości:

- jednemu z 32 analizowanych pracowników nie wydano upoważnienia do zbioru danych osobowych, chociaż wykonując swoje obowiązki korzystał z tego zbioru,
- jednemu z 21 byłych pracowników po zakończeniu zatrudnienia nie odebrano dostępu do używanego przez niego systemu informatycznego,
- nierzetelnie prowadzono rejestr wewnętrzny zbiorów danych osobowych i ewidencję wydanych upoważnień,
- nie szkolono pracowników z zagrożeń bezpieczeństwa informacji,
- w jednym z 16 analizowanych zbiorów danych osobowych gromadzono więcej danych niż było to niezbędne do realizacji zadań, dla których zbiór prowadzono.

---

1 Kontrolą objęto lata 2016 – 2018 (do 13 lutego).
2 Funkcję pełni od 21 listopada 2010 r.
3 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

III. Opis ustalonego stanu faktycznego

1. Rozwiązania dotyczące dostępu do poszczególnych systemów informatycznych i usług sieciowych zabezpieczające przed nieuprawnionym dostępem, przejęciem lub zniszczeniem zasobów informacyjnych

Opis stanu faktycznego

1.1. Do gromadzenia i przetwarzania danych osobowych w Urzędzie stosowano 21 systemów informatycznych (szerzej omówiono tą kwestię w punkcie 4.1. wystąpienia), a także prowadzona była papierowa wersja dokumentacji zawierająca dane osobowe.

(dowód: akta kontroli str. 716-718)

Na wyposażeniu Urzędu znajdowało się 186 komputerów, z których 30 poddano oględzinom. Komputery miały konta administratora lokalnego i były połączone w wewnętrzną sieć. Administrator lokalny miał ograniczone uprawnienia, o czym będzie mowa w dalszej części wystąpienia. Na komputerach stosowano różne wersje systemu operacyjnego, najczęściej był to Windows 7 (19 z nich) i Windows 10 (osiem szt.). Połowa komputerów poddanych oględzinom była podłączona do Systemu Rejestrów Państwowych (dalej: *SRP*) i nie miały one dostępu do Internetu oraz służbowej poczty elektronicznej. Osiem komputerów niepoddanych oględzinom posiadało dostęp do systemu CEPiK i również nie posiadało dostępu do sieci Internet. Część ze 186 komputerów Urzędu pracowała na niewspieranym przez producenta systemie Windows XP, o czym będzie mowa w dalszej części wystąpienia, w sekcji *Uwagi dotyczące badanej działalności.*

Według powołanego przez Najwyższą Izbę Kontroli biegłego – wszyscy pracownicy mieli ograniczony dostęp do zasobów Internetu, serwerów FTP[4] i sieci P2P[5]. Kontrola nad ruchem sieciowym wychodzącym i wchodzącym do sieci LAN[6] realizowana była na poziomie urządzenia wielofunkcyjnej zapory sieciowej UTM.

(dowód: akta kontroli str. 306-316)

1.2. Urząd wywiązywał się z obowiązku określonego w § 20 ust. 2 pkt 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7], dotyczącego przeprowadzania analiz ryzyka utraty integralności, dostępności i poufności.

Raz na pół roku wykonywana była kontrola sprzętu i oprogramowania (nie było to dokumentowane z uwagi na obszerność wydruku)[8] przy pomocy narzędzia informatycznego Uplook Statlook (inne możliwości tej aplikacji omówiono w punkcie 1.4. wystąpienia). Kontrola ta – jak wyjaśnił Naczelnik Wydziału Informatyki – polegała na analizie działań użytkowników, identyfikacji zainstalowanych aplikacji, skanowaniu zawartości dysków, kontroli modyfikacji sprzętu komputerowego[9].

(dowód: akta kontroli str. 880-883)

Podczas prac nad opracowaniem dokumentów do kompleksowego systemu zarządzania bezpieczeństwem (omówionego w punkcie 2.5. wystąpienia) stworzona została macierz ryzyka. Określono w niej zasoby, przypisano im potencjalne zagrożenia i obliczono wielkość ryzyka dla danego zasobu, obliczonego jako iloczyn podatności na zagrożenie i skutku, jaki może przynieść wystąpienie sytuacji niepożądanej. Ustalono, że akceptowalnym poziomem ryzyka jest 35 punktów. Żaden z wymienionych w macierzy elementów nie przekraczał tej wartości. (dowód: akta kontroli str. 239-261)

---

4 Skrót od ang. File Transfer Protocol – protokół komunikacyjny umożliwiający dwukierunkowy transfer plików.

5 Skrót od ang. Peer-to-peer – możliwość wymiany plików pomiędzy użytkownikami.

6 Skrót od ang. local area network – sieć komputerowa łącząca komputery na określonym obszarze, w tym przypadku w Urzędzie.

7 Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: *rozporządzeniem KRI.*

8 Obowiązek przeprowadzania takiej kontroli został zawarty w § 5 zarządzenia Nr 93/2011 Prezydenta Miasta Suwałk z dnia 16 marca 2011 r. w sprawie wprowadzenia regulaminu przestrzegania zasad i procedur korzystania z legalnego oprogramowania oraz ochrony własności intelektualnej w Urzędzie Miejskim w Suwałkach.

9 Sprawdzenie to miało miejsce: 10 sierpnia 2016 r. Zinwentaryzowano wówczas 149 komputerów, 25 stycznia 2017 r. – 172 komputery, 28 września 2017 r. – 192 komputery i serwery, a 29 stycznia 2018 r. – 198 komputerów i serwerów.

Po roku funkcjonowania kompleksowego systemu zarządzania bezpieczeństwem przeprowadzony został jego przegląd okresowy. W okresie objętym kontrolą[10] miały miejsce trzy zdarzenia mające wpływ na bezpieczeństwo informacji: (1) awaria macierzy dyskowej, (2) problemy z instalacją elektryczną w jednej z siedzib Urzędu i (3) próbne wyłączenie całego środowiska IT Urzędu podczas ćwiczeń przeciwpożarowych. W podsumowaniu stwierdzono, że procedury były sprawne, a wszystkie działania następcze wykonano prawidłowo. (dowód: akta kontroli str. 911-913)

1.3. Na zbadanej próbie 32 (z 214) pracowników Urzędu stwierdzono, że 31 z nich posiadało uprawnienia pokrywające się z ich zakresami obowiązków. Jedna z osób objętych analizą nie posiadała upoważnienia do zbioru danych osobowych z którego korzystała. Ponadto jeden z 21[11] byłych pracowników nadal widniał wśród użytkowników jednego z systemów informatycznych. Będzie o tym mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.* (dowód: akta kontroli str. 317-439)

Poza wyznaczonymi pracownikami Wydziału Informatyki, pozostali pracownicy nie posiadali uprawnień administratorów sieciowych. Każdy z nich posiadał własny login i hasło do stanowiska komputerowego i użytkowanego oprogramowania, niektórzy użytkowali karty chipowe. Hasła spełniały wymogi określone dla wysokiego poziomu bezpieczeństwa, o którym mowa w punkcie XIV części C, w związku z punktem VIII części B załącznika do 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[12]. Wysoki poziom bezpieczeństwa został wskazany w Instrukcji Zarządzania Systemami Informatycznymi, omówionej w punkcie 2.10. wystąpienia. Nie stwierdzono, aby użytkowano jedno konto przez kilku użytkowników.
(dowód: akta kontroli str. 157-158, 263, 306-310, 545,548)

1.4. Prowadzony był elektroniczny rejestr dostępu do systemów informatycznych. Informacje o logach[13] były przetwarzane automatycznie i analizowane przy pomocy narzędzia Uplook Statlook. Logi były przechowywane tak długo, jak kopia bezpieczeństwa, których były integralna częścią (30 dni). Biegły z dziedziny informatyki stwierdził, że logi generowane w systemie były zabezpieczone przed utrata integralności i zniszczeniem, co w sytuacji niepożądanej z punktu widzenia bezpieczeństwa danych dawało duże prawdopodobieństwo ustalenia sprawcy lub źródła zagrożenia.
(dowód: akta kontroli str. 311-316)

1.5. Biegły, powołany przez Najwyższą Izbę Kontroli, stwierdził, że wszystkie komputery pracowały pod kontrolą domeny, co gwarantowało zabezpieczenie przed nieautoryzowanym dostępem do komputerów i usług sieciowych. Zastosowane było wymuszenie okresowej zmiany hasła[14]. Urządzenia pracujące w serwerowni były zabezpieczone hasłem, co wykluczało nieautoryzowany dostęp do nich. Sieć WI-FI pracująca na terenie Urzędu została fizycznie odseparowana od sieci LAN i była dostępna gościom UM.
(dowód: akta kontroli str. 311-316)

1.6. Wewnętrzne regulacje (omówione w punktach 2.5. i 2.10. wystąpienia) określały, że zabronione jest podłączanie do sieci LAN urządzeń niebędących własnością Urzędu bez nadzoru pracowników Wydziału Informatyki. Według biegłego, konfiguracja sieciowa umożliwiała podłączenie do infrastruktury jednostki sprzętu (laptopy, telefony, tablety) niestanowiącego własności pracodawcy, ale nie było możliwe korzystanie z jej zasobów za pomocą wspomnianego sprzętu. Informacje o podłączeniu do komputerów zewnętrznych

---

[10] Od 30 czerwca 2016 r. do 25 lipca 2017 r.

[11] Zatrudnienie zakończyło 27 osób, ale siedmioro z nich na dzień kontroli ponownie było pracownikami Urzędu.

[12] Dz. U. Nr 100 poz. 1024. Rozporządzenie zwane dalej: *rozporządzeniem MSWiA*.

[13] Log (inaczej: dziennik, plik dziennika, rejestr zdarzeń) – chronologiczny zapis zawierający informację o zdarzeniach i działaniach dotyczących systemu informatycznego, systemu komputerowego czy komputera. Log tworzony jest automatycznie przez dany program komputerowy, a sama czynność zapisywania do logu nazywana jest też logowaniem – nie należy mylić tego określenia z logowaniem w celu wykonania uwierzytelnienia. https://pl.wikipedia.org/wiki/Log_(informatyka)

[14] Stało się tak po audycie wewnętrznym bezpieczeństwa informacji, omówionym w punkcie 2.7. wystąpienia.

nośników pamięci (np. pendrive lub dysk przenośny) były zaś monitorowane przez aplikację Statlook. (dowód: akta kontroli str. 311-316)

1.7. W okresie objętym kontrolą nie wystąpiły przypadki wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, np. penetracji systemu informatycznego przez nieuprawnioną osobę. (dowód: akta kontroli str. 880-883)

1.8. Według biegłego, w UM nie był przewidziany zdalny dostęp pracowników do zasobów sieci lokalnej (nie licząc administratorów sytemu). O takiej możliwości nie wspominały też wewnętrzne regulacje. (dowód: akta kontroli str. 184-298, 311-316)

1.9. Zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI, we wszystkich 17 umowach serwisowych z lat 2016 – 2017 (zawartych z sześcioma podmiotami), wpisane zostały gwarancje dotyczące poufności oraz opisane warunki, jakie musi spełniać wykonawca w odniesieniu do danych, z którymi ma styczność w związku z realizacją usług serwisowych. (dowód: akta kontroli str. 555-556)

1.10. Wszystkie komputery wchodzące w skład sieci lokalnej – jak stwierdził biegły – były zabezpieczone dedykowanym do tego celu oprogramowaniem antywirusowym z modułem centralnego zarządzania. Badane komputery posiadały aktualne wersje aplikacji zabezpieczających. Dostęp do sieci lokalnej z zewnątrz kontrolowany jest przez firewall sprzętowy marki Stormshield. (dowód: akta kontroli str. 311-316)

1.11. Urząd wykorzystywał zewnętrzne serwery poczty elektronicznej i domen. Dostawca usługi posiadał certyfikat[15] potwierdzający zarządzanie bezpieczeństwem informacji. W regulaminie korzystania z usług zapisano, że usługodawca przetwarza dane osobowe zgodnie z zasadami wskazanymi w ustawie o ochronie danych osobowych oraz o świadczeniu usług drogą elektroniczną, a przed przetwarzaniem danych podejmuje środki zabezpieczające zbiór danych osobowych w sposób, o którym mowa w przepisach polskiego prawa. Wykupiony przez Urząd pakiet zapewniał ochronę przed SPAM-em[16] i wiadomościami zawierającymi wirusy. Poza tym, jak wspomniano w punkcie 1.1. wystąpienia, nad bezpieczeństwem ruchu sieciowego wchodzącego i wchodzącego do sieci LAN czuwała wielofunkcyjna zapora sieciowa UTM, składająca się ze sprzętowego firewalla, ochrony przed włamaniami IPS (Intrusion Prevention System), tuneli sieci prywatnej VPN, systemu antywirusowego i antyspamowego oraz narzędzi do monitoringu sieci. (dowód: akta kontroli str. 311-316, 880-910)

1.12. Częstotliwość wykonywania kopii zapasowych została określona w *Polityce wykonywania kopii zapasowych*, a przyjęte regulacje w tym zakresie były stosowane w praktyce. Systematycznie, raz dziennie backupowane były systemy operacyjne końcówek klienckich oraz profile użytkowników. Do tego celu wykorzystywane było narzędzie Ferro Backup System. Zasoby sieciowe również były archiwizowane codziennie. Wykorzystywane przy tym było narzędzie EMC Avamar. Kopia całego systemu wykonywana była raz w tygodniu poprzez backup różnicowy. Wszystkie kopie bezpieczeństwa zapisywane były na urządzeniu, znajdującym się w innej lokalizacji niż siedziba głównego budynku Urzędu. Backupy przechowywane były przez 30 dni. (dowód: akta kontroli str. 267-268, 306-316)

W okresie objętym kontrolą wystąpiła konieczność odtworzenia zbioru danych z kopii zapasowej i według Naczelnika Wydziału Informatyki odzyskano wszystkie dane. Zbędne kopie były nadpisywane automatycznie. (dowód: akta kontroli str. 545-548)

1.13. Jak ustalił biegły, pracownicy UM nie dysponowali możliwością ściągania aplikacji i plików wykonalnych, jak i nie posiadali uprawnień do instalowania ich na stacjach komputerowych, do których mieli dostęp. (dowód: akta kontroli str. 311-316)

1.14. Wszystkie zbadane przez biegłego i kontrolera komputery posiadały aktualne wersje systemów operacyjnych i aplikacji bezpieczeństwa. Aktualizacje były wykonywane zgodnie z harmonogramem ustawionym przez administratora. Aktualna była również wersja specjalistycznego oprogramowania zainstalowanego na komputerach i na serwerze.
(dowód: akta kontroli str. 306-316)

---

[15] ISO/IEC 27001:2013 i ISO 9001:2008.

[16] Niechciane lub niepotrzebne wiadomości elektroniczne zwykle wysyłane masowo.

Podsumowując swoje badania biegły stwierdził, że poziom zabezpieczeń odpowiedzialnych za autoryzację dostępu do sieci Urzędu był wykonany profesjonalnie. Zasoby informacyjne UM były właściwie chronione przed nieuprawnionym dostępem, kradzieżą lub utratą. Praca sieci znajdowała się pod pełną kontrolą administratora. (dowód: akta kontroli str. 311-316)

1.15. Płatności drogą elektroniczną wykonywane były na zabezpieczonej stronie banku. Zasady realizacji płatności były określone dokumentacją wewnętrzną[17]. Pracownik Wydziału Budżetu i Finansów wyjaśnił, że realizując płatności drogą elektroniczną, po zalogowaniu się do systemu bankowego wprowadza przelew na konto wskazane w dokumencie źródłowym (potwierdzone przez wydział merytoryczny, że numer konta bankowego jest zgodny z zawartą umową), przygotowuje zbiorcze zestawienia przelewów i raz jeszcze sprawdza numer konta bankowego. Wprowadzone przelewy były następnie podpisywane dwuosobowo przez kierownictwo Urzędu. (dowód: akta kontroli str. 596-599)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niezablokowaniu niezwłocznie konta użytkownika programu Płatnik jednemu z 21 (4,7%) byłych pracowników Urzędu. Blokadę pracownikowi M. Ś. z Wydziału Organizacyjnego założono w trakcie kontroli NIK – 2 lutego 2018 r., a zatrudniony był on do 27 lipca 2017 r. Naczelnik Wydziału wyjaśnił, że komputer pracownika został zabrany przez Wydział Informatyki i według jego wiedzy został *wyczyszczony*. Uznał zatem, że nie ma potrzeby aby dodatkowo informować o konieczności zablokowania dostępu do Płatnika, bo nie było już możliwości zalogowania się do tego programu. Z kolei Naczelnik Wydziału Informatyki wyjaśnił, że komputer pracownikowi został odebrany i przechowywany w magazynie. Nie miał on więc możliwości zalogowania się i korzystania z Płatnika. Przy odejściu z pracy oddał kartę chipową do domeny, którą logował się do komputera i kartę z podpisem elektronicznym. W innych użytkowanych przez niego programach dostęp został zablokowany.

(dowód: akta kontroli str. 549-553, 867-868, 880-881)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że na siedmiu spośród 186 komputerów (3,8%) wykorzystywanych w Urzędzie zainstalowany był system operacyjny Windows XP, który nie był objęty wsparciem producenta. Wprawdzie komputery te były wykorzystywane do prostych prac biurowych, to jednak ich podłączenie do sieci Urzędu może stanowić zagrożenie dla jej bezpieczeństwa. (dowód: akta kontroli str. 311-316)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie rozwiązania dotyczące dostępu do poszczególnych systemów informatycznych i usług sieciowych zabezpieczające przed nieuprawnionym dostępem, przejęciem lub zniszczeniem zasobów informacyjnych. Stwierdzona nieprawidłowość nie miała wpływu na ocenę kontrolowanej działalności.

2. Dokumentacja i procedury dotyczące ochrony danych osobowych

Opis stanu faktycznego

2.1. Na dzień rozpoczęcia kontroli NIK, dane przetwarzane były w 93 zbiorach wpisanych do Rejestru Wewnętrznego Zbiorów Danych Osobowych Przetwarzanych przez Urząd Miejski w Suwałkach (dalej: *Rejestr Wewnętrzny Zbiorów*)[18]. Do rejestru prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych (dalej: *GIODO*) zgłoszono 53 z nich[19]. Pozostałe nie podlegały zgłoszeniu i były prowadzone przez Administratora Bezpieczeństwa Informacji (dalej: *ABI*) w jego rejestrze.

(dowód: akta kontroli str. 506-528, 770-792, 931-932)

W latach 2016 – 2017 GIODO nie odmawiał rejestracji zgłaszanych zbiorów. W okresie objętym kontrolą zostało wystosowane do GIODO pismo o wykreślenie 10 zbiorów danych osobowych[20]. Wszystkie sytuacje dotyczyły zaprzestania korzystania z tych zbiorów i przekazania dokumentacji do archiwum. W odpowiedzi GIODO odmówił ich wykreślenia i polecił zarchiwizowanie dokumentacji ich dotyczącej, wskazując, że dane w zbiorach nadal

---

[17] Zarządzenie Nr 685/2012 Prezydenta Miasta Suwałk z dnia 12 grudnia 2012 r. w sprawie przepisów wewnętrznych regulujących zasady rachunkowości w Urzędzie Miejskim w Suwałkach.

[18] Rejestr liczył 96 pozycji, ale trzy zbiory zostały wykreślone w 2015 roku.

[19] Zgłoszenia miały miejsce od 27 września 1999 r. do 29 grudnia 2017 r.

[20] Dotyczyło to zbiorów o numerach księgi 87190, 102020, 110137, 136471, 136475, 136476, 136479, 136481, 136485, 135557.

są przetwarzane – zmianie uległa tylko podstawa prawna i cel przetwarzania danych. W Rejestrze Wewnętrznym Zbiorów sytuację tę opisano jako *archiwizacja*. Zbiory nadal widniały w elektronicznym rejestrze prowadzonym na stronie internetowej GIODO[21] i w Rejestrze Wewnętrznym Zbiorów.

Pomimo wskazań GIODO, w Rejestrze Wewnętrznym Zbiorów nie zaktualizowano podstawy prawnej i celu przetwarzania danych we wspomnianych 10 zbiorach, o czym szerzej będzie mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości*.

(dowód: akta kontroli str. 793-796, 856-866)

2.2. Prezydent powołał obecnego ABI od 1 marca 2015 r.[22] Wnioskiem Prezydenta z 10 marca 2015 r. ABI został zgłoszony GIODO, a więc nastąpiło to w terminie zgodnym z art. 46b ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[23] (30 dni od daty powołania). Poprzedni ABI nie był zgłoszony GIODO (w ówcześnie obowiązującym brzemieniu ustawy o ochronie danych osobowych nie było art. 46b), a zatem nie było również zgłoszone GIODO jego odwołanie. (dowód: akta kontroli str. 557-561, 597)

2.3. W okresie objętym kontrolą ABI dokonał sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ich ochronie w czterech (z 26 istniejących) komórkach organizacyjnych Urzędu, z którego sprawozdanie przekazał Prezydentowi. ABI wypełnił tym samym obowiązek, o którym mowa w art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych. Sprawozdanie zawierało wszystkie elementy, o których mowa w art. 36c tej ustawy. W dwóch kontrolowanych wydziałach stwierdził nieprawidłowości dotyczące m.in. nieposiadania uprawnień do rejestrów albo korzystania z rejestrów pomimo braku potrzeby przez pracownika i niezawarcia umów powierzenia przetwarzania danych osobowych, chociaż były one przekazane innemu podmiotowi. Zalecenia zostały wykonane, poza jednym, dotyczącym dostawienia szafy na dokumenty w jednym z pokojów.

(dowód: akta kontroli str. 562-563)

Wywiązując się z obowiązku, o którym mowa w art. 36a ust. 2 pkt 1 lit. b ustawy o ochronie danych osobowych, ABI uczestniczył w opracowaniu Polityki Bezpieczeństwa, szerzej omówionej w punkcie 2.10. Stanowiła ona cześć Systemu Zarządzania Bezpieczeństwa Informacji, wprowadzonego zarządzeniem Nr 211/2016 Prezydenta Miasta Suwałk z 30 czerwca 2016 r.[24] (dowód: akta kontroli str. 865-866)

Wypełniając obowiązek związany z zapewnieniem zapoznania się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (wskazany w art. 36a ust. 2 pkt 1 lit. c ustawy o ochronie danych osobowych), w latach 2015 – 2016 ABI zorganizował szkolenie dla pracowników Urzędu z zakresu prawnych aspektów legalnego przetwarzania danych osobowych. W 2015 roku przeszkolonych zostało 151 osób, a w 2016 – 43 (byli to pracownicy, którzy nie mogli, z różnych względów, zostać przeszkoleni w roku poprzednim). ABI uczestniczył w szkoleniu[25] przed objęciem swojej funkcji, a następnie jeszcze dwukrotnie[26]. (dowód: akta kontroli str. 569-586)

ABI prowadził Rejestr Wewnętrzny Zbiorów. Na dzień rozpoczęcia kontroli rejestr zawierał 93 pozycje i informacje wymagane § 3 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych[27]. Dopiero w trakcie kontroli NIK zarejestrowano w Rejestrze Wewnętrznym Zbiorów i zgłoszono GIODO zbiór dotyczący osób uprawnionych do korzystania z karty dużej rodziny i kolejny – dotyczący kierowania

---

21 https://egiodo.giodo.gov.pl/.

22 Poprzedni ABI pełni funkcję od 2007 roku do powołania swego następcy.

23 Dz. U. z 2016 r. poz. 922.

24 Pełna nazwa zarządzenia: zarządzenie Nr 211/2016 Prezydenta Miasta Suwałk z dnia 30 czerwca 2016 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji oraz Polityki Bezpieczeństwa Informacji Urzędu Miejskiego w Suwałkach. Zarządzenie zwane w dalszej części: „*zarządzeniem w sprawie SZBI*".

25 *Praktyczne prawne aspekty ochrony danych osobowych i baz danych – szkolenie i warsztaty (wraz z kompletem wniosków, oświadczeń i wzorów innych dokumentów)* – 30 stycznia 2015 r.

26 *Nowelizacja ustawy o ochronie danych osobowych – nowy status ABI, nowe prawa i obowiązki dla ADO, nowe obowiązki dotyczące rejestracji zbiorów. Dokumentacja i procedury bezpieczeństwa* – 31 sierpnia 2015 r. i *Obowiązkowa dokumentacja przetwarzania danych w RODO* – 18 września 2017 r.

27 Dz. U. poz. 719.

na leczenie odwykowe, o czym będzie mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.* (dowód: akta kontroli str. 506-528, 832-856)

2.4. ABI prowadził Ewidencję Osób Upoważnionych do Przetwarzania Danych Osobowych (dalej: *Ewidencja Osób Upoważnionych*). Zawierała ona informacje, o których mowa w art. 39 ust. 1 ustawy o ochronie danych osobowych: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, identyfikator, jeżeli dane są przetwarzane w systemie informatycznym. Ewidencja Osób Upoważnionych była prowadzona nierzetelnie, o czym będzie mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.* Z analizowanej próby 32 z 214 pracowników Urzędu, 31 z nich posiadało wymagane upoważnienia do przetwarzania danych osobowych. O przetwarzaniu danych w zbiorach danych osobowych jednego z pracowników również będzie mowa w sekcji *Ustalone nieprawidłowości.*

(dowód: akta kontroli str. 323-505)

Prezydent posiadał upoważnienie do przetwarzania danych w SRP, nadane przez Ministra Cyfryzacji. Urząd informował również tego Ministra o upoważnieniach wydanych pracownikom realizującym zadania związane z dostępem do SRP.

(dowód: akta kontroli str. 564-568)

2.5. W Urzędzie od 30 czerwca 2016 r. obowiązywał System Zarządzania Bezpieczeństwem Informacji oraz Polityka Bezpieczeństwa Informacji Urzędu Miejskiego w Suwałkach – wprowadzone na podstawie § 20 ust. 1 rozporządzenia KRI. System ten obejmował 20 regulacji wewnętrznych, w tym:

- politykę kontroli dostępu – opisującą sposób uzyskania dostępu do sieci komputerowej Urzędu oraz zasady tworzenia haseł dostępu,
- instrukcję pracy na stanowisku wyposażonym w monitor i drukarkę, gdzie wskazano m.in., że zabronione jest podłączanie do sieci LAN urządzeń niebędących własnością Urzędu bez nadzoru pracowników Wydziału Informatyki,
- procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji – opisującą sposób postępowania pracowników w przypadku wystąpienia incydentu bezpieczeństwa informacji,
- politykę urządzeń mobilnych i telepracy – dotyczącą zasad pracy zdalnej i wymagane środki bezpieczeństwa.

Opis systemu służącego ochronie danych i ich zbiorów, w tym dowodów księgowych i innych dokumentów stanowiących podstawę dokonania w nich zapisów, został zawarty w załączniku nr 4 do Instrukcji obiegu, kontroli i archiwizowania dokumentów finansowo-księgowych w Urzędzie Miejskim w Suwałkach. W mocy było również zarządzenie Prezydenta w sprawie korzystania z legalnego oprogramowania oraz własności intelektualnej[28]. (dowód: akta kontroli str. 184-298)

Do 30 czerwca 2016 r., tj. do wejścia w życie zarządzenia w sprawie SZBI, nie opracowano kompleksowego systemu zarządzania bezpieczeństwem, o czym będzie mowa w dalszej części wystąpienia, w sekcji *Uwagi dotyczące badanej działalności.*

2.6. Czterem pracownikom Wydziału Informatyki powierzono obowiązki związane z administrowaniem systemów informatycznych. Administratorzy posiadali stosowne upoważnienia oraz zostali zobowiązani do przestrzegania przepisów prawa podczas wykonywania swoich zadań[29]. (dowód: akta kontroli str. 612-626)

2.7. Audytor wewnętrzny Urzędu, stosownie do § 20 ust. 2 pkt 14 rozporządzenia KRI, przeprowadził audyt bezpieczeństwa informacji. Audyt za rok 2016 rozpoczęto 4 stycznia

---

[28] Pełna nazwa: zarządzenie Nr 93/2011 Prezydenta Miasta Suwałk z dnia 6 marca 2011 r. w sprawie wprowadzenia regulaminu przestrzegania zasad i procedur korzystania z legalnego oprogramowania oraz ochrony własności intelektualnej w Urzędzie Miejskim w Suwałkach.

[29] W zakresach obowiązków wymieniono następujące akty prawne: ustawa o ochronie danych osobowych, rozporządzenie KRI, ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167, ze zm.), ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 r. poz. 1764, ze zm.), ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570).

2017 r., trwał do 7 grudnia 2017 r. i objął również rok 2017. Wykazał on m.in. niżej wymienione uchybienia.

1. W prowadzonej analizie ryzyka nie został wskazany właściciel ryzyka z imienia i nazwiska, a jedynie wskazane zostało *pracownik merytoryczny*. Prezydent zobowiązał się do wskazywania w przyszłości właściciela ryzyka, co będzie podstawą do skuteczniejszej identyfikacji ryzyka, zapobieganiu jego powstawania lub skutecznego eliminowania w sytuacji zagrożenia.
2. Nie wprowadzono mechanizmu wymuszania okresowej zmiany hasła do sytemu informatycznego co 30 dni. Wprawdzie w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Suwałkach zawarty był zapis o konieczności okresowej zmiany hasła co miesiąc, lecz system informatyczny nie wymuszał takiej zmiany. Prezydent wyjaśnił, że zrealizowano wniosek audytora i wymuszane są okresowe zmiany haseł.
3. Pracownicy Urzędu nie byli objęci szkoleniami z zakresu zagrożenia bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej i stosowania środków zapewniających bezpieczeństwo informacji, czego wymaga § 20 ust. 2 pkt 6 rozporządzenia KRI. Mając na uwadze zachodzące zmiany w otoczeniu, nowe niebezpieczeństwa i źródła zagrożeń, Prezydent polecił Wydziałowi Organizacyjnemu przeprowadzenia analizy potrzeb szkoleniowych w obszarze bezpieczeństwa informacji.
4. W zakresie obowiązków jednego z pracowników Wydziału Informatyki nie został uwzględniony obowiązek prowadzenia ewidencji, w tym oprogramowania i nośników oprogramowania, chociaż wykonywał on te czynności po odchodzącym z pracy innym pracowniku Urzędu. Według odpowiedzi Prezydenta – przypisane zostały obowiązki wykonującemu je pracownikowi.
5. Nieunormowane było funkcjonowanie wewnętrznej strony Urzędu, na której znajdowała się m.in. dokumentacja wewnętrzna i instrukcje, w tym System Zarządzania Bezpieczeństwem Informacji i Polityka Bezpieczeństwa Informacji. Zdaniem audytora nie każdy z pracowników mógł być świadomym istnienia takiego serwisu internetowego. Prezydent polecił przygotowanie propozycji zmian w Regulaminie organizacyjnym i / lub uregulowania tego w Regulaminie pracy.

Audytor wewnętrzny zwrócił także uwagę, że załączniki do zarządzenia w sprawie SZBI nie są dostępne na Biuletynie Informacji Publicznej (dalej: *BIP*), a jedynie na wewnętrznej stronie Urzędu, dostępnej tylko pracownikom. Poza tym tylko trzy z 20 załączników zostało wprowadzonych zarządzeniami Prezydenta. Zdaniem audytora należałoby pozostałe załączniki wprowadzić zarządzeniami Prezydenta. Naczelnik Wydziału Informatyki, odpowiadając na zarzuty audytora wewnętrznego stwierdził, że w § 4 Polityki Bezpieczeństwa Informacji wskazane jest, że za dokumenty powiązane z tą polityką uznaje się wszystkie wymienione w załączniku do niej. Dodał, że nie wszystkie załączniki są opublikowane w BIP i jest to zabieg celowy, gdyż – dbając o bezpieczeństwo – nie można publikować procedur reagowania na zagrożenia. Prezydent podjął decyzję, przychylając się do wniosku audytora wewnętrznego, że w 2018 roku audyt bezpieczeństwa informacji zostanie powierzony podmiotowi zewnętrznemu, który sprawdzi dokumentację, procedury, jej zgodność z aktualnymi wymogami prawnymi oraz zapewnienie akceptowalnego poziomu bezpieczeństwa gromadzonych danych.

Po audycie Prezydent podjął również decyzję, że przy każdym logowaniu do systemu informatycznego pracownikom ukaże się komunikat przypominający m.in. o konieczności zachowania bezpieczeństwa danych, korzystaniu tylko z oprogramowania udostępnionego przez pracodawcę, blokowaniu ekranu podczas nieobecności przy stanowisku.

(dowód: akta kontroli str. 627-715)

2.8. Nie były przeprowadzane szkolenia dotyczące procesu przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: (1) zagrożenia bezpieczeństwa informacji, (2) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, (3) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich. Na nieorganizowanie

takich szkoleń zwracał uwagę audytor wewnętrzny. O nieorganizowaniu szkoleń w powyższym zakresie będzie mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.* (dowód: akta kontroli str. 597-603)

2.9. W latach 2016 – 2017 Urząd nie był objęty kontrolą zewnętrzną dotyczącą zapewnienia bezpieczeństwa elektronicznych zasobów informacyjnych. (dowód: akta kontroli str. 3)

2.10. Od 22 września 2004 r.[30] Urząd posiadał dokumentację opisującą zasady ochrony i zabezpieczania danych księgowych, a 9 maja 2005 r. zastąpiło je zarządzenie w sprawie ustalenia polityki bezpieczeństwa i wprowadzenia do użytku służbowego instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Suwałkach[31]. W okresie objętym kontrolą obowiązywało zarządzenie nr 207/2015 z 12 czerwca 2015 r., zastąpione zarządzeniem nr 68/2016 z 7 marca 2016 r. i zarządzeniem nr 93/2017 z 20 marca 2017 r. Prezydenta Miasta Suwałk w tej sprawie.

Polityka Bezpieczeństwa zawierała elementy określone w § 4 rozporządzenia MSWiA:

- aktualny wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie,
- aktualny wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania,
- opis struktury przetwarzanych zbiorów danych osobowych,
- sposób przepływu danych pomiędzy poszczególnymi systemami Urzędu,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Jednocześnie Polityka Bezpieczeństwa zwierała procedurę postępowania z kluczami do pomieszczeń biurowych, wzór upoważnienia dla ABI, wzór umowy powierzenia przetwarzania danych osobowych, wzór wniosku zgłoszenia zbioru do rejestracji w Rejestrze Wewnętrznym Zbiorów. (dowód: akta kontroli str. 62-183)

Instrukcja Zarządzania Systemami Informatycznymi zawierała elementy określone w § 5 rozporządzenia MSWiA:

- procedurę nadawania, zarządzania i użytkowania uprawnień do przetwarzania danych osobowych,
- stosowane metody i środki uwierzytelniania oraz związane z ich zarządzaniem i użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego,
- procedury tworzenia, przechowywania i niszczenia kopii zapasowych,
- procedury używania, przechowywania i niszczenia elektronicznych nośników informacji zawierających dane osobowe,
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
- procedury wykonywania przeglądów, konserwacji i naprawy systemów oraz elektronicznych nośników informacji służących do przetwarzania danych.

Instrukcja Zarządzania Systemami Informatycznymi zawierała także opis obowiązków pracowników związanych z przetwarzaniem danych osobowych, opis postępowania w przypadku naruszenia ochrony zbioru danych, ogóle zasady eksploatacji systemów komputerowych i systemów przetwarzania danych osobowych, wzór wniosku o nadanie lub cofnięcie uprawnień do przetwarzania danych osobowych, wzór upoważnienia

---

[30] Z tym dniem weszło w życie zarządzenie nr 216/04 Prezydenta Miasta Suwałk z dnia 22 września 2004 r. w sprawie zasad ochrony i zabezpieczenia danych księgowych. Dostępne na stronie BIP Urzędu pod adresem: http://bip.um.suwalki.pl/zarzadzenie_s/zarz_0922_216_04.html.

[31] Zarządzenie nr 77/05 Prezydenta Miasta Suwałk z dnia 9 maja 2005 r. w sprawie ustalenia polityki bezpieczeństwa i wprowadzenia do użytku służbowego instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Suwałkach. Dostępne na stronie BIP Urzędu pod adresem: http://bip.um.suwalki.pl/zarzadzenie_s/zarz_0509_77_05.html.

do przetwarzania danych osobowych i wzór oświadczenia osoby, której udzielono tego upoważnienia. Zawarty był również zapis, że stosuje się wysoki poziom bezpieczeństwa przetwarzania danych osobowych, stosownie do § 6 ust. 4 rozporządzenia MSWiA.

(dowód: akta kontroli str. 62-183)

Ustalone nieprawidłowości

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

1. Rejestr Wewnętrzny Zbiorów nie był prowadzony rzetelnie:
   - Nie został w nim zarejestrowany zbiór *Rządowy Program pomocy rodzinom wielodzietnym Karta Dużej Rodziny*[32] oraz zbiór *Ewidencja osób kierowanych na leczenie odwykowe*. Rejestracji tych zbiorów dokonano w trakcie kontroli NIK (5 i 29 grudnia 2017 r.), chociaż były one prowadzone od 20 czerwca 2014 r. i 3 stycznia 1997 r. Zbiory zawierały dane wrażliwe i wnioskami z 29 grudnia 2017 r. zostały zgłoszone GIODO. ABI wyjaśnił, że nie zarejestrował tych zbiorów, ponieważ nie przekazano mu wniosków o ich rejestrację, pomimo pism ze strony Prezydenta o konieczności zgłaszania wszystkich przetwarzanych zbiorów zawierających dane osobowe. Prezydent wyjaśnił, że nie miał świadomości, że te zbiory nie były zarejestrowane i potwierdził, że pisemnie zwracał się do osób odpowiedzialnych za organizację pracy o zgłaszanie ABI tych zbiorów, celem zarejestrowania.

     (dowód: akta kontroli str. 506-528, 731, 756-792, 832-856, 865-866, 877-879)

     Naczelnik Wydziału Spraw Społecznych wyjaśnił z kolei, że w przypadku zbioru dotyczącego Karty Dużej Rodziny – był przekonany, że rejestracji dokonał poprzedni ABI. Pośrednim dowodem na to miałaby być korespondencja do obecnego ABI, aby dokonać zmian w zakresie danych gromadzonych w tym zbiorze po nowelizacji ustawy o Karcie Dużej Rodziny. Zbiór dotyczący osób kierowanych na leczenie odwykowe nie został zgłoszony ABI, gdyż nie było uregulowań prawnych w tym zakresie. Na zapytanie wystosowane do GIODO, czy zbiór powinien zostać zgłoszony, Naczelnik otrzymał odpowiedź, że: *kwestia przetwarzania danych osobowych przez gminne komisje rozwiązywania problemów alkoholowych nie została objęta kompleksową regulacją.* Podobne stanowisko pracownicy Wydziału usłyszeli podczas szkolenia *Prawne aspekty legalnego przetwarzania danych osobowych*, w trakcie którego trener szkolenia wskazał, że czynności podejmowane przez gminne komisje rozwiązywania problemów alkoholowych są podejmowane na potrzeby postępowania sądowego, a zatem – w myśl art. 43 ust. 1 pkt 2 ustawy o ochronie danych osobowych – zwolnione są z rejestracji. Jednak pomimo wątpliwości, Naczelnik zapobiegawczo zgłosił zbiór do rejestracji, aby sprawę ostatecznie zamknąć.

     (dowód: akta kontroli str. 914-922)

   - Po zawnioskowaniu do GIODO o wykreślenie 10 zbiorów danych[33] w odpowiedzi Dyrektor Departamentu Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych w biurze GIODO nie zgodził się na wykreślenie zbiorów. Stwierdził, że zmianie uległa podstawa prawna prowadzenia zbiorów na ustawę z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach[34] oraz cel przetwarzania danych – na archiwalny. Pomimo takiej informacji, w Rejestrze Wewnętrznym Zbiorów nie zmieniono podstawy prawnej prowadzenia zbiorów i nie zmieniono celu ich przetwarzania. ABI wyjaśnił, że źle zrozumiał pismo GIODO w tym zakresie. (dowód: akta kontroli str. 793-796, 865-866)

2. Pracownik E. R. z Biura Prezydenta Miasta została zatrudniona od 2 listopada 2016 r. i w zakresie obowiązków z tego dnia miała wskazaną obsługę skarg, natomiast upoważnienie do zbioru danych *Skargi*[35] zostało jej nadane dopiero w trakcie kontroli NIK – 2 stycznia 2018 r. Kierownik Biura Prezydenta Miasta sądził, że sprawa ta została uregulowana przez jego poprzednika. Prezydent wyjaśnił z kolei, że nie miał świadomości

---

[32] Według informacji na stronie internetowej GIODO – gmina administratorem danych przetwarzanych w celu przyznania Karty Dużej Rodziny: https://giodo.gov.pl/pl/259/10094.

[33] Zbiory o numerach księgi: 87190, 102020, 110137, 136471, 136475, 136476, 136479, 136481, 136485, 135557.

[34] Dz. U. z 2018 r. poz. 217.

[35] Nie wiązało się to z użytkowaniem specjalistycznego oprogramowania.

tej sytuacji. Wnioski o nadanie lub cofnięcie uprawnień składają bezpośredni przełożeni pracowników. (dowód: akta kontroli str. 434-436, 473, 592-595, 862-863, 877-879)

Stosownie do przepisu § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI, kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji, a także bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań tych osób.

3. Ewidencja Osób Upoważnionych była prowadzona nierzetelnie. Stosownie do art. 39 ust. 1 ustawy o ochronie danych osobowych, powinna ona zawierać: (1) imię i nazwisko osoby upoważnionej, (2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, (3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym. W trakcie kontroli ustalono, że w ewidencji[36]:
   - W 103 pozycjach (14%) wskazano identyfikator użytkownika (najczęściej była to pierwsza litera imienia i nazwisko pisane łącznie), co stosuje się, gdy przetwarzanie danych odbywa się w systemie informatycznym. W przedmiotowych sytuacjach przetwarzanie danych, według zestawienia przygotowanego w trakcie kontroli, odbywało się papierowo. ABI wyjaśnił, że wpisał nazwę użytkownika dostępu do komputera, bo część obowiązków może być realizowana elektronicznie, np. napisanie dokumentu w systemie Word. Najwyższa Izba Kontroli zwraca jednak uwagę, że wspomniany system jest co najwyżej narzędziem do prowadzenia sprawy. Sam zbiór nadal jest prowadzony w wersji papierowej i niewłaściwe jest nadawanie upoważnień z identyfikatorem użytkownika do zbioru prowadzonego w formie papierowej.
   - W 38 pozycjach (5%) nie wpisany został identyfikator użytkownika, chociaż przetwarzanie danych odbywało się w systemie informatycznym. ABI wyjaśnił, że identyfikator jest zawarty w upoważnieniu, ale przez pomyłkę nie został wpisany w ewidencji.
   - W pięciu pozycjach (nr. 260, 265, 271, 564, 710) nie została wpisana data nadania upoważnienia, a nadano je 27 listopada i 30 grudnia 2015 r. oraz 22 września 2017 r. ABI wyjaśnił, że data nie została wpisana przez przeoczenie.
   - Do Ewidencji Osób Upoważnionych nie wpisano siedmiu upoważnień wydanych pięciu pracownikom[37]:
     - A. O. z Wydziału Ochrony Środowiska i Gospodarki Komunalnej (upoważnienie nr In.1334.273.2012 z 21 listopada 2012 r.) do zbioru *Rejestru gruntów i budynków*,
     - R. R. z Wydziału Ochrony Środowiska i Gospodarki Komunalnej (upoważnienie nr In.1334.280.2012 z 21 listopada 2012 r.) do zbioru *Rejestr gruntów i budynków* oraz kolejnego upoważnienia (nr In.1334.279.2012 z 21 listopada 2012 r.), do zbioru *Rejestr Mieszkańców*,
     - A. Ś. z Wydziału Spraw Społecznych do przetwarzania danych osobowych w zbiorze *Suwalska rodzina plus* (upoważnienie nr In.1334.24.2013 z 14 czerwca 2013 r.) oraz kolejnego upoważnienia (nr In.1334.46.2014 z 17 czerwca 2014 r.), do zbioru danych *Program pomocy rodzinom wielodzietnym – Karta Dużej Rodziny*,
     - I. S. z Wydziału Inwestycji (upoważnienie nr In.1334.251.2012 z 14 maja 2012 r.) do zbioru *Rejestru gruntów i budynków*,
     - A. G.-K. z Wydziału Geodezji, Gospodarki Nieruchomościami i Rolnictwa (upoważnienie nr In.1334.41.2013 z 16 września 2013 r.) do zbioru *Podatki lokalne Miasta Suwałki*.

       ABI wyjaśnił, że po objęciu stanowiska postanowił stworzyć od nowa ewidencję osób upoważnionych do przetwarzania danych osobowych w Urzędzie. Prezydent wystąpił do naczelników wydziałów o aktualizację wszystkich

[36] 5 grudnia 2017 r. Ewidencja Osób Upoważnionych liczyła 737 pozycji.
[37] Analizę przeprowadzono na próbie 32 pracowników Urzędu.

upoważnień i złożenie nowych wniosków, celem nadania nowych upoważnień i umieszczenia w tej ewidencji. W piśmie Prezydenta zawarte zostało, że w miejsce przedstawionych nowych wniosków o upoważnienia anulowane będą upoważnienia wydane przez poprzedniego ABI. Jeśli ktoś nie przedstawił mu nowego upoważnienia, to ABI nie anulował poprzedniego, stąd nadal było ono w mocy. Niezgłoszenie wszystkich pracowników i wszystkich wymaganych upoważnień, ABI uważa jako przeoczenia naczelników. Upoważnienia wydane wcześniej nadal były ważne, nikt ich nie cofnął, jednak nie znalazły się w ewidencji. Naczelnicy wyjaśnili, że wynikało to z przeoczenia, z długotrwałej nieobecności w pracy jednej z osób albo z niewłaściwego zinterpretowania pisma Prezydenta w tym zakresie.

- Ewidencja Osób Upoważnionych zawierała wpisy o udzieleniu upoważnienia do zbiorów, które formalnie w tym czasie nie istniały (nie były zarejestrowane przez ABI w Rejestrze Wewnętrznym Zbiorów). Dotyczyło to dwóch upoważnień[38] do zbioru *Rządowy Program pomocy rodzinom wielodzietnym* (zarejestrowanego 5 grudnia 2017 r., podczas gdy upoważnienia wydane zostały 16 listopada 2015 r.) oraz zbioru *Ewidencja osób kierowanych na leczenie odwykowe* (zarejestrowanego 29 grudnia 2017 r., do którego 14 upoważnień[39] zostało wydanych między 9 marca 2015 r. a 6 lutego 2017 r.). ABI wyjaśnił, że pracownicy przekonywali go, że były to zbiory niewymagające rejestracji. W przypadku Karty Dużej Rodziny – argumentowano, że jest to program rządowy, a nie lokalny i rejestracji nie wymaga, w odróżnieniu do zbioru *Suwalska rodzina plus* – lokalnego programu pomocy rodzinom.

(dowód: akta kontroli str. 455-460, 463-467, 474-505, 587, 716-722, 865-866, 871-872, 922, 925-927)

4. Nie były organizowane szkolenia z zakresu bezpieczeństwa informacji, których obowiązek przeprowadzania wprowadzono § 20 ust. 2 pkt 6 rozporządzenia KRI. Naczelnik Wydziału Organizacyjnego wyjaśnił, że obowiązek jego wydziału, związany z organizacją szkoleń, rozumie jako działania organizacyjne przy wyborze szkolącego albo organizacji pracy Urzędu przy szkoleniach. Nie było sygnału z innych wydziałów, że jest potrzeba przeprowadzenia szkoleń dotyczących bezpieczeństwa informatycznego. Naczelnik Wydziału Informatyki wyjaśnił, że w ww. rozporządzeniu nie jest określone jak powinno wyglądać takie szkolenie. Wydały mu się wystarczające szkolenia w grupie kierowników – gdzie przedstawiał zakres dokumentacji dotyczący Systemu Zarządzania Bezpieczeństwem Informacji. *Później wykonane było badanie na użytkownikach – do wszystkich pracowników został wysłany email z informacją o przesyłce do odebrania z linkiem do tej przesyłki. Cztery osoby kliknęły w link i została z nimi przeprowadzona rozmowa dotycząca zagrożeń związanych z użytkowaniem poczty elektronicznej. Zapadła jednak decyzja, że szkolenia te nie są wystarczające i będziemy w przyszłości posiłkować się firmą zewnętrzną.*

(dowód: akta kontroli str. 579-603, 867-868, 880-883)

Najwyższa Izba Kontroli zwraca dodatkowo uwagę, że audytor wewnętrzny podczas swoich czynności w 2017 roku przeprowadził analizę logowania się na konta pracowników przebywających na urlopach. W ośmiu z 20 przypadków (40%) występowały logowania na konta nieobecnych pracowników, co sugeruje przekazywanie haseł dostępu współpracownikom na czas nieobecności. Jednocześnie w ankiecie przeprowadzonej wśród 40 pracowników Urzędu – 11 ankietowanych (27,5%) odpowiedziało, że zastępując współpracownika dysponuje hasłem i / lub kartą dostępu do komputera. Sytuacje te tym bardziej wskazują na konieczność przeprowadzania szkoleń z zakresu bezpieczeństwa informatycznego. (dowód: akta kontroli str. 693-697)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że do 30 czerwca 2016 r., tj. do dnia wejścia w życie zarządzenia w sprawie SZBI nie opracowano kompleksowego systemu zarządzania bezpieczeństwem. Tymczasem obowiązek opracowania tego typu dokumentów istniał

[38] Pozycje nr 244 i 248 ewidencji osób upoważnionych do przetwarzania danych osobowych.
[39] Pozycje nr 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 245 i 674 ewidencji osób upoważnionych do przetwarzania danych osobowych.

od 31 maja 2012 r., tj. od dnia wejścia w życie rozporządzenia KRI, i został zawarty w § 20 ust. 1 tego rozporządzenia. (dowód: akta kontroli str. 597-599)

Prezydent wyjaśnił, że elementy SZBI funkcjonowały w Urzędzie przed wydaniem zarządzenia w sprawie SZBI, chociaż nie wprowadzono ich w formie określonej rozporządzeniem KRI. Jako te elementy Prezydent wymienił: Politykę Bezpieczeństwa i Instrukcję Zarządzania Systemami Informatycznymi, wprowadzone zarządzeniem od 9 maja 2005 r. i zarządzenie w sprawie regulaminu przestrzegania zasad i procedur korzystania z legalnego oprogramowania oraz ochrony własności intelektualnej w Urzędzie – wprowadzone od 16 marca 2011 r.

Prezydent wymienił również szereg działań realizowanych w celu wypełnienia obowiązków wskazanych w § 20 ust. 2 rozporządzenia KRI: (1) zakup urządzenia UTM w 2009 roku, (2) prowadzenie inwentaryzacji sprzętu i oprogramowania od 2006 roku, (3) prowadzenie rejestru ryzyk od 2012 roku, (4) utworzenie sieci komputerowej Urzędu i pracę w domenie, bez uprawnień administratora przez użytkowników – od 2006 roku, (5) zawieranie w umowach serwisowych zapisów o stosowaniu bezpieczeństwa danych, (6) korzystanie z centralnego systemu antywirusowego od 2008 roku, (7) zabezpieczenie serwerów i urządzeń serwerowni przed utratą zasilania, (8) prowadzenie audytu wewnętrznego bezpieczeństwa informacji od 2013 roku.

Po wewnętrznym audycie w 2015 roku (protokół ze stycznia 2016 roku), w którym audytor zalecił sporządzenie kompleksowej dokumentacji dotyczącej systemu zarządzania bezpieczeństwem – została ona opracowana i weszła w życie.

(dowód: akta kontroli str. 873-876, 923-924)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie pomimo stwierdzonych nieprawidłowości opracowanie dokumentacji i procedur dotyczących ochrony danych osobowych.

3. Sposób przechowywania zasobów informacyjnych oraz ich zabezpieczenia

Opis stanu faktycznego

3.1. Polityka Bezpieczeństwa określała zabezpieczenia organizacyjne i techniczne pomieszczeń Urzędu, zlokalizowanych w czterech budynkach na terenie miasta.

W budynku Urzędu przy ul. Mickiewicza 1 okna na parterze posiadały szyby antywłamaniowe, zainstalowany został system alarmowy oraz system ostrzegania pożarowego, wewnętrzny i zewnętrzny monitoring wizyjny oraz całodobowy dozór pełniony przez portierów, którzy w gablocie przechowywali klucze do pokojów budynku. Serwerownia posiadała elektroniczny zamek dostępu. W budynku przy ul. Kościuszki 45 (sąsiadujący z budynkiem przy ul. Mickiewicza 1) okna na parterze zabezpieczone były kratą, zastosowano system alarmowy połączony z centrum monitorującym. Włączanie i wyłączanie alarmu powierzono czterem uprawnionym pracownikom. W budynku przy ul. Noniewicza 71A zastosowano system alarmowy połączony z centrum monitorującym (w budynku tym mieści się m.in. siedziba Straży Miejskiej), a w budynku przy ul. Sejneńskiej 13 zastosowano całodobowy dozór. (dowód: akta kontroli 161-162, 299-305)

Oględzinom poddano 22 pomieszczenia w budynkach przy ul. Mickiewicza 1 i Kościuszki 45. W pomieszczeniach tych mieściły się Wydziały: Spraw Obywatelskich, Budżetu i Finansów, Podatków i Opłat, Komunikacji oraz Urząd Stanu Cywilnego i archiwa. Stwierdzono, że 78 szaf posiadało możliwość zamknięcia, a klucze od nich przechowywane były w portierni, w zamykanych biurkach lub sejfie. 10 szaf nie miało możliwości zamknięcia (przechowywana w nich była dokumentacja Wydziałów). Będzie o tym mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.*

W Wydziale Komunikacji dokumentacja przechowywana była na 61 regałach nieposiadających drzwi i możliwości zamknięcia, przy czym klienci Urzędu nie mieli do nich dostępu, a sprzątanie odbywało się – według oświadczenia p.o. Naczelnika Wydziału Organizacyjnego – w godzinach pracy wydziału i w obecności jego pracowników (nie było to uregulowane). Pomieszczenia były zamykane i posiadały własny system alarmowy, aktywowany przez wyznaczonych pracowników po zakończeniu pracy. Jednocześnie budynek był całodobowo monitorowany. O przechowywaniu dokumentacji w tym Wydziale oraz o archiwach zakładowych będzie mowa w dalszej części wystąpienia, w sekcji *Uwagi dotyczące badanej działalności.* (dowód: akta kontroli str. 299-305)

W rozdz. 6 § 8 ust. 2 Instrukcji Zarządzania Systemami Informatycznymi wskazano, że pomieszczenia w obszarze przetwarzania danych osobowych muszą być zamknięte na zamek w czasie nieobecności pracowników. Załącznikiem do Polityki Bezpieczeństwa była Procedura postępowania z kluczami od pomieszczeń biurowych, w których przetwarzane są dane osobowe. Regulowała ona sposób przechowywania kluczy do pomieszczeń w poszczególnych budynkach Urzędu. Nie regulowała zaś kwestii przechowywania kluczy do szaf z dokumentacją. (dowód: akta kontroli str. 156, 177)

3.2. Wydział Informatyki prowadził elektronicznie rejestr zasobów informatycznych, czyli inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującą jego rodzaj i konfigurację. Wypełniony został tym samym obowiązek wskazany w § 20 ust. 2 pkt 2 rozporządzenia KRI. (dowód: akta kontroli str. 554)

3.3. Nośniki danych nie były przekazywane do utylizacji firmom zewnętrznym. Dyski z komputerów przeznaczonych do utylizacji były pozbawiane zapisu, a następnie rozbierane i niszczone ręcznie, co było zgodne z rozdz. 14 § 17 Instrukcji Zarządzania Systemami Informatycznymi. W latach 2016 – 2017 zniszczonych zostało 36 dysków. Komputery wymagające naprawy były przekazywane bez nośników danych – zapisy takie znajdowały się w umowach o zakupie sprzętu[40]. (dowód: akta kontroli str. 159, 543-544)

3.4. Niszczenie dokumentów papierowych odbywało się przy użyciu 60 niszczarek. Sposób niszczenia dokumentów został opisany w Polityce postępowania z nośnikami, stanowiącej załącznik nr 13 do Polityki Bezpieczeństwa Informacji. (dowód: akta kontroli str. 280, 542)

3.5. Korzystanie ze sprzętu informatycznego poza Urzędem zostało omówione w załączniku nr 10 do Polityki Bezpieczeństwa Informacji. Polityka urządzeń mobilnych i telepracy wskazywała m.in. na konieczność zastosowania środków ochrony gwarantujących zabezpieczenie przed nieuprawnionym dostępem. (dowód: akta kontroli str. 276-277)

3.6. Sprzątanie pomieszczeń zostało uregulowane w Regulaminie pracy[41]. Odbywało się w godzinach 14 – 22 (do 20 października 2016 r.) i 13 – 21 (od 21 października 2016 r.). Osoby sprzątające były pracownikami Urzędu i posiadały zgody na przebywanie w obszarze przetwarzania danych osobowych. Pozostałych pracowników zobowiązano do przestrzegania zasady *czystego biurka*[42].

(dowód: akta kontroli str. 198, 597-599, 604-611)

3.7. Szczegółowe procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji zostały opisane w rozdz. 14 Instrukcji Zarządzania Systemami Informatycznymi, w której wskazano m.in., że prace zlecone podmiotom zewnętrznym wykonywane są pod nadzorem ASI, bez możliwości dostępu do danych osobowych (przedstawiono to w punkcie 3.3. wystąpienia). (dowód: akta kontroli str. 159)

3.8. Budynki Urzędu przy ul. Mickiewicza 1 i Kościuszki 45 wyposażone były w agregat prądotwórczy o mocy 85 kVa (68 kW), a wszystkie poddane oględzinom komputery również w bezprzewodowe zasilacze awaryjne (urządzenie UPS), podtrzymujące energię na wypadek braku zasilania. Układ składał się z agregatu, sterownika (SZR) i UPS-a. W przypadku braku zasilania od dostawcy prądu, urządzenie SZR uruchamiał agregat, który podtrzymywał serwerownie, ale nie cały budynek i pracujące komputery. W lokalizacji Urzędu przy ul. Sejneńskiej 13 nie było agregatu i układu sterownia. Znajdował się zaś UPS o mocy 32 kVa, który podtrzymywał serwerownię i klimatyzację. Z kolei w lokalizacji przy ul. Noniewicza 71A znajdował się awaryjny zasilacz serwera, lecz nie było tam zbiorów danych prowadzonych w systemach informatycznych, które wymagały dodatkowego źródła zasilania w przypadku braku prądu.

Załącznikiem do Polityki Bezpieczeństwa była również Procedura postępowania w przypadku zalania pomieszczeń biurowych, w których jest zlokalizowany sprzęt komputerowy przetwarzający dane. (dowód: akta kontroli str. 161-162, 176, 880-883)

---

[40] Zapis o treści: *Wymontowanie przez Zamawiającego twardego dysku nie stanowi naruszenia warunków gwarancji.*

[41] Załącznik do Zarządzenia 308/2016 Prezydenta Miasta Suwałk z dnia 7 października 2016 r. w sprawie nadania Regulaminu Pracy Urzędu Miejskiego w Suwałkach, które weszło w życie 21 października 2016 r., a wcześniej załącznik do zarządzenia nr 122/2015 Prezydenta Miasta Suwałk z dnia 27 marca 2015 r. w tej samej sprawie.

[42] § 6 Polityki Bezpieczeństwa.

3.9. Nie zdarzyło się, aby utracono dane w wyniku kradzieży nośnika, przekazania go nieuprawnionej osobie, przypadkowego skasowania lub zniszczenia.

(dowód: akta kontroli str. 880-881)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość związaną z niezabezpieczeniem dokumentacji papierowej. Dziesięć z 88 szaf (11,8%) w których przechowywana była dokumentacja w wydziałach: Podatków i Opłat oraz Budżetu i Finansów[43] nie posiadało zamków lub były one niesprawne, a w dwóch z 22 objętych oględzinami pokojów[44] dokumentacja gromadzona była na półkach niemających możliwości zamknięcia. Nie zapewniało to należytej ochrony gromadzonych dokumentów oraz było niezgodne z art. 36 ust. 1 ustawy o ochronie danych osobowych. P.o. Naczelnika Wydziału Organizacyjnego wyjaśnił, że było to niedopatrzenie z naszej strony. *Na bieżąco usuwamy obecnie usterki w zamkach. W niektórych szafkach bez zamków już zamontowaliśmy zamki. Dołożymy starań o zamykane szafki na dokumenty.*

(dowód: akta kontroli str. 299-305, 867-868)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że:

1. W pomieszczeniach archiwów: zakładowego i Urzędu Stanu Cywilnego, zlokalizowanych w podpiwniczeniu budynku przy ul. Mickiewicza 1, przy ścianach biegły rury odpływowe. W przypadku ich pęknięcia zalaniu może ulec część dokumentacji. Należałoby zatem podjąć działania, aby w przypadku powstania takiej szkody, nie miało to wpływu na zgromadzone materiały archiwalne. Naczelnik Wydziału Organizacyjnego wyjaśnił, że zasygnalizuje ten problem swojemu przełożonemu.

   (dowód: akta kontroli str. 299-305, 867-868)

2. Przechowywania dokumentacji w Wydziale Komunikacji na otwartych półkach powinno być traktowane jako rozwiązanie przejściowe. Docelowo dokumentacja tego Wydziału powinna być przechowywana w zamknięciu. (dowód: akta kontroli str. 299-305, 867-868)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie pomimo stwierdzonej nieprawidłowości działania Urzędu dotyczące przestrzegania przyjętych procedur w zakresie przechowywania i zabezpieczania danych oraz zapewnienia ich właściwej ochrony.

4. Zakres przetwarzanych danych osobowych

Opis stanu faktycznego

4.1. Według danych na dzień rozpoczęcia kontroli, Urząd posiadał w swojej ewidencji 93 zbiory danych osobowych. W trakcie kontroli wpisane do tej ewidencji były kolejne trzy zbiory, z których dwa zgłoszono również GIODO, gdyż zawierały dane wrażliwe. Przetwarzanie danych w zbiorach Urzędu odbywało się za pomocą 21 programów m.in. SIO, SmartDoc, Płatnik, Fiskus, indexel, Foris, edytora tekstowego i arkusza kalkulacyjnego oraz w formie papierowej. Wykaz zbiorów danych, będący załącznikiem nr 3 do Polityki Bezpieczeństwa, był niepełny, o czym będzie mowa w dalszej części wystąpienia, w sekcji *Ustalone nieprawidłowości.*

(dowód: akta kontroli str. 165-168, 506-528, 716-718, 770-792, 832-856)

4.2. Nie były dokonywane aktualizacje danych w rejestrze prowadzonym przez GIODO. W punkcie 2.1. wystąpienia omówiono wniosek do GIODO o wykreślenie zbiorów z rejestru.

(dowód: akta kontroli str. 506-528)

4.3. Analiza danych przetwarzanych w 16 zbiorach wykazała, że w 15 z nich były dane niezbędne do realizacji zadań, dla których je prowadzono. W jednym zbiorze gromadzono dane, do których posiadania nie obligują przepisy prawa, a w trzech kolejnych przetwarzano dane osobowe w zakresie szerszym niż wynikało to ze zgłoszeń do rejestru GIODO lub z zapisów Rejestru Wewnętrznego Zbiorów, co zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji *Ustalone nieprawidłowości.*

(dowód: akta kontroli str. 535-540)

---

[43] W pokojach nr 7, 8, 111, 213 i 214 w Wydziale Podatków i Opłat oraz w pokoju nr 147 w Wydziale Budżetu i Finansów.

[44] W pokoju nr 107 w Wydziale Budżetu i Finansów oraz w pokoju nr 213 w Wydziale Podatków i Opłat.

W latach 2016 – 2017 ogłoszonych zostało 75 ofert pracy (odpowiednio 20 i 55). Analiza losowo wybranych 23 z nich (31%) wskazała, że w każdym ogłoszeniu zamieszczona została klauzula o konieczności wyrażenia zgody na przetwarzanie danych osobowych.

(dowód: akta kontroli str. 534)

4.4. Urząd posiadał dostęp do zewnętrznych zbiorów danych, dla których Prezydent nie był administratorem. Dotyczyło to systemów: Źródło (System Rejestrów Państwowych), CEIDG (Centralna Ewidencja i Informacja o Działalności Gospodarczej), KDR (Rejestr Wniosków o Kartę Dużej Rodziny), CEPiK (dla zbioru Pojazd i Ewidencja Kierowców). W przypadku wszystkich wymienionych wyżej baz danych uzyskano dostęp dla pracowników Urzędu od administratorów tych zbiorów danych. W przypadku dostępu do Systemu Rejestrów Państwowych i CEPiK – Urząd spełnił warunki dostępu, gdyż stanowiska do ich obsługi nie miały dostępu do otwartego Internetu, a pracownicy mieli stosowne upoważnienia.

(dowód: akta kontroli str. 306-310, 716-718, 474-505)

Ustalone nieprawidłowości

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

1. Jednym z elementów polityki bezpieczeństwa, stosownie do § 4 ust. 2 rozporządzenia MSWiA, był wykaz zbiorów danych osobowych wraz ze wskazaniem programów do przetwarzania tych danych. Załącznik nr 3 do Polityki Bezpieczeństwa zawierał niepełną, w stosunku do Rejestru Wewnętrznego Zbiorów, listę zbiorów danych. Nie zawierała ona bowiem pozycji zarchiwizowanych (o których wspomniano w punkcie 2.1. wystąpienia) oraz zbiorów zamkniętych. ABI wyjaśnił, że jego zdaniem nie było potrzeby umieszczać w Polityce Bezpieczeństwa tych zbiorów, gdyż faktycznie się z nich nie korzysta. Jego zdaniem wykaz powinien być aktualny, tj. zawierać zbiory będące w użytku. Zapisy § 4 ust. 2 rozporządzenia MSWiA wskazują jednak, że wykaz powinien obejmować zbiory danych osobowych, bez względu czy są one w użytkowaniu.

   (dowód: akta kontroli str. 506-528, 793-796, 865-866)

2. W zbiorze danych *Licencje, zezwolenia, zaświadczenia na transport drogowy*, poza wymaganymi dokumentami, gromadzono kopie wydanych orzeczeń lekarskich o braku przeciwwskazań zdrowotnych do pracy na stanowisku kierowcy. Takich dokumentów nie wymieniono w art. 7a ust. 3 ustawy z dnia 6 września 2001 r. o transporcie drogowym[45]. Naczelnik Wydziału Komunikacji wyjaśniła, że wnioskujący – chociaż nie wszyscy – wraz z wnioskiem przynosili kopie wydanych orzeczeń lekarskich i pozostawiali je w aktach. Argumentowali to faktem, że podczas kontroli, którą Wydział Komunikacji musi przeprowadzić w ciągu pięciu lat od wydania licencji, mogą nie posiadać tego dokumentu przy sobie, a nawet go zgubić, a zdaniem wnioskodawców – w dokumentacji urzędowej dokument ten nie zagubi się. W trakcie kontroli NIK usunięto kopie wydanych orzeczeń lekarskich z tego zbioru danych osobowych.

   (dowód: akta kontroli str. 538, 858, 864)

3. W trzech zbiorach przetwarzano dane osobowe niewymienione (lub nieprecyzyjnie wymienione) w Rejestrze Wewnętrznym Zbiorów i zgłoszeniach do rejestru prowadzonego przez GIODO (dane te były niezbędne do realizacji zadań):
   - W zbiorze *Wykaz decyzji administracyjnych oraz wniosków z zakresu administracji architektoniczno budowlanej*[46], poza zgłoszonymi danymi gromadzono dane o rodzaju, serii i numerze dokumentu, którym legitymował się wnioskodawca dysponujący nieruchomością na cele budowlane, co wynikało załącznika do wniosku o pozwolenie na budowę[47]. Naczelnik Wydziału Architektury i Gospodarki

---

[45] Dz. U. z 2017 r. poz. 2200, ze zm.

[46] Chodzi o sprawy związane z wydaniem decyzji o pozwoleniu na budowę.

[47] Treść tego dokumentu określona była w załączniku nr 3 do rozporządzenia Ministra Infrastruktury i Rozwoju z dnia 24 lipca 2015 r. w sprawie wzorów: wniosku o pozwolenie na budowę, oświadczenia o posiadanym prawie do dysponowania nieruchomością na cele budowlane, decyzji o pozwoleniu na budowę, oraz zgłoszenia budowy i przebudowy budynku mieszkalnego jednorodzinnego (Dz. U. poz. 1146 ze zm.), a po zmianie w załączniku nr 3 do rozporządzenia Ministra Infrastruktury i Budownictwa z dnia 24 sierpnia 2016 r. w sprawie wzorów: wniosku o pozwolenie na budowę lub rozbiórkę, zgłoszenia budowy i przebudowy budynku mieszkalnego jednorodzinnego, oświadczenia o posiadanym prawie do *dysponowania nieruchomością na cele budowlane, oraz decyzji o pozwoleniu na budowę lub rozbiórkę (Dz. U. poz. 1493).

Przestrzennej wyjaśniła, że nie wiedziała, że musi podać ABI tak dokładne dane, które wynikają z przepisów prawa, bo wzór wniosku i załączników do wniosku o pozwolenie na budowę jest określony rozporządzeniem. W trakcie kontroli NIK Naczelnik zawnioskowała do ABI o doprecyzowanie zakresu przetwarzanych danych. (dowód: akta kontroli str. 506-528, 537, 869, 930)

- W zbiorach *Rejestr mężczyzn objętych rejestracją* i *Rejestr kobiet objętych rejestracją* nieprecyzyjnie wskazano jakie dane są gromadzone. Wskazano, że gromadzeniu podlegają *dane personalne, dane adresowe.* Faktycznie gromadzono dane o imieniu, nazwisku, nazwisku rodowym, imionach i nazwiskach rodziców, numerze PESEL, dacie i miejscu urodzenia, adresie zameldowania na pobyt stały lub czasowy, co wynikało z załącznika nr 1 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 17 listopada 2009 r. w sprawie rejestracji osób na potrzeby prowadzenia kwalifikacji wojskowej oraz założenia ewidencji wojskowej[48]. Naczelnik Wydziału Spraw Obywatelskich wyjaśnił, że uważał, że skoro w przepisach szczegółowych doprecyzowane jest, które dane gromadzone są w związku z prowadzeniem ww. rejestrów, to nie wyliczał tych danych we wnioskach o rejestrację zbiorów. W trakcie kontroli NIK Naczelnik złożył do ABI wniosek o doprecyzowanie zakresu przetwarzanych danych.
(dowód: akta kontroli str. 506-528, 539-540, 754-755, 870, 929)

Niezgłoszenie powyższych danych do zbiorów stanowiło naruszenie art. 41 ust. 1 pkt 3a ustawy o ochronie danych osobowych, zgodnie z którym zgłoszenie powinno zawierać m.in. zakres przetwarzanych danych.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości sposób przetwarzania posiadanych zbiorów danych osobowych oraz spełnienie wymogów związanych z uzyskaniem dostępu do zbiorów zewnętrznych.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[49], wnosi o:

1. Bezzwłoczne odbieranie dostępu do systemów informatycznych pracownikom kończącym zatrudnienie w Urzędzie.
2. Rzetelne prowadzenie Ewidencji Osób Upoważnionych, zgodnie z art. 39 ust. 1 ustawy o ochronie danych osobowych.
3. Rzetelne prowadzenie Rejestru Wewnętrznego Zbiorów, w szczególności w zakresie przetwarzanych informacji, zgodnie z art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych.
4. Prowadzenie szkoleń, o których mówi w § 20 ust. 2 pkt 6 rozporządzenia KRI.
5. Zapewnienie bezpieczeństwa przechowywanej dokumentacji papierowej, stosownie do art. 36 ust. 1 ustawy o ochronie danych osobowych.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden kierownikowi 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 Delegatury NIK w Białymstoku.

---

[48] Dz. U z 2015 r. poz. 991.

[49] Dz. U. z 2017 r. poz. 524. Ustawa zwana dalej *ustawą o NIK.*

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK, proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i 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.

Białystok, 26 lutego 2018 r.

Kontroler
Wojciech Zambrzycki
starszy inspektor kontroli państwowej

.....
podpis

DYREKTOR DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
z up. WICEDYREKTOR
Robert Skwarko

.....
podpis