LBI.430.002.2018
Nr. ewid. 100/2018/P/17/062/LBI

Informacja o wynikach kontroli

BEZPIECZEŃSTWO ELEKTRONICZNYCH ZASOBÓW INFORMACYJNYCH W JEDNOSTKACH SAMORZĄDU TERYTORIALNEGO W WOJEWÓDZTWIE PODLASKIM

DELEGATURA W BIAŁYMSTOKU

MISJĄ

Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

WIZJĄ

Najwyższej Izby Kontroli jest cieszący się powszechnym autorytetem najwyższy organ kontroli państwowej, którego raporty będą oczekiwanym i poszukiwanym źródłem informacji dla organów władzy i społeczeństwa

Informacja o wynikach kontroli

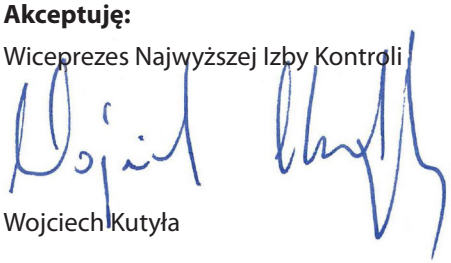
Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w Województwie Podlaskim

Dyrektor Delegatury NIK w Białymstoku

Barbara Chilińska

Akceptuję:

Wiceprezes Najwyższej Izby Kontroli



Wojciech Kutyła

Zatwierdzam:

Prezes Najwyższej Izby Kontroli

Krzysztof Kwiatkowski

Warszawa, dnia 18.07.2018 r.

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00

www.nik.gov.pl

SPIS TREŚCI

Wykaz stosowanych skrótów, skrótowców i pojęć

ABI	administrator bezpieczeństwa informacji – osoba, o której mowa w art. 36a ust. 1 ustawy o ochronie danych osobowych, powołana przez administratora danych osobowych do wykonywania zadań związanych z zapewnieniem przestrzegania przepisów o ochronie danych osobowych (od 25 maja 2018 r. inspektor ochrony danych);
ADO	administrator danych osobowych – organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych;
ASI	administrator systemów informatycznych – osoba sprawująca kontrolę nad przestrzeganiem zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych;
GIODO	Generalny Inspektor Ochrony Danych Osobowych (od 25 maja 2018 r. Prezes Urzędu Ochrony Danych Osobowych);
GOPS	gminny ośrodek pomocy społecznej;
instrukcja zarządzania systemem informatycznym	dokument, o którym mowa w § 3 i § 5 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, opisujący środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych;
jednostka	starostwo, urząd gminy lub gminny ośrodek pomocy społecznej;
j.s.t.	jednostka samorządu terytorialnego;
MOPS	miejski ośrodek pomocy społecznej;
MGOPS	miejsko-gminny ośrodek pomocy społecznej;
MOPR	miejski ośrodek pomocy rodzinie;
nowa ustawa o ochronie danych osobowych	ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000);
OPS	ośrodek pomocy społecznej;
podręcznik kontroli systemów IT	podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli, opracowany przez INTOSAI Working Group on IT Audit (WGITA), zatwierdzony przez XXI Międzynarodowy Kongres Najwyższych Organów Kontroli w Pekinie, październik 2013 r.;
polityka bezpieczeństwa	dokument, o którym mowa w § 3 i § 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, opisujący zasady ochrony danych osobowych;
polityka bezpieczeństwa informacji	dokument, o którym mowa w § 2 pkt 15 rozporządzenia KRI, stanowiący zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania;
PUODO	Prezes Urzędu Ochrony Danych Osobowych;

rozporządzenie KRI	rozporządzenie 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 (Dz. U. z 2017 r. poz. 2247);
RODO	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych obowiązujące od 25 maja 2018 r.) (Dz. Urz. UE L 119 z 4.05.2016, s. 1);
rozporządzenie w sprawie dokumentacji oraz warunków technicznych	rozporządzenie 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 do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);
rozporządzenie w sprawie sposobu prowadzenia rejestru zbiorów danych	rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. poz. 719);
rozporządzenie w sprawie trybu i sposobu realizacji zadań przez administratora bezpieczeństwa informacji	rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. poz. 745);
rozporządzenie w sprawie wzoru zgłoszenia zbioru danych	rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536);
rozporządzenie w sprawie wzorów zgłoszeń administratora bezpieczeństwa informacji	rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. poz. 1934);
ustawa o informatyzacji	ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570);
ustawa o NIK	ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524, ze zm.);
ustawa o ochronie danych osobowych	ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, ze zm.);
zasób informacyjny	znajdujące się w dyspozycji j.s.t. informacje i dane, na które składają się głównie dane osobowe (wynika to ze specyfiki zadań realizowanych przez te jednostki), dane geodezyjne, dane finansowe i statystyczne oraz informacje o strukturze i zasadach organizacji i funkcjonowania tych jednostek.

1. WPROWADZENIE

Pytanie definiujące cel główny kontroli

Czy elektroniczne zasoby informacyjne w jednostkach samorządu terytorialnego są właściwie chronione?

Pytania definiujące cele szczegółowe kontroli

1. Czy przyjęte rozwiązania dotyczące dostępu do poszczególnych systemów informatycznych i usług sieciowych zabezpieczały przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych?
2. Czy opracowano wymaganą dokumentację i procedury dotyczące ochrony danych?
3. Czy sposób przechowywania oraz zabezpieczenia danych odpowiadał przepisom oraz przyjętym procedurom i zapewniał ich ochronę?
4. Czy przetwarzane dane mieściły się w ramach uprawnień wynikających z przepisów oraz zadań, do jakich jednostka została powołana?

Jednostki kontrolowane

Kontrolą objęte zostały trzy starostwa powiatowe ziemskie, 11 urzędów gmin (w tym jedno miasto na prawach powiatu) oraz 11 ośrodków pomocy społecznej (w tym jeden w mieście na prawach powiatu) z terenu województwa podlaskiego

Okres objęty kontrolą

Od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych. Badania kontrolne dotyczyły działań sprzed tego okresu, jeśli mały związek z zagadnieniami będącymi przedmiotem kontroli.

Szybki rozwój informatyzacji, obejmujący także jednostki samorządu terytorialnego, w których w coraz większym stopniu wykorzystywane są systemy teleinformatyczne, niesie ze sobą zagrożenia związane z bezpieczeństwem informacji. Zagrożenia te można opisać za pomocą trzech podstawowych zagadnień składających się na bezpieczeństwo informacji, tj. utrata poufności, ograniczenie dostępności oraz naruszenie integralności informacji. Każde z nich może mieć charakter zdarzenia przypadkowego takiego jak awaria, błąd oprogramowania lub pomyłka ludzka, może być powodowane przez czynniki naturalne np.: pożar, powódź, wyładowania atmosferyczne, a także wynikać z celowych działań ludzi.

Na przestrzeni lat zauważamy wyraźną zmianę dotyczącą zagrożeń związanych z bezpieczeństwem informacji. W przeszłości dotyczyły one głównie awarii sprzętu, błędów oprogramowania, zakłócenia łączności oraz wirusów. Obecnie daje się zauważyć coraz bardziej celowe i wyrafinowane ataki na systemy informatyczne. Coraz częściej łączą one wiele elementów technicznych i socjotechnik oraz bardzo często polegają na długotrwałym i ostrożnym sondowaniu sieci organizacji. Atakujący penetrują serwery i stacje robocze ofiary na długo przed tym, jak zaczynają wykradać dane lub zachowywać się agresywnie. Tak przeprowadzony atak ma charakter strategiczny, a nie taktyczny i może spowodować znacznie większe szkody[1].

Zmianie w ostatnich kilku latach uległ również cel ataku. Jeszcze kilka lat temu celem cyberprzestępców byli głównie indywidualni użytkownicy. Teraz większość ataków jest wymierzona w przedsiębiorstwa i instytucje, które dysponują większymi środkami finansowymi i danymi wrażliwymi[2].

W ocenie ekspertów z dziedziny cyberbezpieczeństwa rok 2017 był rekordowy pod względem aktywności cyberprzestępców na całym świecie, stosujących głównie ataki typu *ransomware*, tj. zagrożeń, które blokują dostęp do urządzenia lub danych na nim zgromadzonych, żądając okupu za ich przywrócenie. W 2018 roku zaobserwowano trzy fale ataków, które dotknęły wielkie i małe firmy, ale również samodzielnych użytkowników, gdzie złośliwy kod sam się przemieszczał między komputerami i sprawił dzięki temu szkody na dużą skalę. Prognozy na 2018 rok wskazują, że ataki te będą się nasilać, a także pojawią się nowe typy wirusów i sposoby hakerów. Prawdziwym zagrożeniem mogą być ataki typu *data sabotage*, które polegają na włamaniu się do instytucji i długotrwałym modyfikowaniu danych, czego skutkiem jest brak możliwości ich odtworzenia. Eksperci podają tu przykład rejestru PESEL, gdzie po zmienieniu danych, ich odtworzenie jest w praktyce niemożliwe. W roku 2018 prognozowany jest także wzrost ataków skierowanych na urządzenia mobilne i nowe rozwiązania z zakresu Internetu. Wymienia się tu środowisko obejmujące pojazdy, urządzenia medyczne, a także nowe aplikacje, które bardzo często

[1] Tego powinieneś się bać – 12 największych cyberzagrożeń w 2017, http://interaktywnie.com/biznes/newsy/bezpieczenstwo/tego-powinienes-sie-bac-12-najwiekszych-cyberzagrozen-w-2017-254647, dostęp z dnia 5 października 2017 r.

[2] Wzrost liczby ataków ransomware o 748% w 2016 roku, http://itfocus.pl/dzial-it/bezpieczenstwo/wzrost-liczby-atakow-ransomware-o-748-w-2016-r/, dostęp z dnia 5 października 2017 r.

nie mają gwarancji bezpieczeństwa. Światowi analitycy podkreślają, że globalne straty związane z cyberprzestępczością z roku na rok są coraz większe. Obecnie szacowane są na 500 mld dolarów[3].

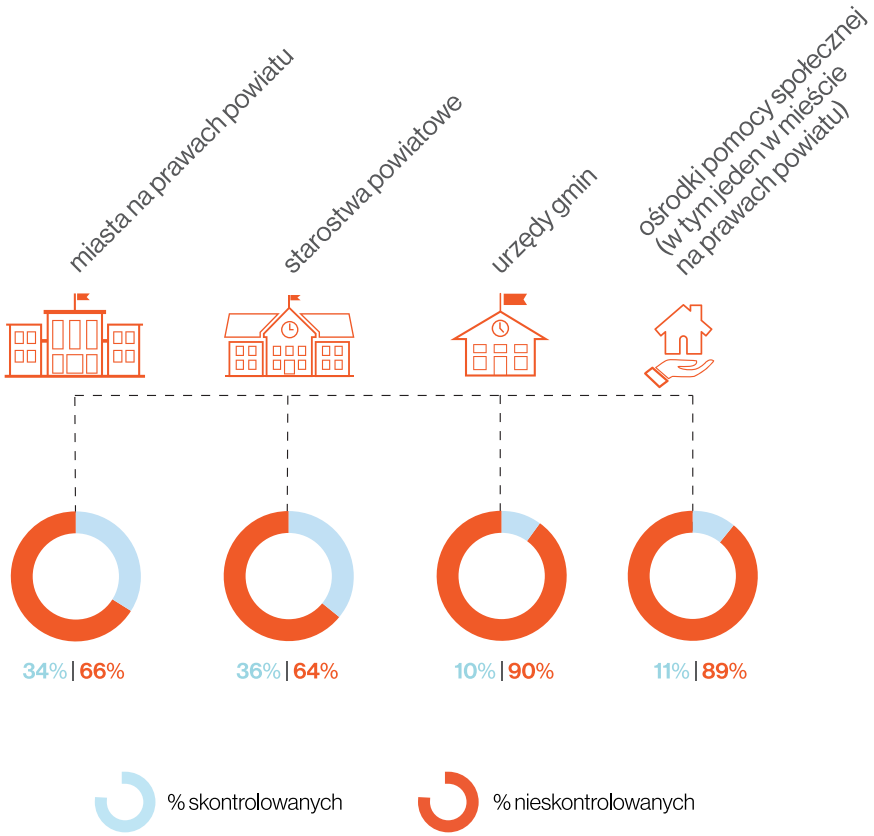
W obliczu takich zagrożeń istotnym staje się właściwe zabezpieczenie posiadanych baz danych, m.in. poprzez regularne tworzenie kopii danych, które można w pełni przywrócić w przypadku zaistnienia takiego ataku oraz posiadanie aktualnego oprogramowania antywirusowego. Ważnym elementem jest również odpowiednia konfiguracja wykorzystywanych systemów, która zapobiegnie lub utrudni rozprzestrzenianie się złośliwego oprogramowania. Należy zwrócić szczególną uwagę na sposób zarządzania uprawnieniami w dostępie do plików systemowych oraz konfiguracyjnych urządzeń. Dotyczy to zarówno osób administrujących systemami (informatycy bądź ASI), jak również pracujących na stanowiskach merytorycznych. To od ich poziomu wiedzy, nadanych im uprawnień oraz świadomości istniejących zagrożeń w dużej mierze zależy skuteczność przyjętych rozwiązań. Ważną kwestią staje się zatem posiadanie bieżących informacji o poszczególnych użytkownikach systemu i zakresie, w jakim mają oni do niego dostęp oraz danych na temat wykorzystywanego sprzętu i jego konfiguracji. Niezbędnym staje się również zapewnienie odpowiedniego systemu szkoleń, pozwalających na bieżące utrzymywanie wiedzy w dynamicznie rozwijającym się sektorze informatycznym. Świadoma zagrożeń kadra pracownicza powinna być priorytetem każdej polityki bezpieczeństwa w cyberprzestrzeni i każdego systemu cyberbezpieczeństwa.

Kontrolę NIK przeprowadzono w 25 jednostkach z terenu województwa podlaskiego, tj. w trzech starostwach powiatowych, w 11 urzędach gmin (w tym w jednym mieście na prawach powiatu) oraz w 11 ośrodkach pomocy społecznej (w tym w jednym w mieście na prawach powiatu). W niniejszej Informacji wykorzystano również ustalenia z kontroli rozpoznawczej, przeprowadzonej od stycznia do kwietnia 2017 r. w sześciu j.s.t. (dwóch starostwach powiatowych, dwóch gminach oraz dwóch ośrodkach pomocy społecznej) z województwa podlaskiego4. Kontrolą objętych zostało zatem 14% j.s.t. z województwa podlaskiego.

[3] W 2018 r. nowe, innowacyjne ataki hakerów, https://www.polskieradio.pl/42/273/Artykul/1992245,W-2018-r-nowe-innowacyjne-ataki-hakerow, dostęp z dnia 20 marca 2018 r.

[4] Kontrola R/17/001 *„Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim"*.

Infografika nr 1
Liczba i rodzaj jednostek objętych kontrolą



Źródło: Opracowanie własne na podstawie wyników kontroli NIK oraz danych GUS dotyczących liczby jednostek samorządu terytorialnego w województwie podlaskim.

W 31 objętych kontrolami j.s.t. sprawdzono głównie: [1] przyjęte rozwiązania dotyczące zabezpieczenia dostępu do poszczególnych systemów informatycznych i usług sieciowych, [2] opracowanie dokumentacji i procedur dotyczących ochrony danych, [3] sposób przechowywania oraz zabezpieczenia danych, [4] zakres przetwarzanych danych.

W ramach kontroli badaniami objęto również sposób realizacji zadań wynikających z przepisów obowiązującej do 25 maja 2018 r. ustawy o ochronie danych osobowych. Uwagę zwrócono także, czy jednostki podejmowały działania, aby przygotować się na wejście w życie RODO z dniem 25 maja 2018 r.

2. OCENA OGÓLNA

Najwyższa Izba Kontroli negatywnie ocenia ochronę elektronicznych zasobów informacyjnych w skontrolowanych starostwach, urzędach gmin i ośrodkach pomocy społecznej z województwa podlaskiego. Podejmowane przez nie działania stały bowiem często w sprzeczności z regulacjami dotyczącymi bezpieczeństwa informacji, zawartymi w rozporządzeniu KRI i nie gwarantowały zabezpieczenia tych zasobów przed nieuprawnionym dostępem, przejęciem lub zniszczeniem.

Nie zapewniono właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem

Wprawdzie we wszystkich jednostkach opracowano wymaganą dokumentację i procedury dotyczące ochrony danych, to dokumenty te w 22 (z 31) podmiotach były nieaktualne (nie były aktualizowane nawet przez ponad 10 lat) lub niekompletne. Nie spełniały zatem wymogów określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne do przetwarzania danych osobowych.

Dokumentację i procedury ochrony danych posiadały wszystkie jednostki, lecz w 2/3 z nich była ona nieaktualna lub niekompletna

W 19 jednostkach (61%) przyjęty sposób przechowywania oraz zabezpieczenia danych nie odpowiadał przepisom oraz przyjętym procedurom, przez co nie zapewniał im właściwej ochrony. W podmiotach tych nie sporządzano lub w niewłaściwy sposób tworzono kopie bezpieczeństwa baz danych, a nośniki, na których zapisywano kopie oraz urządzenia przechowywano w sposób niegwarantujący im bezpieczeństwa. Niemal we wszystkich podmiotach nie monitorowano dostępu do informacji, a w ponad połowie pracownikom nadano uprawnienia administratora systemów operacyjnych wykorzystywanych przez nich komputerów. Z kolei w ponad $^{1}/_{3}$ jednostek nie zapewniono środków uniemożliwiających nieautoryzowany dostęp do danych elektronicznych.

W ponad połowie jednostek sposób przechowywania oraz zabezpieczenia danych nie zapewniał im właściwej ochrony

Systemy informatyczne nie były zabezpieczone przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych

Większość danych przetwarzanych w jednostkach mieściła się w ramach uprawnień wynikających z przepisów oraz zadań, do jakich zostały one powołane. Niemniej w siedmiu z nich gromadzono dane osobowe, których przetwarzanie nie było niezbędne do realizacji zadań, dla których zbiory te były prowadzone (w trzech jednostkach były to dane wrażliwe, dotyczące m.in. stanu zdrowia).

W siedmiu jednostkach gromadzono dane osobowe, których przetwarzanie nie było niezbędne do realizacji zadań, dla których zbiory te były prowadzone

Jednostki nie wywiązywały się także z obowiązków określonych w ustawie o ochronie danych osobowych. Dotyczyło to głównie nieaktualizowania danych o zbiorach już zarejestrowanych w GIODO, niezgłaszania do tego rejestru nowych zbiorów oraz niewydawania pracownikom upoważnień do przetwarzania danych osobowych. Swoich obowiązków nie realizowało również aż dziewięciu z 13 Administratorów Bezpieczeństwa Informacji.

Jednostki nie przestrzegały przepisów o ochronie danych osobowych

Przyczyną powstania nieprawidłowości była marginalizacja przez kontrolowane jednostki zadań związanych z zapewnieniem bezpieczeństwa informacji i ochrony przetwarzanych danych osobowych, a w opinii kierowników tych jednostek, również brak środków na szkolenia i zakup nowej infrastruktury oraz brak w małych miejscowościach kadry posiadającej odpowiednie kwalifikacje.

Skala i istotność stwierdzonych nieprawidłowości rodzi uzasadnione obawy, co do przygotowania jednostek objętych kontrolą do wdrożenia regulacji przewidzianych w nowej ustawie o ochronie danych osobowych oraz rozporządzeniu 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), które weszły w życie 25 maja 2018 r.

Liczne i istotne nieprawidłowości rodzą obawy co do przygotowania jednostek do wdrożenia RODO

3. SYNTEZA WYNIKÓW KONTROLI

Niekompletna i nieaktualna dokumentacja opisująca przetwarzanie danych

We wszystkich 31 skontrolowanych jednostkach opracowano wymaganą dokumentację i procedury dotyczące ochrony danych, określone w § 3 rozporządzenia w sprawie dokumentacji oraz warunków technicznych. W 22 z nich dokumentacja ta była jednak niekompletna, tj. nie spełniała wymogów określonych w rozporządzeniu w sprawie dokumentacji i warunków technicznych lub była nieaktualna (nawet od 10 lat). Obowiązek dostosowania tych regulacji do zmian na przykład w strukturze organizacji jednostki lub jej otoczeniu wynika z § 20 ust. 2 pkt 1 rozporządzenia KRI. [str. 17–18]

Jedynie siedem z 31 jednostek posiadało politykę bezpieczeństwa informacji, wymaganą od 31 maja 2012 r. przepisem § 20 ust. 1 rozporządzenia KRI. Brak takich regulacji wyjaśniano w jednostkach głównie brakiem wiedzy o konieczności ich opracowania oraz nieposiadaniem odpowiednich kompetencji do podjęcia tych działań. [str. 17–18]

Nieprzeprowadzanie audytów bezpieczeństwa informacji

Aż w 26 (z 31) skontrolowanych jednostkach nie przeprowadzono audytów wewnętrznych z zakresu bezpieczeństwa informacji, chociaż wymóg corocznego ich przeprowadzania – określony w § 20 ust. 2 pkt 14 rozporządzenia KRI – wszedł w życie już 31 maja 2012 r. W dwóch kolejnych jednostkach audyt po raz pierwszy przeprowadzono w 2017 roku, tj. z pięcioletnim opóźnieniem. W rezultacie kierownicy jednostek nie dysponowali rzetelną oceną skuteczności przyjętych rozwiązań w zakresie ochrony danych. [str. 18–19]

Brak szkoleń

W 23 (z 31) jednostkach objętych kontrolą, wbrew przepisom § 20 ust. 2 pkt 6 rozporządzenia KRI, nie zapewniono szkoleń wszystkim osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo. Powodem nieorganizowania szkoleń był głównie brak środków finansowych na ten cel. Jedynie w sześciu jednostkach wybrani pracownicy (głównie ABI) w latach 2017 i 2018 wzięli udział w szkoleniach, których tematyka dotyczyła zmian w przepisach o ochronie danych osobowych, wprowadzanych 25 maja 2018 r., w związku z wejściem w życie RODO. Biorąc pod uwagę skalę nieprawidłowości stwierdzonych w wyniku kontroli, brak tych szkoleń rodzi uzasadnione obawy, co do przygotowania jednostek objętych kontrolą do wdrożenia nowych regulacji. [str. 20, 43]

Nieprowadzenie analiz ryzyka w zakresie bezpieczeństwa

W 19 (z 31) skontrolowanych jednostkach, mimo obowiązku wynikającego z § 20 ust. 2 pkt 3 rozporządzenia KRI, nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji bądź zostały one przeprowadzone po raz pierwszy dopiero w 2017 r. Nie posiadano zatem bieżących informacji o występujących ryzykach w zakresie bezpieczeństwa. Podawanymi w jednostkach powodami nieprzeprowadzania analiz były głównie brak wiedzy, jak taka analiza powinna być przeprowadzona oraz brak czasu, wynikający z wykonywania innych obowiązków służbowych. [str. 22–23]

Niemonitorowanie dostępu do systemów informatycznych

Jedynie w jednej z 31 skontrolowanych jednostek prowadzono elektroniczny rejestr dostępu do systemów informatycznych. Informacje z dziennika systemu były przetwarzane automatycznie i na bieżąco analizowane.

Zapewniono im także właściwy okres przechowywania, co – w sytuacji niepożądanej z punktu widzenia bezpieczeństwa danych – dawało duże prawdopodobieństwo ustalenia sprawcy lub źródła zagrożenia. Powodem niezapewnienia pełnego i bieżącego monitorowania dostępu do systemów w pozostałych 30 jednostkach – które w myśl § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI jest jednym z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami – był głównie brak środków finansowych na zakup nowej infrastruktury i zatrudnienie osób o odpowiednich kwalifikacjach informatycznych oraz brak szkoleń. [str. 25–26]

Nadawanie nadmiernych uprawnień w systemach informatycznych

W 18 (z 31) skontrolowanych jednostkach pracownikom zaangażowanym w proces przetwarzania danych nadano uprawnienia administratora systemu operacyjnego wykorzystywanych przez nich komputerów, tj. wykraczające poza zadania wynikające z ich zakresów obowiązków (w siedmiu jednostkach uprawnienia takie posiadali wszyscy pracownicy wykorzystujący sprzęt komputerowy). Umożliwiono im zatem pełny dostęp do zasobów oraz konfiguracji użytkowanych komputerów. Posiadali oni możliwość ściągana aplikacji i plików wykonywalnych oraz ich instalacji. Taka sytuacja narusza wymogi § 20 ust. 2 pkt 4 rozporządzenia KRI i stwarza ryzyko obniżenia skuteczności ochrony przetwarzanych danych oraz zainstalowania na komputerze złośliwego oprogramowania, umożliwiającego penetrację systemu informatycznego. Główną przyczyną nieprawidłowości było niezatrudnianie informatyków w tych jednostkach. [str. 23–24]

Nieodbieranie uprawnień w systemach informatycznych

W ośmiu (z 31) jednostkach stwierdzono nieprawidłowości, polegające na nieodebraniu (lub odbieraniu z opóźnieniem) byłym pracownikom uprawnień w systemach informatycznych. Stanowiło to naruszenie obowiązku wynikającego z § 20 ust. 2 pkt 5 rozporządzenia KRI. Osoby odpowiedzialne za zarządzanie uprawnieniami, jako powód tej sytuacji wskazywały głównie przeoczenie spowodowane nadmiarem innych obowiązków. [str. 24]

Brak zabezpieczenia przed nieautoryzowanym dostępem

W 12 (z 31) jednostkach nie zapewniono środków uniemożliwiających nieautoryzowany dostęp do informacji, naruszając w ten sposób dyspozycję § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI. Polegało to głównie na braku wymogu uwierzytelniania hasłem przy logowaniu się do systemów operacyjnych, wprowadzeniu haseł o złożoności nieodpowiadającej wymaganiom określonym w rozporządzeniu w sprawie dokumentacji oraz warunków technicznych, dla wysokiego poziomu bezpieczeństwa. W jednym zaś z ośrodków pomocy społecznej niewłaściwie zabezpieczono też dostęp do sieci bezprzewodowej, pozwalając na anonimowy dostęp osób z zewnątrz do sieci wewnętrznej jednostki. [str. 24–25]

Brak odpowiedniego nadzoru nad zdalnym dostępem do zasobów

W 14 (z 31) jednostkach umożliwiono zdalny dostęp do zasobów informatycznych z wykorzystaniem aplikacji pulpitu zdalnego, z której korzystali pracownicy firm zewnętrznych podczas realizacji prac serwisowych. Dostęp taki następował bez autoryzacji i nadzoru ze strony osób odpowiedzialnych za bezpieczeństwo systemów informatycznych. Przy połącze-

niach tego typu wykorzystywano konta i uprawnienia (w systemach informatycznych) nadane poszczególnym pracownikom, którzy byli zalogowani w chwili nawiązania połączenia z wykorzystaniem ww. aplikacji. Stanowiło to naruszenie obowiązku wynikającego z § 20 ust. 2 pkt. 7 lit. a rozporządzenia KRI. [str. 25–26]

Brak regulacji dotyczących bezpieczeństwa poczty elektronicznej

Siedem (z 31) jednostek, mimo obowiązku wynikającego z § 20 ust. 2 pkt 9 rozporządzenia KRI, w umowach na świadczenie usług poczty elektronicznej nie zamieściło zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym bądź umów takich nie zawarło (korzystano wówczas z kont pocztowych umieszczonych na ogólnodostępnych serwerach komercyjnych, wykorzystywanych także do celów prywatnych). [str. 26–27]

Wykorzystywanie systemów operacyjnych nieposiadających wsparcia producenta

W 18 (z 31) jednostkach wykorzystywano systemy operacyjne, dla których producent zakończył udzielanie wsparcia technicznego, a wiec nie były publikowane nowe aktualizacje bezpieczeństwa tych systemów. Komputery te stanowiły od 4% do 43% ogółu komputerów w poszczególnych jednostkach. Stanowiło to zagrożenie dla bezpieczeństwa sieci jednostek, w których wykorzystywano takie oprogramowanie. Użytkowanie przestarzałego oprogramowania było uzasadniane głównie brakiem środków na zakup nowego. W dwóch jednostkach z kolei nie aktualizowano systemów operacyjnych, mimo posiadania takiej możliwości. Było to sprzeczne z § 20 ust. 2 pkt 12 lit. a rozporządzenia KRI. [str. 27–28]

Nieodpowiednie zabezpieczenie zbiorów danych i infrastruktury informatycznej

W dziewięciu (z 31) jednostkach nie podjęto działań minimalizujących ryzyko kradzieży informacji i środków przetwarzania informacji. Brak było bowiem odpowiedniej ochrony fizycznej infrastruktury informatycznej wykorzystywanej do przetwarzania danych. Urządzenia typu: router, switch bądź dysk zawierający kopie bezpieczeństwa baz danych znajdowały się w miejscach ogólnodostępnych. W 15 jednostkach posiadanym zbiorom danych osobowych nie zapewniono zaś właściwego zabezpieczenia przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem[5]. Dokumentację zawierającą dane osobowe przechowywano na przykład w pomieszczeniach bez odpowiedniego wyposażenia i miejscach nieposiadających możliwości zamknięcia. Naruszono w ten sposób wymogi art. 36 ust. 1 ustawy o ochronie danych osobowych. [str. 29–31]

W 19 jednostkach nie sporządzano lub w niewłaściwy sposób tworzono i przechowywano kopie bezpieczeństwa baz danych. W 11 z nich nie wszystkie bazy danych były poddawane regularnemu procesowi tworzenia kopii, a w kolejnych ośmiu kopie były przechowywane w sposób niegwarantujący bezpieczeństwa (umieszczano je na urządzaniach, w których znajdowały się dane podlegające procesowi tworzenia kopii bądź nośniki zawierające kopie przetrzymywano w tych samych pomieszczeniach co baza danych). Stanowiło to naruszenie prze-

[5] Od 25 maja 2018 r. wymogi ochrony danych osobowych określa art. 32 RODO.

pisu cz. A pkt IV ust. 4 lit. a załącznika do rozporządzenia w sprawie dokumentacji oraz warunków technicznych oraz dyspozycji § 20 ust. 2 pkt 12b rozporządzenia KRI. Powodami były m.in. brak odpowiedniej liczby aplikacji wykonujących kopie danych oraz brak świadomości istnienia ww. zagrożeń. [str. 31–32]

Niegromadzenie bieżących informacji o posiadanym sprzęcie i oprogramowaniu

W ponad połowie jednostek (17 z 31), mimo wymogu określonego w § 20 ust. 2 pkt 2 rozporządzenia KRI, nie gromadzono bieżących informacji o posiadanym sprzęcie i oprogramowaniu służącym do przetwarzania danych, obejmujących ich rodzaj i konfigurację. Prowadzono wprawdzie ewidencję posiadanych urządzeń na potrzeby rachunkowości, ale nie zawierała ona pełnych danych o sprzęcie, programach i ich konfiguracji. Nieprowadzenie takich działań uzasadniano m.in.: brakiem wiedzy o istnieniu takiego obowiązku, nieposiadaniem odpowiednich umiejętności do zebrania i usystematyzowania danych, założeniem, że obowiązek ten nie musi być spełniony z uwagi na niewielką liczbę posiadanego sprzętu. [str. 32–33]

Brak regulacji dotyczących odtwarzania utraconych zasobów

W 19 (z 31) jednostkach nie opracowano planu ciągłości działania (odtworzenia utraconych zasobów), niezbędnego do przywrócenia utraconych aplikacji o znaczeniu krytycznym. Powinien on określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. [str. 33–35]

Niezapewnienie bezpieczeństwa informacji w ośrodkach pomocy społecznej

Szczególnie niepokojącym zjawiskiem jest niezapewnienie odpowiedniego poziomu bezpieczeństwa danym zgromadzonym we wszystkich 13 skontrolowanych ośrodkach pomocy społecznej. Pomimo że dysponują one danymi wrażliwymi swoich klientów, w żadnym z nich nie ograniczono dostępu tylko do stron internetowych i narzędzi niezbędnych do realizacji zadań służbowych, w 11 pracownikom nadano uprawnienia administratora systemu operacyjnego wykorzystywanych przez nich komputerów, chociaż wykraczało to poza zakres realizowanych zadań, jaki wynikał z ich zakresów obowiązków, w dziewięciu nie przeprowadzano okresowych szkoleń, w siedmiu wykorzystywano systemy operacyjne, które nie posiadały wsparcia producenta i nie zapewniono właściwej autoryzacji przy logowaniu do systemów informatycznych, w sześciu niewłaściwie wykonywano i przechowywano kopie bezpieczeństwa, a w pięciu niewłaściwie zabezpieczono stacje robocze oraz systemy poczty elektronicznej przed złośliwym oprogramowaniem[6]. [str. 20, 23–33, 43–44]

Gromadzenie zbędnych danych osobowych

W siedmiu (z 31) jednostkach gromadzono dane osobowe, których przetwarzanie nie było niezbędne do realizacji zadań, dla których prowadzono zbiory danych osobowych. W trzech z nich dotyczyło to także danych wrażliwych (np.: kopie orzeczeń lekarskich o braku przeciwwskazań zdrowotnych do pracy na stanowisku kierowcy, kopie orzeczeń o potrzebie kształcenia specjalnego oraz orzeczeń o potrzebie wcześniejszego wspomagania

[6] 8 stycznia 2018 r. do wszystkich gmin w województwie podlaskim Podlaski Urząd Wojewódzki wystosował pismo, w którym zawarto zestaw wytycznych (dotyczących bezpieczeństwa informacji), jakie powinny być stosowane przez ośrodki pomocy społecznej. Jak wskazano w tym dokumencie, w ostatnich tygodniach 2017 r. wystąpiły bezpośrednie ataki cyberprzestępców na systemy IT wykorzystywane w tych jednostkach, o czym Podlaski Urząd Wojewódzki został poinformowany przez Ministerstwo Rodziny, Pracy i Polityki Społecznej.

rozwoju dziecka). Stanowiło to naruszenie art. 23 ust. 1 pkt 2 i art. 27 ust. 2 ustawy o ochronie danych osobowych, w myśl których przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, a danych wrażliwych – co do zasady jest zabronione. Za naruszenie tych zasad, przewidziane były sankcje karne określone w art. 49 tej ustawy, a obecnie w art. 107 nowej ustawy o ochronie danych osobowych. [str. 37–38]

Nierejestrowanie zbiorów danych osobowych

Dwadzieścia cztery jednostki (z 31) nie zgłosiły GIODO do zrejestrowania części prowadzonych zbiorów danych osobowych, które podlegały temu wymogowi, naruszając dyspozycję art. 40 ustawy o ochronie danych osobowych. Dotyczyło to od jednego do 17 zbiorów danych (czyli od 2% do nawet 71% prowadzonych zbiorów). Od 25 maja 2018 r. w myśl RODO obowiązek rejestracji zbiorów nie istnieje, wymagane jest natomiast prowadzenie rejestru czynności przetwarzania danych w jednostce. [str. 38–39]

Niemal we wszystkich jednostkach (28 z 31) nie wywiązywano się też z – określonego w art. 41 ust. 2 i 3 tej ustawy – obowiązku zaktualizowania w rejestrze GIODO danych dotyczących zbiorów już zarejestrowanych. Rejestr ten nie zawierał zatem aktualnych informacji o zakresie danych gromadzonych w zbiorach lub ewentualnym zaprzestaniu prowadzenia danego zbioru. W 17 przypadkach brak aktualizacji dotyczył zbiorów zawierających dane wrażliwe, o których mowa w art. 27 ustawy o ochronie danych osobowych. Od 25 maja 2018 r. są to tzw. szczególne kategorie danych osobowych, określone w art. 9 ust. 1 RODO. [str. 39–40]

Dostęp do danych osobowych bez upoważnienia

W 12 (z 31) jednostkach stwierdzono przypadki umożliwienia pracownikom dostępu i przetwarzania danych w zbiorach danych osobowych, bez upoważnienia wydanego przez ADO, wymaganego art. 37 ustawy o ochronie danych osobowych. Z reguły sytuacja taka dotyczyła od jednej do 25 osób, którym umożliwiono dostęp do kilku odrębnych zbiorów danych osobowych. Od 25 maja 2018 r. art. 29 RODO normuje obowiązki osób przetwarzających dane z upoważnienia lub na polecenie ADO, ale nie wskazuje sankcji karnych za nieprzestrzeganie tych regulacji. [str. 40]

Nierealizowanie zadań przez ABI i ADO

Dziewięciu z 13 ABI nie realizowało swoich ustawowych zadań i obowiązków wynikających z art. 36a ust. 2 ustawy o ochronie danych osobowych oraz dokumentacji wewnętrznej jednostek. Często do pełnienia tej funkcji wskazywano bowiem pracowników merytorycznych jednostek, którzy w swoich zakresach obowiązków mieli realizację innych zadań, które wykonywali w pierwszej kolejności. Od 25 maja 2018 r. RODO nie przewiduje stanowiska ABI. W jego miejsce, w myśl art. 37 tego rozporządzenia należy powołać Inspektora Ochrony Danych. [str. 40–41]

Czternastu z 18 ADO nie realizowało obowiązków określonych w art. 36a ust. 2 pkt 1 ustawy o ochronie danych osobowych, które winni wykonywać w przypadku niepowołania ABI. Nie dokonywali bowiem sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz nie nadzorowali opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych, tj. polityki bezpieczeństwa

i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Od 25 maja 2018 r. obowiązek wdrożenia, poddawania przeglądom oraz uaktualniania środków technicznych i organizacyjnych zapewniających właściwe przetwarzanie danych osobowych, określony został także w art. 24 RODO. [str. 42]

4. WNIOSKI

Starostowie, prezydenci miast, burmistrzowie, wójtowie oraz kierownicy ośrodków pomocy społecznej

W celu zapewnienia właściwej ochrony elektronicznych zasobów informacyjnych, Najwyższa Izba Kontroli uznaje za niezbędne:

1. Nadawanie pracownikom uprawnień w systemach operacyjnych komputerów w stopniu adekwatnym do realizowanych przez nich zadań.
2. Wprowadzenie odpowiedniej autoryzacji dostępu do posiadanych zasobów informatycznych, w tym podmiotom, które zdalnie uzyskują dostęp do infrastruktury jednostki, a także zawieranie w umowach z tymi podmiotami zapisów gwarantujących odpowiedni poziom bezpieczeństwa.
3. Dokonywanie aktualizacji regulacji wewnętrznych uwzględniających zmiany w strukturze jednostki, prawie oraz otoczeniu zewnętrznym.
4. Przeprowadzanie obowiązkowych, corocznych audytów bezpieczeństwa informacji oraz okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a także podejmowania działań stosownie do wyników tej analizy.
5. Monitorowanie dostępu do informacji poprzez bieżącą analizę zapisów w dziennikach systemów (logach).
6. Przeprowadzanie regularnych szkoleń osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem zagrożeń bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji.
7. Tworzenie, przechowywanie oraz testowanie kopii zapasowych posiadanych zasobów informacyjnych w celu zminimalizowania ryzyka utraty informacji.
8. Zapewnienie zabezpieczeń fizycznych infrastruktury informatycznej, uniemożliwiających dostęp osób nieuprawnionych oraz zapewniających ochronę przed skutkami zdarzeń losowych (np. pożar, powódź, wichura).
9. Wdrożenie regulacji wprowadzonych z dniem 25 maja 2018 r. przez RODO, w szczególności w zakresie zapewnienia prowadzenia rejestru czynności przetwarzania danych.
10. Zapewnienie aby osoby, które uzyskują dostęp do danych osobowych posiadały stosowne upoważniania ADO w tym zakresie.

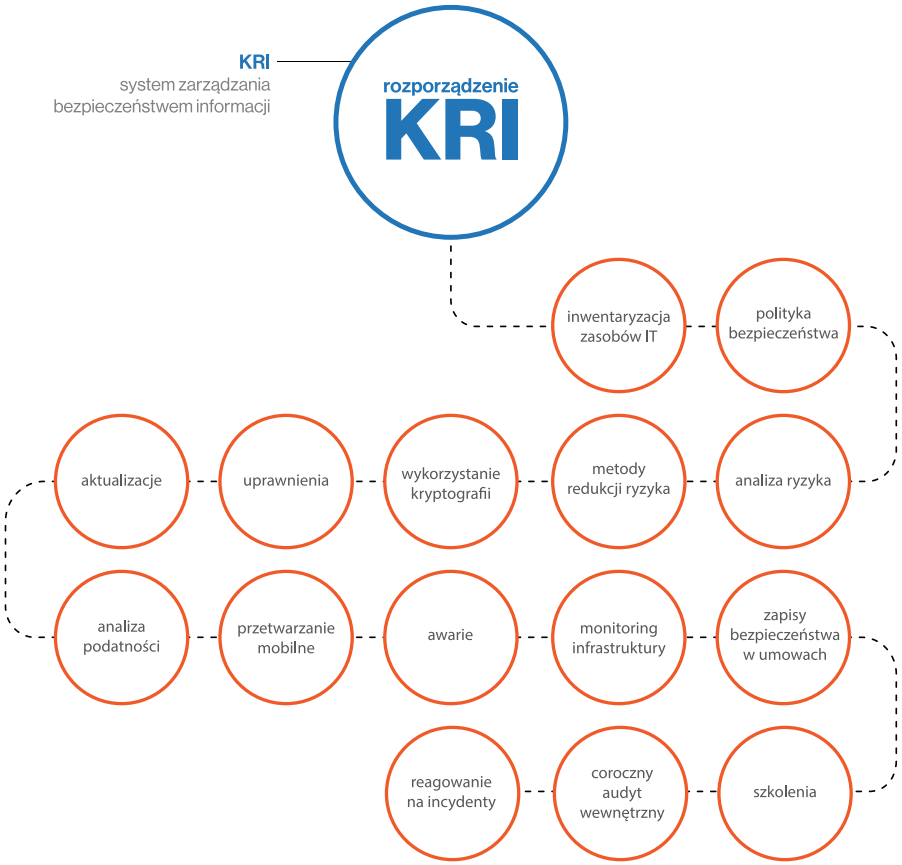
5. WAŻNIEJSZE WYNIKI KONTROLI

5.1. Dokumentacja i procedury ochrony danych

Opracowana przez wszystkie jednostki objęte kontrolą dokumentacja i procedury ochrony danych były w większości przypadków niekompletne i nieaktualne. Nie przeprowadzano także regularnych audytów wewnętrznych z zakresu bezpieczeństwa informacji, a pracownikom przetwarzającym dane nie zapewniono szkoleń z tego zakresu.

Głównym aktem prawnym określającym katalog działań dotyczących sposobu zabezpieczenia informacji jest rozporządzenie KRI. Zgodnie z nim, podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalności, niezaprzeczalność i niezawodność.

Diagram nr 1
System zarządzania bezpieczeństwem informacji określony w rozporządzeniu KRI



Źródło: Opracowanie własne NIK na podstawie przepisów rozporządzenia KRI.

W 22 jednostkach dokumentacja opisująca sposób przetwarzania danych oraz środki zapewniające ich ochronę była niekompletna lub nieaktualna

W 15[7] (z 31) jednostkach przyjęta polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym były niekompletne, tj. nie spełniały wymogów określonych w rozporządzeniu w sprawie dokumentacji i warunków technicznych lub były nieaktualne. W kolejnych siedmiu[8] jednostkach stwierdzono nieprawidłowości dotyczące jednego z ww. dokumentów. Obowiązek dostosowania tych regulacji do zmian na przykład w strukturze organizacji jednostki lub jej otoczeniu, wynika z § 20 ust. 2 pkt 1 rozporządzenia KRI.

Przykłady

W Urzędzie Miejskim w Nowogrodzie oraz Urzędzie Gminy Sidra obowiązywała polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym przyjęte w 2007 r., które przez ponad 10 lat nie były aktualizowane.

Podobnie w MOPS w Supraślu nie dokonano aktualizacji zapisów ww. dokumentacji, mimo iż taka konieczność zachodziła z uwagi na zmianę siedziby tej jednostki. W wyniku tego przez 10 miesięcy (od stycznia do grudnia 2017 r.) obowiązywała polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym, które w części były nieaktualne.

Braki w dokumentacji opisującej sposób przetwarzania danych osobowych często świadczyły o lekceważeniu wymogu posiadania rzetelnych procedur.

Przykład

Zaktualizowana w 2017 r. polityka bezpieczeństwa w Starostwie Powiatowym w Łomży nie określała wszystkich pomieszczeń, w których przetwarzano dane osobowe, nie wymieniono w niej też miejsca przechowywania wykonanych kopii danych dla jednego z systemów, co naruszało § 4 pkt 1 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Natomiast w instrukcji zarządzania systemem informatycznym nie określono okresu przechowywania kopii zapasowych zbiorów danych oraz sposobu realizacji wymogów, o których mowa w § 7 powołanego rozporządzenia, czym naruszono jego § 5 pkt 5 lit. b.

Jedynie w siedmiu jednostkach opracowano politykę bezpieczeństwa informacji

Jedynie siedem[9] z 31 jednostek posiadało politykę bezpieczeństwa informacji, wymaganą od 31 maja 2012 r. przepisem § 20 ust. 1 rozporządzenia KRI. W pozostałych przypadkach nieopracowanie takich regulacji uzasadniano brakiem odpowiednich kompetencji do ich opracowania (np. GOPS w Dobrzyniewie Dużym), brakiem wiedzy o konieczności ich opracowania (np. GOPS w Sztabinie) lub omyłkowym pominięciem tego zagadnienia w trakcie opracowywania polityki bezpieczeństwa informacji (np. Starostwo Powiatowe w Łomży).

26 jednostek nie dysponowało rzetelną oceną skuteczności przyjętych rozwiązań w zakresie ochrony danych

W 26 (z 31) skontrolowanych jednostkach nie przeprowadzono audytów wewnętrznych z zakresu bezpieczeństwa informacji, chociaż wymóg

[7] GOPS w Dobrzyniewie Dużym i Sztabinie, MGOPS w Czarnej Białostockiej i Suchowoli, MOPS w Supraślu i Zambrowie, OPS w Ciechanowcu, starostwa powiatowe w: Kolnie, Łomży i Zambrowie, urzędy gmin w: Jaświłach, Milejczycach i Sidrze, urzędy miejskie w: Nowogrodzie i Szczuczynie.

[8] GOPS w Rudce, MOPS w Siemiatyczach, Starostwo Powiatowe w Hajnówce, Urząd Gminy w Klukowie, urzędy miejskie w Kleszczelach, Michałowie i Wysokiem Mazowieckiem.

[9] GOPS w Narewce, MOPR w Suwałkach, MOPS w Supraślu, starostwa powiatowe w: Białymstoku i Zambrowie, Urząd Gminy Szudziałowo, Urząd Miejski w Bielsku Podlaskim.

corocznego ich przeprowadzania – określony w § 20 ust. 2 pkt 14 rozporządzenia KRI – wszedł w życie 31 maja 2012 r. W dwóch kolejnych jednostkach (Starostwo Powiatowe w Białymstoku i Urząd Gminy Szudziałowo) audyt po raz pierwszy przeprowadzono zaś w 2017 r., tj. pięć lat po wejściu w życie takiego obowiązku. W konsekwencji kierownicy jednostek nie dysponowali rzetelną oceną skuteczności przyjętych rozwiązań w zakresie ochrony danych. Jedynie trzy jednostki[10] corocznie wykonywały ww. audyty, w wyniku których zidentyfikowano szereg uchybień związanych z bezpieczeństwem informacji oraz wystosowano rekomendacje, dotyczące m.in.: dodania w umowach serwisowych z firmami zewnętrznymi zapisów o postępowaniu z danymi osobowymi, wyeliminowania nieścisłości i aktualizacji dokumentacji wewnętrznej, w tym określenia zasad postępowania z zewnętrznymi nośnikami danych, opracowania projektu polityki bezpieczeństwa informacji, wyodrębnienia pomieszczenia serwerowni i zamontowania w nim odpowiednich zabezpieczeń, wyeliminowania działających w sieci komputerów z systemem operacyjnym nieposiadającym wsparcia producenta, uruchomienia automatycznych aktualizacji poprawek bezpieczeństwa na wszystkich komputerach.

Przykład

W Urzędzie Miejskim w Suwałkach audyt przeprowadzony został przez audytora wewnętrznego Urzędu i obejmował lata 2016 i 2017. W jego wyniku ujawniono m.in. następujące uchybienia: [1] w prowadzonej analizie ryzyka nie został wskazany właściciel ryzyka z imienia i nazwiska, a jedynie wskazane zostało *pracownik merytoryczny*; [2] nie wprowadzono mechanizmu wymuszania okresowej zmiany hasła do sytemu informatycznego co 30 dni; [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; [4] w zakresie obowiązków jednego z pracowników Wydziału Informatyki nie został uwzględniony obowiązek prowadzenia ewidencji oprogramowania i nośników oprogramowania, chociaż wykonywał on te czynności po odchodzącym z pracy innym pracowniku Urzędu; [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, przez co nie każdy z pracowników mógł być świadomy istnienia takiego serwisu internetowego. Uchybienia te usunięto.

Podawanymi przez kierowników jednostek powodami nieprzeprowadzania audytów był brak m.in.: środków na jego sfinansowanie; pracowników posiadających odpowiednie doświadczenie i niezbędną wiedzę do jego przeprowadzenia; wymogów w zakresie sposobu, trybu realizacji oraz formy prowadzonych audytów, a także wymagań stawianych osobom, które miałyby realizować to zadanie. Inni natomiast wskazywali, że nie mieli świadomości istnienia obowiązku przeprowadzania audytu lub audyt nie był wykonywany z uwagi na nadmiar obowiązków.

[10] Urząd Gminy Jaświły, urzędy miejskie w Bielsku Podlaskim i Suwałkach.

W 23 jednostkach nie zapewniono szkoleń dotyczących bezpieczeństwa danych

Obowiązkiem kierownika jednostki – ustalonym w § 20 ust. 2 pkt 6 rozporządzenia KRI – jest zapewnienie szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo. W 23 jednostkach szkolenia takie nie były jednak przeprowadzane (10 podmiotów[11]) lub objęto nimi jedynie niewielką liczbę osób (od jednej do 36), które w ramach swoich obowiązków przetwarzały dane (13 jednostek[12]). Podawanym powodem nieorganizowania takich szkoleń były w szczególności brak: środków finansowych na ten cel, sygnałów od pracowników o potrzebie przeprowadzenia takich szkoleń, wytycznych, jak szkolenie ma zostać przeprowadzone i co powinno zawierać.

Przykład

W Urzędzie Miejskim w Suwałkach nie były organizowane szkolenia z zakresu bezpieczeństwa informacji. 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. W Urzędzie wykonano badanie polegające na przesłaniu do wszystkich pracowników wiadomości e-mail z informacją o przesyłce do odebrania z linkiem do tej przesyłki. Cztery osoby kliknęły w link i – jak poinformował Naczelnik Wydziału Informatyki – została z nimi przeprowadzona rozmowa dotycząca zagrożeń związanych z użytkowaniem poczty elektronicznej. Dodał również, że po tym badaniu zapadła decyzja, że dotychczasowe szkolenia są niewystarczające i w przyszłości Urząd będzie korzystać z usług firm zewnętrznych w tym zakresie.

Pracownicy Urzędu Miejskiego w Nowogrodzie nie uczestniczyli w szkoleniach dotyczących zagadnień związanych z ochroną danych osobowych oraz bezpieczeństwem informacji. W wyjaśnieniu Burmistrz Nowogrodu podał, że powodem były ograniczone środki na ten cel.

5.2. Skuteczność przyjętych rozwiązań dotyczących zabezpieczenia poszczególnych systemów informatycznych i usług sieciowych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem

W niemal wszystkich skontrolowanych jednostkach poziom bezpieczeństwa systemów informatycznych i usług sieciowych był na niezadowalającym lub bardzo niskim poziomie, a zasoby informacyjne nie były właściwie chronione przed nieuprawnionym dostępem, prze-

[11] MGOPS w Suchowoli, MOPS w Zambrowie, OPS w Ciechanowcu, starostwa powiatowe w: Hajnówce, Kolnie i Zambrowie, Urząd Gminy Milejczyce, urzędy miejskie w: Nowogrodzie, Suwałkach i Szepietowie.

[12] GOPS w: Boćkach, Dobrzyniewie Dużym, Rudce i Sztabinie, MGOPS w Czarnej Białostockiej i Krynkach, MOPS w Siemiatyczach i Supraślu, Starostwo Powiatowe w Łomży, Urząd Gminy Szudziałowo, urzędy miejskie w Bielsku Podlaskim, Kleszczelach i Szczuczynie.

jęciem lub zniszczeniem danych. Wynikało to z zaniechania lub podejmowania niewłaściwych działań, w wyniku których bezpieczeństwo posiadanych zasobów było narażone na duże ryzyko wystąpienia zdarzeń niepożądanych. Jedynie w Urzędzie Miejskim w Suwałkach poziom zabezpieczeń odpowiedzialnych za autoryzację dostępu do sieci wykonano profesjonalnie, zasoby informacyjne były właściwie chronione przed nieuprawnionym dostępem, kradzieżą lub utratą, a praca sieci znajdowała się pod pełną kontrolą jej administratora.

Zasoby informatyczne j.s.t.

W skontrolowanych jednostkach użytkowano od pięciu[13] do 25[14] systemów informatycznych, w których przetwarzano dane. Do ich obsługi wykorzystywano od czterech[15] do 186[16] komputerów.

Niemal na wszystkich komputerach wykorzystywanych w jednostkach objętych kontrolą umożliwiono dostęp do Internetu. Brak takiego dostępu dotyczył użytkowanych w 12 (z 13) urzędach gmin urządzeń wykorzystywanych do obsługi Systemu Rejestrów Państwowych[17]. Konieczność wprowadzenia blokady dostępu do zasobów internetowych wynikała z dokumentu: „*Wymagania dla stacji roboczych stanowisk obsługi dla użytkowników końcowych SRP*”[18]. Wyjątkiem był Urząd Gminy Milejczyce, w którym jeden z dwóch komputerów wykorzystywanych do obsługi Systemu Rejestrów Państwowych okresowo (na czas działań podejmowanych przez podmiot serwisujący) podłączano do Internetu.

Umożliwienie dostępu do Internetu na komputerach wykorzystywanych do przetwarzania danych wiązało się z koniecznością wprowadzenia wysokiego poziomu bezpieczeństwa, wynikającą z § 6 ust. 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych. Skontrolowane j.s.t. na ogół w przyjętej dokumentacji wewnętrznej dotyczącej sposobu przetwarzania danych wprowadziły wymagany poziom bezpieczeństwa. Brak uregulowań w tym zakresie został stwierdzony w pięciu[19] (z 31) jednostkach.

Przykład

W MGOPS w Czarnej Białostockiej regulacje składające się na politykę bezpieczeństwa informacji nie określały poziomu bezpieczeństwa, co Kierownik Ośrodka wyjaśniła przeoczeniem. Natomiast brak tych regulacji w polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym Urzędu Miejskiego w Michałowie, Burmistrz motywował tym, że określenie odpowiedniego poziomu bezpieczeństwa wymaga przeprowadzenia analizy ryzyka, a taka nie była przeprowadzona.

[13] GOPS w Dobrzyniewie Dużym.

[14] Urząd Miejski w Kleszczelach.

[15] GOPS w Rudce.

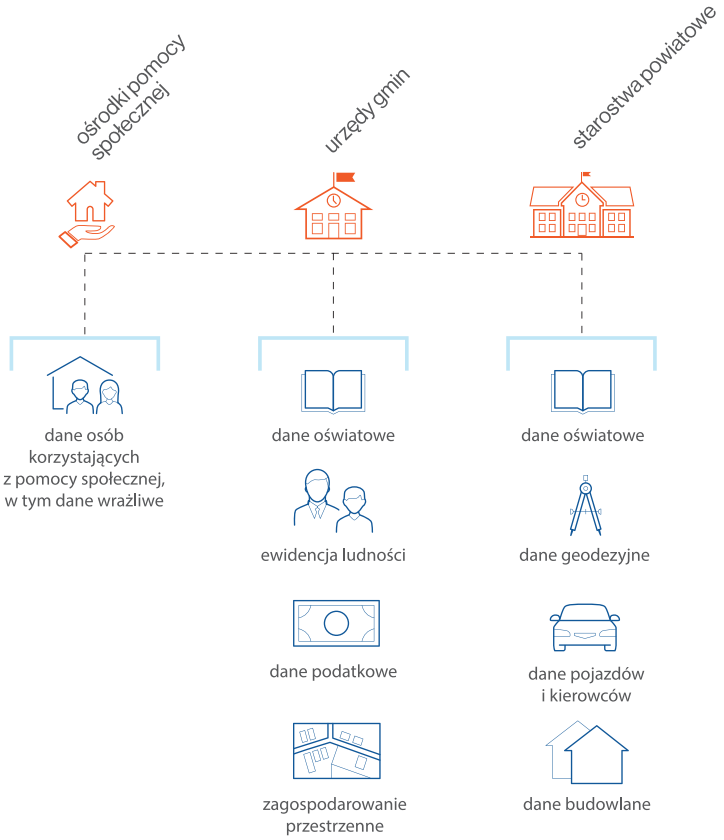
[16] Urząd Miejski w Suwałkach.

[17] System łączący pięć rejestrów: Centralny Rejestr Sprzeciwów, PESEL, Rejestr Dowodów Osobistych, Rejestr Stanu Cywilnego, System Odznaczeń Państwowych.

[18] Str. 1 pkt 1 „Wymagania sprzętowe” instrukcji: „Wymagania sprzętowe dla stacji roboczych i stanowisk obsługi dla użytkowników końcowych SRP”, opracowanej przez Centralny Ośrodek Informatyki – dokument dostępny na stronie: http://plid.obywatel.gov.pl/wp-content/uploads/2014/08/Wymagania-dla-stacji-koncowych-SRP-v-5-0.pdf.

[19] GOPS w Dobrzyniewie Dużym, MGOPS w Czarnej Białostockiej i Krynkach, Urząd Gminy w Milejczycach, Urząd Miejski w Michałowie.

Infografika nr 2
Główne rodzaje zasobów informacyjnych w poszczególnych jednostkach objętych kontrolą



Źródło: Opracowanie własne na podstawie wyników kontroli NIK.

Nieprowadzenie analizy ryzyka w zakresie bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI (obowiązującego od 31 maja 2012 r.), zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań polegających na przeprowadzaniu okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowaniu działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy. W 19[20] (z 31) skontrolowanych jednostkach nie wywiązano się z obowiązku prowadzenia takich analiz bądź zostały one przeprowadzone dopiero w 2017 r. W konsekwencji nie posiadano bieżących informacji o występujących ryzykach w zakresie bezpieczeństwa. Nieprzeprowadzanie analiz uzasadniano m.in.: brakiem wiedzy o sposobie przeprowadzenia analizy (GOPS w Sztabinie), brakiem czasu, wynikającym z wykonywania innych obowiązków służbowych (Starostwo Powiatowe w Łomży), natłokiem wielu zadań i obowiązków, w wyniku którego przeoczono konieczność przeprowadzania analizy (MOPS w Supraślu).

W 12 jednostkach, w których przeprowadzone zostały analizy ryzyka, jako główne zagrożenia bezpieczeństwa informacji wskazano m.in.: nieuprawniony dostęp oraz atak wirusa (GOPS w Dobrzyniewie Dużym,

[20] GOPS w Boćkach i Sztabinie, MGOPS w Krynkach i Suchowoli, MOPS w: Siemiatyczach, Supraślu i Zambrowie, starostwa powiatowe w Kolnie i Łomży, urzędy gminy w: Jaświłach, Klukowie, Milejczycach, Sidrze i Szudziałowie, urzędy miejskie w: Michałowie, Nowogrodzie, Szczuczynie, Szepietowie i Wysokiem Mazowieckiem.

Starostwo Powiatowe w Białymstoku); złośliwe oprogramowanie systemu operacyjnego lub aplikacji biurowych (MOPR w Suwałkach); zaniedbania pracowników i pozostawienie sprzętu bez wylogowania się, niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania danych oraz pokonanie zabezpieczeń informatycznych (OPS w Ciechanowcu).

Pracownikom nadawano nadmierne uprawnienia w systemach operacyjnych

W 18[21] (z 31) skontrolowanych jednostkach nie przestrzegano wymogu ustalonego w § 20 ust. 2 pkt 4 rozporządzenia KRI, że kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, aby osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia i uczestniczyły w tym procesie w stopniu adekwatnym do realizowanych zadań. Pracownikom zaangażowanym w proces przetwarzania danych nadano bowiem uprawnienia administratora systemu operacyjnego wykorzystywanych przez nich komputerów, chociaż nie posiadali oni w swych zakresach obowiązków zadań związanych z administrowaniem systemami oraz nie uczestniczyli w szkoleniach w tym zakresie (w siedmiu jednostkach uprawnienia takie posiadali wszyscy pracownicy wykorzystujący sprzęt komputerowy). W rezultacie osoby te posiadały pełny dostęp do zasobów komputerów. Umożliwiono im zatem ściąganie aplikacji i plików wykonywalnych oraz nadano uprawnienia pozwalające na ich instalację na stacjach komputerowych, do których mieli dostęp. Występowały także przypadki, w których pracownicy realizowali określone zadania w systemach informatycznych, choć nie wynikało to z ich zakresów obowiązków. Taka sytuacja stwarza ryzyko obniżenia skuteczności ochrony przetwarzanych danych i zainstalowania na komputerze złośliwego oprogramowania, umożliwiającego penetrację systemu informatycznego.

Przykłady

Wszystkim 10 pracownikom MGOPS w Suchowoli nadano uprawnienia administratora systemu operacyjnego. Dysponowali oni zatem możliwością ściągania aplikacji i plików wykonalnych oraz posiadali uprawnienia do instalowania ich na stacjach komputerowych, do których mieli dostęp. Były Kierownik MGOPS poinformowała, że: *„Użytkownicy przetwarzający dane osobowe na wszystkich ośmiu komputerach posiadali w systemach operacyjnych Windows uprawnienia administratora, ponieważ nie posiadałam świadomości ani wiedzy informatycznej. W omawianym okresie, tj. 2016–2017, w naszym ośrodku nie był zatrudniony informatyk, który obsługiwałby systemy operacyjne Windows od strony informatycznej. Brak zatrudnienia informatyka wynikał z braku środków finansowych na ten cel".*

Użytkownicy wszystkich 15 poddanych oględzinom komputerów w Urzędzie Miejskim w Kleszczelach w bieżącej pracy wykorzystywali konta z uprawnieniami administratora systemu operacyjnego tych urządzeń. W wyniku tego mogli – nawet w sposób przypadkowy – pobierać aplikacje i pliki wykonalne oraz instalować je na stacjach komputerowych, do których mieli dostęp. Burmistrz Kleszczel wyjaśnił, że: *„wynikało to z braku Administratora Systemów Informatycznych. Podkreślam jednak, że pracownicy Urzędu są świadomi*

[21] GOPS w: Boćkach, Dobrzyniewie Dużym, Rudce i Sztabinie, MGOPS w: Czarnej Białostockiej, Krynkach i Suchowoli, MOPS w: Siemiatyczach, Supraślu i Zambrowie, OPS w Ciechanowcu, Starostwo Powiatowe w Białymstoku, urzędy gmin w: Jaświłach, Klukowie, Milejczycach i Szudziałowie, urzędy miejskie w Kleszczelach i Michałowie.

zagrożeń związanych z bezpieczeństwem danych. Wiedzą, że nie mogą instalować aplikacji innych, niż wykorzystywane do celów służbowych. Ponadto komputery posiadają aplikacje antywirusowe, które powinny uniemożliwić instalowanie aplikacji podejrzanych i infekujących komputer".

Użytkownikom wszystkich 11 komputerów OPS w Ciechanowcu, mimo nadania profili z ograniczonymi uprawnieniami, umożliwiono pełny dostęp do panelu zarządzania komputerem, w tym kontem administratora systemu operacyjnego tych urządzeń. Dyrektor OPS wyjaśniła, że wynikało to z niezatrudnienia informatyka.

Nieodbieranie uprawnień do systemów informatycznych byłym pracownikom

W ośmiu[22] (z 31) jednostkach nie w pełni wywiązywano się z obowiązku wynikającego z § 20 ust. 2 pkt 5 rozporządzenia KRI, zgodnie z którym zarządzanie bezpieczeństwem informacji realizowane jest poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. Nie odebrano bowiem (lub odebrano z opóźnieniem) uprawnienia w systemach informatycznych byłym pracownikom tych jednostek.

Przykłady

Trzem pracownikom Starostwa Powiatowego w Łomży, którzy zaprzestali świadczenia pracy w 2016 roku odebrano uprawnienia do systemu SmartDoc dopiero po upływie od 21 do 355 dni od dnia rozwiązania umów o pracę.

Cofnięcie uprawnień do systemu SmartDoc pracownikowi Urzędu Miejskiego w Szepietowie, którego stosunek pracy wygasł 28 października 2017 r nastąpiło dopiero w trakcie kontroli (8 stycznia 2018 r.), tj. z dwumiesięcznym opóźnieniem.

W obu przypadkach jako przyczynę nieodebrania uprawnień wskazano przeoczenie.

Niewłaściwy sposób autoryzacji użytkowników w systemach operacyjnych

Obowiązek zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji wynika z § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI, zgodnie z którym jest on jednym z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. W 12 (z 31) skontrolowanych jednostkach stwierdzono lekceważenie tego wymogu. Brak było bowiem konieczności uwierzytelniania hasłem przy logowaniu się do systemu (w przypadku części komputerów użytkowanych w czterech jednostkach[23]), wprowadzono hasła o złożoności nieodpowiadającej wymaganiom określonym w rozporządzeniu w sprawie dokumentacji oraz warunków technicznych, dla wysokiego poziomu bezpieczeństwa (w dziewięciu jednostkach[24]), a w GOPS w Dobrzyniewie Dużym funkcjonowała sieć bezprzewodowa, która pozwalała na anonimowy i niewymagający autoryzacji dostęp osób z zewnątrz do sieci wewnętrznej jednostki.

[22] Starostwa powiatowe w Białymstoku i Łomży, Urząd Gminy w Klukowie, urzędy miejskie w: Kleszczelach, Michałowie, Suwałkach, Szepietowie i Wysokiem Mazowieckiem.

[23] GOPS w Boćkach i Dobrzyniewie Dużym, MOPS w Siemiatyczach, Starostwo Powiatowe w Łomży.

[24] MGOPS w Suchowoli, MOPS w Siemiatyczach, starostwa powiatowe w Hajnówce i Kolnie, urzędy gmin w Jaświłach i Szudziałowie, urzędy miejskie w: Kleszczelach, Szepietowie i Wysokiem Mazowieckiem.

Przykłady

Mimo że zgodnie z regulacjami wewnętrznymi GOPS w Dobrzyniewie Dużym, środkiem uniemożliwiającym nieautoryzowany dostęp do systemów operacyjnych było hasło dostępowe, to oględziny komputerów Ośrodka wykazały, że nie zostało ono wprowadzone na pięciu z siedmiu urządzeń. Kierownik GOPS wyjaśniła, że nie miała wiedzy na ten temat, natomiast w odniesieniu do zabezpieczeń WI-FI wskazała, że: *„urządzenie to zostało zainstalowane przez informatyka obsługującego Urząd jeszcze, kiedy Ośrodek zajmował pomieszczenia w urzędzie gminy. Nikt nigdy nie zarzucił, że zastosowano hasło, które nie gwarantuje skutecznego zabezpieczenia tego urządzenia".*

Na jednym (z pięciu) komputerów wykorzystywanych w GOPS w Boćkach nie zastosowano hasła dostępowego do systemu operacyjnego. Na komputerze tym nie aktywowano też automatycznego wygaszacza ekranu, co było niezgodne z § 7 pkt 3 obowiązującej w Ośrodku Instrukcji zarządzania systemem informatycznym GOPS. Oba zabezpieczenia aktywowano dopiero podczas kontroli NIK. Kierownik Ośrodka wyjaśniła, że: *„po otrzymaniu tej jednostki komputerowej takie hasło i wygaszacz były aktywowane. Po aktualizacji systemu operacyjnego do wyższej wersji wystąpiły problemy techniczne z hasłem i wygaszaczem i w związku z tym zrezygnowaliśmy z tych rozwiązań".*

Hasła dostępowe ośmiu (z 15) pracowników Urzędu Miejskiego w Kleszczelach do trzech systemów operacyjnych komputerów nie spełniały wymogów złożoności, określonych w § 7 obowiązującej w Urzędzie Instrukcji. Burmistrz Kleszczel wyjaśnił, że: *„wynikało to z braku aktywowania mechanizmu wymuszającego określoną złożoność hasła."*

Hasło dostępu do komputerów 14 (z 16) pracowników Urzędu Gminy Szudziałowo nie spełniało wymogów określonych w Instrukcji Zarządzania Systemami Informatycznymi Urzędu oraz w cz. A pkt IV ust. 2 załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych dla wysokiego poziomu zabezpieczeń, w odniesieniu do określonej w tych przepisach liczby znaków oraz zmiany hasła. ASI błędnie bowiem uważał to za stan normalny.

Ustalenia kontroli wskazują zatem na lekceważący sposób podejścia do wymogów istotnych z punktu widzenia bezpieczeństwa informacji.

Brak kontroli dostępu do systemów informatycznych

Tylko w Urzędzie Miejskim w Suwałkach prowadzony był elektroniczny rejestr dostępu do systemów informatycznych. Informacje o logach[25] były przetwarzane automatycznie i analizowane przy pomocy narzędzia Uplook Statlook. Logi były przechowywane tak długo, jak kopia bezpieczeństwa, której były integralną częścią (30 dni). Były też zabezpieczone przed utratą integralności i zniszczeniem, co – w sytuacji niepożądanej z punktu widzenia bezpieczeństwa danych – dawało duże prawdopodobieństwo ustalenia sprawcy lub źródła zagrożenia. W pozostałych 30 jednostkach, wbrew przepisom § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI, nie wprowadzono takiej kontroli. Logi tworzono jedynie na poszczególnych stanowiskach komputerowych lub obejmowały tylko wybrane systemy. Nie dokonywano ich agregacji oraz bieżącej analizy pod kątem wystąpienia zdarzeń niepożądanych związanych z bezpieczeństwem danych. Podobnie nie gromadzono i nie analizowano logów związanych z pracą urządzeń sieciowych.

[25] *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)

Przykłady

W Urzędzie Miasta Bielsk Podlaski nie prowadzono rejestru dostępu do systemów informatycznych wykorzystywanych do przetwarzania danych osobowych. Informacje w ograniczonym zakresie były gromadzone przez kontroler domeny (logi dotyczące logowania się użytkowników na poszczególnych komputerach oraz do zasobów sieciowych), przy czym – jak wyjaśnił Informatyk Urzędu – z uwagi na fabryczne ustawienia (50kB dla poszczególnych stacji roboczych) logi te obejmowały kilka ostatnich dni. Pozostałe informacje o aktywności użytkowników gromadzone były na poszczególnych stanowiskach użytkowników przez system operacyjny oraz w siedmiu (z dziesięciu) aplikacjach/programach dziedzinowych związanych z przetwarzaniem danych osobowych w rejestrach lub w dziennikach zdarzeń. Pozostałe trzy nie posiadały możliwości technicznych pozwalających na gromadzenie takich danych – były to programy pozwalające jedynie na pogląd danych (w zakresie ewidencji gruntów i budynków) lub obsługiwane przez jedynego pracownika (program do obsługi kasy zapomogowo-pożyczkowej). Informatyk Urzędu wyjaśnił, że informacje takie, jak dziennik podłączeń urządzeń przenośnych USB, z uwagi na brak poważniejszych incydentów w przeszłości, nie były gromadzone i weryfikowane.

W MOPS w Supraślu nie prowadzono rejestru dostępu do systemów informatycznych. Każdy z komputerów domyślnie (rejestr zdarzeń systemu Windows) gromadził swoje logi systemowe na własnym dysku lokalnym. Logi te nie były zabezpieczane przed modyfikacją, nie były agregowane ani automatycznie analizowane. Logi ruchu sieciowego gromadzono na routerze, ale nie były one analizowane. Nie zastosowano żadnych środków, które chroniłyby gromadzące się na komputerach logi przed utratą integralności lub skasowaniem, tj.: logi nie były objęte procesem tworzenia kopii danych (nie były backupowane). Ich trwałość zależała od ustawień producenta systemu, co stwarza zagrożenie, że mogą zostać skasowane lub nadpisane, uniemożliwiając odtworzenie tego co działo się z zasobami. Nie gromadzono ich centralnie na głównym serwerze jednostki, nie wprowadzono także harmonogramu tworzenia backupów logów. Powodem takiej sytuacji było uznanie przez Kierownik MOPS, że logi nie wymagają dodatkowego zabezpieczania.

W 14 jednostkach umożliwiono zdalny dostęp do zasobów bez odpowiedniego nadzoru

W 14[26] z 31 skontrolowanych jednostek umożliwiono zdalny dostęp do zasobów informatycznych z wykorzystaniem aplikacji pulpitu zdalnego, z której korzystali pracownicy firm zewnętrznych podczas realizacji prac serwisowych. Dostęp taki następował bez autoryzacji i nadzoru ze strony osób odpowiedzialnych za bezpieczeństwo systemów informatycznych jednostki, co stanowiło naruszenie obowiązku określonego w § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI. Przy połączeniach tego typu wykorzystywano konta i uprawnienia (w systemach informatycznych) nadane poszczególnym pracownikom, którzy byli zalogowani w chwili nawiązania połączenia z wykorzystaniem ww. aplikacji.

W umowach z podmiotami trzecimi brakowało zapisów gwarantujących odpowiednie bezpieczeństwo informacji

W ośmiu[27] (z 31) skontrolowanych jednostkach, mimo obowiązku wynikającego z przepisu § 20 ust. 2 pkt 10 rozporządzenia KRI, w umowach serwisowych podpisanych ze stronami trzecimi nie zamieszczono zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

[26] GOPS w Narewce, MGOPS w Suchowoli, OPS w Ciechanowcu, Starostwo Powiatowe w Białymstoku, urzędy gmin w: Klukowie, Milejczycach, Sidrze i Szudziałowie, urzędy miejskie w: Bielsku Podlaskim, Kleszczelach, Nowogrodzie, Szczuczynie, Szepietowie i Wysokiem Mazowieckiem.

[27] GOPS w: Dobrzyniewie Dużym, Narewce i Rudce, MGOPS w Czarnej Białostockiej, MOPS w Siemiatyczach, Starostwo Powiatowe w Hajnówce, urzędy miejskie w Nowogrodzie i Szczuczynie.

Przykład

W Urzędzie Miejskim w Nowogrodzie w okresie objętym kontrolą w jednej (z dwóch) umowie serwisowej, dotyczącej świadczenia usługi serwisu eksploatacyjnego oprogramowania komputerowego, nie zawarto regulacji zobowiązujących dostawcę programu do zachowania w tajemnicy i nieudostępniania danych osobowych przekazanych przez Urząd. Burmistrz wyjaśnił, że powodem było przygotowanie umowy przez firmę świadczącą usługi.

Z kolei siedem[28] jednostek, mimo obowiązku ustalonego w § 20 ust. 2 pkt 9 rozporządzenia KRI, w umowach na świadczenie usług poczty elektronicznej nie zamieściło zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym bądź umów takich nie zawierano w ogóle, gdy korzystano z kont pocztowych umieszczonych na ogólnodostępnych serwerach komercyjnych.

Przykłady

W Urzędzie Gminy Szudziałowo poczta elektroniczna zakładana była przez każdego z pracowników samodzielnie na domenach internetowych należących do podmiotów komercyjnych (bez zawierania pisemnych umów w tym zakresie). W przypadku sześciu pracowników konta pocztowe założone do celów służbowych wykorzystywano również do celów prywatnych. ASI Urzędu wyjaśnił, że nie zdawał sobie sprawy, że taki stan jest nieprawidłowy oraz poinformował, że po oględzinach przeprowadzonych w trakcie kontroli NIK wykupił domenę pocztową i założył pracownikom Urzędu konta imienne oraz konta zależne od stanowiska.

Główne konto poczty elektronicznej GOPS w Boćkach hostingowane było bezpłatnie przez operatora komercyjnego, z którym Ośrodek nie miał podpisanej umowy, co nie gwarantowało bezpieczeństwa usługi. Kierownik jednostki wyjaśnił, że konto pocztowe zostało założone dawno i z powodów organizacyjnych go nie zmieniano. W trakcie kontroli NIK dokonano zmiany serwera poczty.

Wykorzystywanie nieaktualnych systemów operacyjnych

W ponad połowie jednostek (18[29]) w dalszym ciągu wykorzystywano systemy operacyjne Windows XP i Windows Vista, dla których odpowiednio od 8 kwietnia 2014 r. i 11 kwietnia 2017 r. producent zakończył udzielanie wsparcia technicznego, a wiec nie są publikowane nowe poprawki bezpieczeństwa, których zadaniem było likwidowanie luk w zabezpieczeniach tych systemów. Liczba komputerów działających na ww. systemach wynosiła od jednego (GOPS w Narewce) do 39 (Starostwo Powiatowe w Białymstoku). Komputery te stanowiły od 4% do 43% ogółu komputerów w poszczególnych jednostkach. Największy odsetek tych urządzeń stwierdzono w MOPS w Siemiatyczach (43%) oraz MOPR w Suwałkach (36%). W obu przypadkach kierownicy jednostek wyjaśnili, że komputery z ww. systemami operacyjnymi są sukcesywnie wycofywane z użycia, a główną przeszkodą do ich całkowitej eliminacji jest brak środków finansowych. W obu jednostkach – z uwagi na specyfikę realizowanych zadań – urządzenia

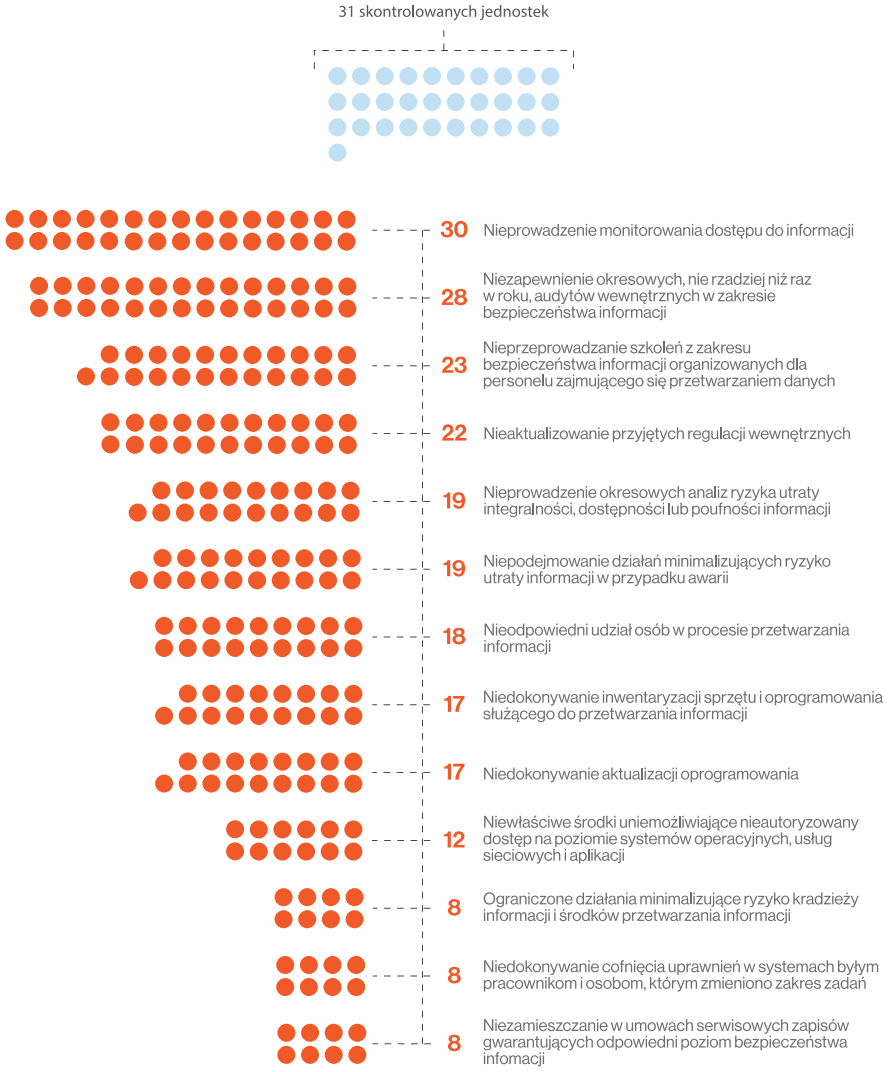
[28] GOPS w Boćkach, MGOPS w Czarnej Białostockiej i Suchowoli, starostwa powiatowe w Łomży i Zambrowie, Urząd Gminy w Szudziałowie, Urząd Miejski w Kleszczelach.

[29] GOPS w Narewce, MGOPS w Czarnej Białostockiej i Krynkach, MOPR w Suwałkach, MOPS w Siemiatyczach i Supraślu, OPS w Ciechanowcu, starostwa powiatowe w Białymstoku i Kolnie, urzędy gminy w: Jaświłach, Milejczycach, Sidrze i Szudziałowie, urzędy miejskie w: Kleszczelach, Michałowie, Suwałkach, Szepietowie i Wysokiem Mazowieckiem.

te mogły być wykorzystywane do przetwarzania danych wrażliwych, o których mowa w art. 27 ustawy o ochronie danych osobowych. Komputery pracujące na niewspieranych systemach operacyjnych stanowią zaś zagrożenie dla bezpieczeństwa sieci jednostek, w których są wykorzystywane.

W dwóch jednostkach nie zapewniono aktualizacji systemów operacyjnych, mimo że posiadały one wsparcie producenta i możliwość automatycznej aktualizacji. Dotyczyło to dwóch (z 11) komputerów wykorzystywanych w Urzędzie Miejskim w Kleszczelach oraz aż 22 (z 25) komputerów użytkowanych w Urzędzie Miejskim w Szepietowie. Przy czym niektóre z systemów operacyjnych na komputerach w tej jednostce nie były aktualizowane od momentu instalacji, a na dwóch nie była zainstalowana aplikacja bezpieczeństwa. Było to sprzeczne z § 20 ust. 2 pkt 12 lit a rozporządzenia KRI, zgodnie z którym zarządzanie bezpieczeństwem informacji realizowane jest poprzez zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na dbałości o aktualizację oprogramowania.

Diagram nr 2
Najczęściej występujące nieprawidłowości związane z zapewnieniem bezpieczeństwa informacji oraz liczba jednostek, w których je stwierdzono

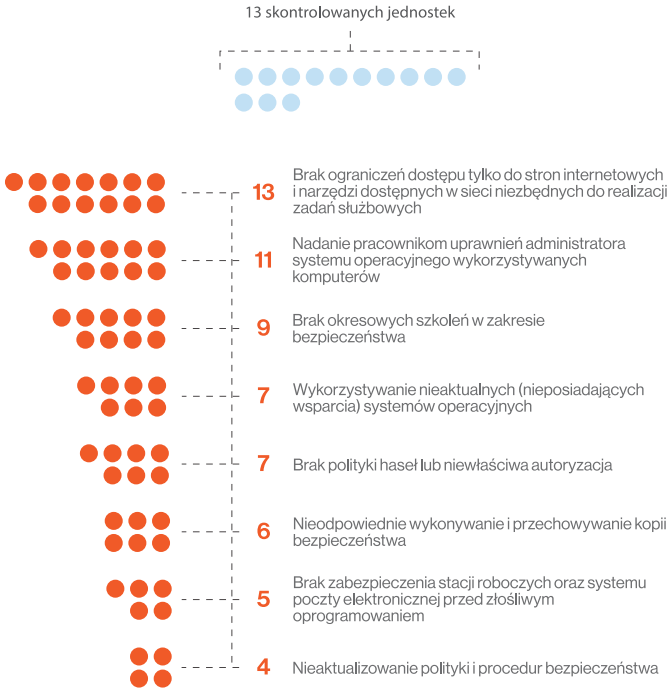


Źródło: Opracowanie własne na podstawie wyników kontroli NIK.

W żadnym spośród 13 skontrolowanych ośrodków pomocy społecznej nie zapewniono odpowiedniego poziomu bezpieczeństwa danym w nich gromadzonym. Pomimo że dysponowały one danymi wrażliwymi swoich klientów, w ośrodkach tych stwierdzono szereg nieprawidłowości dotyczących bezpieczeństwa zasobów, w tym niewłaściwe zarządzanie uprawnieniami użytkowników w systemach operacyjnych, brak okresowych szkoleń, niezapewnienie właściwej autoryzacji przy logowaniu do systemów informatycznych, niewłaściwe wykonywanie i przechowywanie kopii bezpieczeństwa. Szczegółowe dane w tym zakresie przedstawia poniższy wykres.

W żadnym o.p.s. nie zapewniono danym odpowiedniego poziomu bezpieczeństwa

Diagram nr 3
Dane dotyczące liczby ośrodków pomocy społecznej, w których nie były podejmowane działania dotyczące bezpieczeństwa informacji.



Źródło: Opracowanie własne na podstawie wyników kontroli NIK.

Powyższe ustalenia wskazują, że istotnymi ryzykami mającymi wpływ na bezpieczeństwo systemów informatycznych skontrolowanych jednostek oraz przyczynami dużej liczby istotnych nieprawidłowości w tym zakresie były głównie: niezatrudnianie informatyków do obsługi systemów informatycznych w 12 z 31 jednostek oraz znikoma liczba pracowników przeszkolonych z zakresu bezpieczeństwa systemów informatycznych (szkolenia takie organizowano dla części pracowników jedynie w ośmiu jednostkach).

5.3. Sposób przechowywania oraz zabezpieczenia danych

W większości jednostek przyjęty sposób przechowywania oraz zabezpieczenia danych nie odpowiadał przepisom oraz przyjętym procedurom, przez co nie zapewniał im właściwej ochrony. Nie wprowadzono także bieżącego monitorowania dostępu do zasobów informacyjnych oraz niewłaściwie zarządzano uprawnieniami w systemach wykorzystywanych do przetwarzania danych.

W dokumentacji opisującej sposób przetwarzania danych osobowych każdej z jednostek określono fizyczne środki ochrony tych danych. Regulacje te w szczególności wskazywały, że: dokumenty i systemy informatyczne służące do przetwarzania danych osobowych mogą być przechowywane wyłącznie w przeznaczonych do tego pomieszczeniach, gwarantujących prawidłową ochronę i zabezpieczenie danych przed wglądem osób nieupoważnionych; pomieszczenia te po zakończeniu pracy powinny być skontrolowane przez ostatniego opuszczającego je pracownika, czy nie zostały niezabezpieczone dokumenty; przebywanie w tych pomieszczeniach poza godzinami pracy możliwe jest tylko za zgodą ADO, a osoby nieupoważnione mogą w nich przebywać wyłącznie w obecności osób uprawnionych do przetwarzania danych osobowych.

Infrastruktura sieciowa jednostek – brak wydzielonych serwerowni

Większość jednostek posiadała własne urządzenia serwerowe usytuowane w specjalnie wydzielonych i zabezpieczonych pomieszczeniach oraz zarządzała siecią, do której były podłączone komputery wykorzystywane do przetwarzania danych. W dziewięciu jednostkach[30] nie stworzono odpowiednio wyposażonych pomieszczeń serwerowni, a w ośmiu[31] właściwej ochrony fizycznej urządzeń, co było niezgodne z dyspozycją art. 36 ust. 1 ustawy o ochronie danych osobowych. W konsekwencji serwery wykorzystywanych aplikacji oraz infrastruktura informatyczna (urządzenia typu router i switch) znajdowały się w miejscach nieposiadających odpowiedniego wyposażenia (np. w czujniki ostrzegające o pożarze lub zalaniu) oraz niezabezpieczonych przed dostępem osób postronnych. Wystąpił też przypadek wykorzystywania ww. pomieszczenia do przetrzymywania zużytego sprzętu komputerowego (Urząd Gminy Sidra). Jako powód takiego stanu podawano głównie brak środków finansowych na zakup odpowiedniego wyposażenia.

Przykłady

OPS w Ciechanowcu nie posiadał własnej serwerowni (korzystał z pomieszczenia Urzędu Miejskiego w Ciechanowcu). Sieć komputerowa OPS stanowiła element sieci Urzędu, przez co część zasobów informacyjnych (plików) Ośrodka była udostępniana również pracownikom Urzędu Miejskiego (nie dotyczyło to danych osobowych pracowników i klientów OPS).

W MOPS w Siemiatyczach pomieszczenie, w którym znajdował się serwer nie posiadało czujników ostrzegających o pożarze oraz nie zastosowano w nim rozwiązań zapobiegających zalaniu zainstalowanego tam sprzętu i przetrzymywanych dokumentów. Nie zapewniało to właściwej ochrony zbiorów danych przed działaniem czynników fizycznych i zdarzeń losowych. Powodem takiej sytuacji – wg kierownik ośrodka – były warunki lokalowe, nieadekwatne do zadań realizowanych przez MOPS, przez co brakowało pomieszczeń na wydzielenie serwerowni bądź ustawienie szafy chłodniczej dla serwera. Dodała, że pomieszczenia MOPS nie mają zabezpieczeń przed włamaniem, pożarem i zalaniem, gdyż planowana jest zmiana siedziby Ośrodka.

[30] GOPS w: Boćkach, Dobrzyniewie Dużym, Narewce i Rudce, MGOPS w: Czarnej Białostockiej, Krynkach i Suchowoli, MOPS w Siemiatyczach, OPS w Ciechanowcu.

[31] GOPS w Narewce, MOPS w Siemiatyczach, starostwa powiatowe w Białymstoku i Łomży, urzędy gmin w: Klukowie, Sidrze i Szudziałowie, Urząd Miejski w Michałowie.

W blisko połowie jednostek nie zapewniono właściwej ochrony fizycznej zbiorów danych

W 15[32] (z 31) jednostkach posiadanym zasobom informacyjnym nie zapewniono właściwego zabezpieczenia, czym naruszono wymogi art. 36 ust. 1 ustawy o ochronie danych osobowych, nakazujące zapewnienie ochrony przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Nieprawidłowości w tym zakresie dotyczyły głównie sytuacji polegających na: umiejscowieniu dokumentacji zawierającej dane osobowe w pomieszczeniach bez odpowiedniego wyposażenia (np.: alarm, system przeciwpożarowy), przechowywaniu części zbiorów danych osobowych w miejscach (szafach, półkach) nieposiadających możliwości zamknięcia, nieokreśleniu zasad gospodarowania kluczami do poszczególnych pomieszczeń, niewyrażeniu przez ADO zgody na przebywanie w obszarze przetwarzania danych osobom zajmującym się sprzątaniem pomieszczeń pod nieobecność osób upoważnionych do przetwarzania danych osobowych. Kierownicy jednostek, wyjaśniając przyczyny niewłaściwego zabezpieczenia zasobów informacyjnych, wskazywali głównie na brak środków finansowym na zakup odpowiedniego wyposażenia.

W 19 jednostkach nie zapewniono bezpieczeństwa kopiom baz danych

W 19 (z 31) jednostkach nie sporządzano lub w niewłaściwy sposób tworzono i przechowywano kopie bezpieczeństwa baz danych. W 11 przypadkach[33] nie wszystkie bazy danych były poddawane regularnemu procesowi tworzenia kopii, a w kolejnych ośmiu[34] wykonane kopie były niewłaściwie przechowywane. Nieprawidłowości w tym zakresie polegały głównie na umieszczaniu wykonanych kopii w urządzaniach, w których znajdowały się dane podlegające procesowi tworzenia kopii lub przetrzymywaniu nośników zawierających kopie w tym samym pomieszczeniu co baza danych. Powszechne było też niewykonywanie testowania stworzonych kopii baz danych, co nie daje pewności poprawności ich tworzenia. Działania te były niezgodne z przepisem cz. A pkt IV ust. 4 lit. a załącznika do rozporządzenia w sprawie dokumentacji oraz warunków technicznych, zgodnie z którym kopie zapasowe przechowuje się w miejscach zabezpieczających je przed uszkodzeniem lub zniszczeniem. Takie działania skutkowały również naruszeniem dyspozycji § 20 ust. 2 pkt 12b rozporządzenia KRI, w myśl którego należy podejmować działania minimalizujące ryzyko utraty informacji w wyniku awarii. Przechowywanie kopii baz danych w miejscu skąd pochodzą dane stwarza duże ryzyko ich utraty, np. w przypadku wystąpienia pożaru, w wyniku którego zniszczeniu może ulec baza danych i jej kopia zapasowa.

[32] GOPS w Dobrzyniewie Dużym i Sztabinie, MGOPS w Czarnej Białostockiej, MOPS w Siemiatyczach i Zambrowie, starostwa powiatowe w: Białymstoku, Kolnie i Łomży, Urząd Gminy w Klukowie, urzędy miejskie w: Kleszczelach, Michałowie, Nowogrodzie, Suwałkach, Szczuczynie i Szepietowie.

[33] GOPS w Rudce, MGOPS w Czarnej Białostockiej i Suchowoli, starostwa powiatowe w: Hajnówce, Kolnie i Łomży, urzędy gmin w: Jaświłach, Klukowie, Milejczycach, urzędy miejskie w Kleszczelach i Szepietowie.

[34] GOPS w: Boćkach, Dobrzyniewie Dużym i Sztabinie, OPS w Ciechanowcu, Starostwo Powiatowe w Białymstoku, urzędy gmin w Sidrze i Szudziałowie, Urząd Miejski w Michałowie.

Przykłady

W Urzędzie Miejskim w Kleszczelach kopie zapasowe wszystkich 12 aplikacji bazodanowych tworzono niezgodnie z § 13 obowiązującej w Urzędzie Instrukcji. Nie tworzono kopii zapasowych baz danych dwóch aplikacji, a kopii zapasowych baz danych czterech aplikacji nie przenoszono na oddzielne nośniki informatyczne. Chociaż kopie baz danych sześciu pozostałych aplikacji przenoszono na nośniki zewnętrzne, to jednak przechowywano je w tym samym pomieszczeniu co jednostka komputerowa z danymi produkcyjnymi. Dodatkowo w Urzędzie nie testowano części tworzonych kopii zapasowych. Z wyjaśnień burmistrza Kleszczel wynika, że przyczyną tego było przeoczenie pracowników wykonujących kopie zapasowe, brak odpowiedniej liczby aplikacji wykonujących kopie danych oraz brak odpowiednich aplikacji do testowania kopii.

W GOPS w Dobrzyniewie Dużym kopie zapasowe obejmujące bazy danych aplikacji dziedzinowych gromadzono na nośniku typu pendrive, który przechowywany był w zamykanej na klucz szafie, znajdującej się w tym samym pomieszczeniu, co komputer, z którego dane były archiwizowane. Przechowywanie tych kopii w miejscu skąd pochodzą dane stwarza duże ryzyko ich utraty. Kierownik GOPS wyjaśniła, że nie miała świadomości takiego zagrożenia.

W GOPS w Boćkach jedynie osiem ze 104 kopii zapasowych programu dziedzinowego, służącego do wspomagania realizacji zadań GOPS wynikających z ustawy o pomocy społecznej, zostało w 2017 r. przeniesionych na dysk zewnętrzny, mimo że – zgodnie z Instrukcją zarządzania systemem informatycznym GOPS – wszystkie kopie zapasowe powinny być przechowywane na komputerze stacjonarnym Kierownika GOPS oraz na dysku zewnętrznym. Dodatkowo w Ośrodku nie testowano tworzonych kopii zapasowych, a dysk zewnętrzny z kopiami zapasowymi był przetrzymywany w tym samym pomieszczeniu co jednostka komputerowa z danymi produkcyjnymi. Kierownik GOPS wyjaśniła, że: *„przenoszenie kopii zapasowej na dysk przenośny zajmuje sporo czasu. Wobec dużego obciążenia pracą nie zawsze znajdowałam czas na wykonanie kopii na dysku przenośnym. Ze względu na brak sejfu dysk przenośny z kopiami zapasowymi jest przetrzymywany w moim pokoju. Nie przeprowadzano testów* (kopii zapasowych – przyp. NIK*) z powodu braku odpowiednich narzędzi informatycznych".*

17 jednostek nie gromadziło bieżących informacji o posiadanym sprzęcie i jego konfiguracji

Jednym z elementów procesu zapewnienia bezpieczeństwa informatycznego jest konieczność gromadzenia bieżących informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację. Obowiązek ten wynika bezpośrednio z § 20 ust. 2 pkt 2 rozporządzenia KRI. Informacje te są niezbędne przy wprowadzaniu zmian w środowisku teleinformatycznym jednostki, ograniczając możliwość zaistnienia zakłóceń w pracy, które wynikłyby z błędnych decyzji i podejmowanych działań, wynikających z braku aktualnej i kompleksowej wiedzy o stanie infrastruktury teleinformatycznej.

W ponad połowie jednostek (17[35]) dane takie nie były jednak gromadzone. Prowadzono wprawdzie okresowe ewidencje posiadanych urządzeń na potrzeby rachunkowości, ale nie zawierały one pełnych danych o sprzęcie, programach i ich konfiguracji. Nieprowadzenie takich działań uzasadniane było m.in.: brakiem wiedzy o istnieniu takiego obowiązku, nie-

[35] GOPS w: Boćkach, Dobrzyniewie Dużym, Rudce i Sztabinie, MGOPS w: Czarnej Białostockiej, Krynkach i Suchowoli, MOPS w Siemiatyczach i Zambrowie, OPS w Ciechanowcu, Starostwo Powiatowe w Hajnówce, urzędy gmin w: Milejczycach, Sidrze i Szudziałowie, urzędy miejskie w: Michałowie, Szepietowie i Wysokiem Mazowieckiem.

posiadaniem odpowiednich umiejętności do zebrania i usystematyzowania takich danych, założeniem, że obowiązek ten nie musi być spełniony z uwagi na niewielką liczbę posiadanego sprzętu.

W 19[36] (z 31) jednostkach nie opracowano planu ciągłości działania (odtworzenia utraconych zasobów), który jest niezbędny do przywrócenia aplikacji o znaczeniu krytycznym w sytuacji ich utracenia. Plan ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany.

W 19 jednostkach nie opracowano regulacji dotyczących odtwarzania utraconych zasobów

Diagram nr 3
Główne elementy planowania ciągłości działania jednostki

Źródło: Opracowanie własne NIK na podstawie podręcznika kontroli systemów IT.

Głównymi powodami nieopracowania takich regulacji były: brak środków finansowych na ten cel, nieodnotowywanie częstych awarii, uznanie za wystarczające posiadanie agregatu prądotwórczego, który jest wykorzystywany w przypadku wystąpienia awarii zasilania. Sytuacje nadzwyczajne to jednak nie tylko okresowy zanik energii elektrycznej, lecz także skutki innych zdarzeń np. pożaru czy zalania, w wyniku których zniszczeniu mogą ulec zarówno urządzenia i dane na nich przechowywane, jak też dokumentacja papierowa. Stąd istotnym jest stworzenie zasad i metod odtwarzania utraconych zasobów oraz funkcjonowania danej jednostki po takim zdarzeniu[37].

[36] GOPS w Dobrzyniewie Dużym i Sztabinie, MGOPS w Czarnej Białostockiej i Suchowoli, MOPS w: Siemiatyczach, Supraślu i Zambrowie, OPS w Ciechanowcu, starostwa powiatowe w: Białymstoku, Łomży i Zambrowie, urzędy gmin w: Milejczycach, Sidrze i Szudziałowie, urzędy miejskie w: Bielsku Podlaskim, Kleszczelach, Nowogrodzie, Szepietowie i Wysokiem Mazowieckiem.

[37] Zgodnie z Podręcznikiem kontroli systemów IT, plan ciągłości działania powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby plany te były jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności jednostki.

Przykłady

W GOPS w Narewce opracowano Plan ciągłości działania systemu informatycznego oraz Instrukcję postępowania w sytuacji naruszenia systemu ochrony danych osobowych i bezpieczeństwa informacji[38]. W dokumentach tych zawarto m.in. opis typowych incydentów wpływających na bezpieczeństwo danych oraz działań zapewniających przywrócenie zdolności realizacji działalności statutowej jednostki (ze wskazaniem niezbędnych zasobów i osób odpowiedzialnych).

Niemal wszystkie jednostki posiadały rozwiązania na wypadek krótkotrwałych przerw w zasilaniu

Jednostki objęte kontrolą w przeważającej części posiadały rozwiązania na wypadek krótkotrwałych przerw w dostawie energii elektrycznej. Zabezpieczenia te polegały na wyposażeniu poszczególnych komputerów oraz urządzeń sieciowych (serwerów, switch) w układy podtrzymujące napięcie typu UPS. Takie rozwiązania nie zostały w pełni wprowadzone w pięciu jednostkach, tj. w:

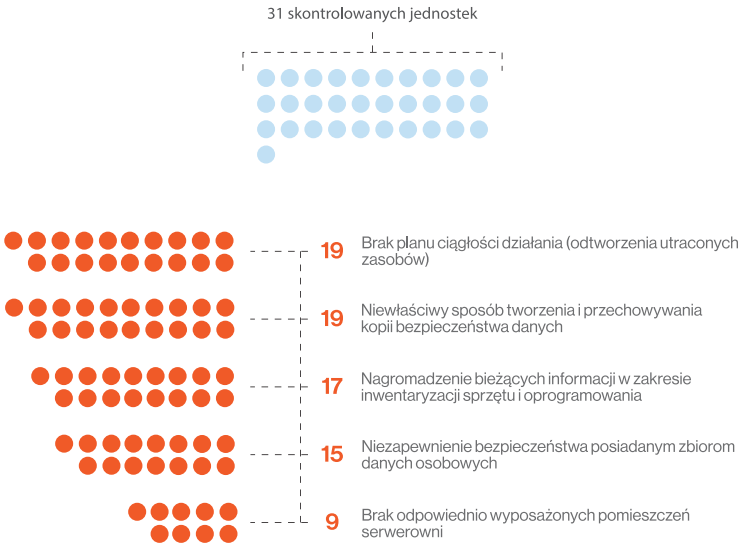
- MOPS w Siemiatyczach, nieposiadającym takich rozwiązań dla dziewięciu z 21 komputerów;
- MOPS w Zambrowie, w którym do układów typu UPS nie podłączono 11 z 32 komputerów;
- Urzędzie Gminy Klukowo, gdzie rozwiązań takich nie posiadały dwa z 19 komputerów;
- Starostwie Powiatowym w Zambrowie, w którym dwa z 30 komputerów nie posiadały takiego zabezpieczenia;
- Urzędzie Miasta Wysokie Mazowieckie, gdzie tylko jeden (z 29) komputerów oraz serwer tego urzędu został zabezpieczony przed utratą zasilania.

W jednej jednostce naruszono bezpieczeństwo systemu informatycznego

Pomimo szeregu nieprawidłowości w zabezpieczeniu systemów informatycznych, zgodnie z wyjaśnieniami pracowników odpowiedzialnych za bezpieczeństwo danych w poszczególnych jednostkach, w okresie objętym kontrolą tylko w Urzędzie Miejskim w Michałowie wystąpił jeden udokumentowany przypadek naruszenia bezpieczeństwa systemu informatycznego, polegający na zainfekowaniu jednego z komputerów wirusem znajdującym się w załączniku wiadomości e-mail. W wyniku działania złośliwego oprogramowania zaszyfrowane zostały wszystkie dokumenty na dysku komputera. Podjęte działania polegały na sformatowaniu dysku i ponownej instalacji systemu operacyjnego. Skutkiem naruszenia bezpieczeństwa systemu informatycznego była utrata wszystkich dokumentów znajdujących się na dysku lokalnym komputera (dane z systemów zostały przywrócone z dostępnych kopii zapasowych). W raporcie z tego zdarzenia wskazano, że okolicznością sprzyjającą naruszeniu było podłączenie do sieci nowego komputera, który nie posiadał zaktualizowanej bazy wirusów w zainstalowanym programie antywirusowym. Podjęte środki zapobiegawcze polegały na aktualizacji ww. programu oraz poinstruowaniu pracownika o zakazie otwierania załączników e-mail pochodzących z nieznanych źródeł.

[38] Obydwa dokumenty zostały opracowane przez ABI i 17 stycznia 2017 r. zatwierdzone przez kierownika GOPS.

Diagram nr 4
Najczęściej występujące błędy w przechowywaniu oraz zabezpieczeniu danych



Źródło: Opracowanie własne na podstawie wyników kontroli NIK.

5.4. Realizacja obowiązków w zakresie przetwarzania danych osobowych

Większość jednostek nie przestrzegała przepisów dotyczących rejestracji i aktualizacji zbiorów danych osobowych w GIODO oraz zapewnienia dostępu do nich osobom upoważnionym, a ADO i ABI w tych jednostkach nie wywiązywali się z obowiązków związanych z ochroną danych oraz nie podejmowali działań w celu przygotowania się do nowych uregulowań wynikających z RODO.

Liczba prowadzonych zbiorów danych

Liczba i rodzaj zbiorów danych osobowych prowadzonych w poszczególnych jednostkach zależały od wielkości (determinowanej liczbą osób zamieszkałych na terenie, na którym funkcjonowała) oraz rodzaju jednostki i liczby zadań, do realizacji których była ona powołana (inny rodzaj danych przetwarzają ośrodki pomocy społecznej, inny urzędy gmin, a jeszcze inny starostwa powiatowe).

Najmniejszą liczbę zbiorów danych posiadały ośrodki pomocy społecznej. Znajdowało się w nich od siedmiu do 11 takich zbiorów (wyjątkiem był MOPR w Suwałkach[39], w którym prowadzono 19 zbiorów). Były to jednak przede wszystkim zbiory zawierające dane wrażliwe, o których mowa w art. 27 ustawy o ochronie danych osobowych. Większość zbiorów danych osobowych w ośrodkach pomocy społecznej prowadzona była zarówno w formie elektronicznej, jak i papierowej. Do elektronicznego prowadzenia zbiorów wykorzystywano szereg aplikacji dziedzinowych, pozwalających na prowadzenie spraw z zakresu pomocy społecznej.

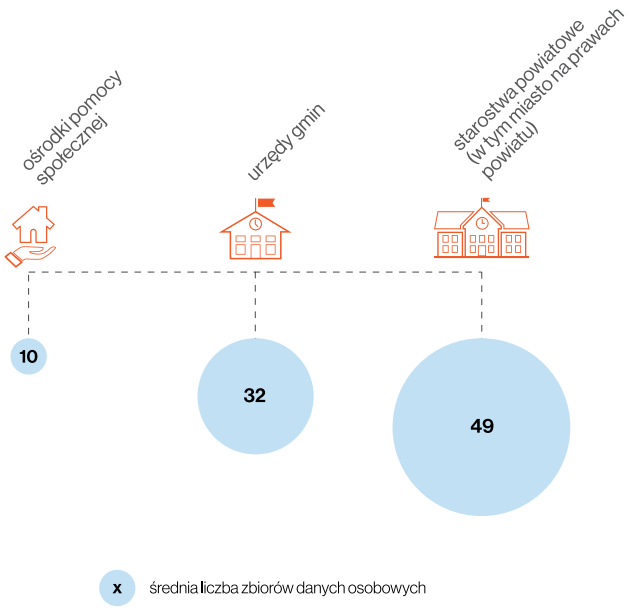
[39] Ośrodek w mieście na prawach powiatu.

W urzędach gmin prowadzono od 15 do 58 zbiorów danych osobowych, w formie elektronicznej, papierowej albo w obu formach jednocześnie. Na przykład w Urzędzie Miasta Wysokie Mazowieckie wyodrębniono 58 zbiorów, z których 44 prowadzono wyłącznie w formie papierowej.

Najwięcej zbiorów danych osobowych prowadzonych było w skontrolowanych starostwach powiatowych. Ich liczba kształtowała się od 47 w Starostwie Powiatowym w Zambrowie do 64 w Starostwie Powiatowym w Łomży. W jednostkach tych (podobnie jak w gminach) odpowiednio 53% i 77% zbiorów prowadzono wyłącznie w formie papierowej.

Spośród skontrolowanych jednostek największą liczbą wyodrębnionych i prowadzonych zbiorów danych osobowych (93) dysponował Urząd Miejski w Suwałkach.

Infografika nr 3
Średnia liczba zbiorów danych osobowych prowadzonych w jednostkach objętych kontrolą



Źródło: Opracowanie własne na podstawie wyników kontroli NIK.

Infografika nr 4
Główne regulacje dotyczące ustawy o ochronie danych osobowych

Źródło: Opracowanie własne NIK na podstawie ustawy o ochronie danych osobowych.

W siedmiu jednostkach przetwarzano zbędne dane osobowe

Przetwarzanie danych osobowych, w myśl przepisu art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, jest dopuszczalne m.in. tylko wtedy, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Za naruszenie tych zasad, przewidziane były sankcje karne określone w art. 49 tej ustawy (szczególnie dotkliwe w przypadku danych wrażliwych), a od 25 maja 2018 r. wynikające z art. 107 nowej ustawy o ochronie danych osobowych. W siedmiu skontrolowanych jednostkach[40] gromadzono jednak w zbiorach dane osobowe, których przetwarzanie nie było niezbędne do realizacji zadań,

[40] Starostwa powiatowe w: Hajnówce, Kolnie i Łomży, Urząd Gminy Klukowo, urzędy miejskie w: Michałowie, Suwałkach i Wysokiem Mazowieckiem.

dla których zbiory te były prowadzone. W trzech[41] z nich wśród zbędnych danych, które gromadzono znalazły się dane wrażliwe takie, jak: kopie wydanych orzeczeń lekarskich o braku przeciwwskazań zdrowotnych do pracy na stanowisku kierowcy, kopie orzeczeń o potrzebie kształcenia specjalnego oraz orzeczeń o potrzebie wcześniejszego wspomagania rozwoju dziecka.

Przykład

W Starostwie Powiatowym w Łomży w formie papierowej prowadzono Rejestr klubów sportowych. Gromadzono w nim m.in. imiona i nazwiska oraz daty urodzin członków zarządu i organu kontroli wewnętrznej, a także nr PESEL i adresy zamieszkania ww. osób, chociaż przepisy § 5 rozporządzenia Ministra Sportu i Turystyki z dnia 18 października 2011 r. w sprawie ewidencji klubów sportowych[42] nie przewidują gromadzenia i zamieszczania w ewidencji takich danych.

Większość jednostek nie zgłosiła GIODO wszystkich z prowadzonych zbiorów danych osobowych

Aż 24[43] (z 31) jednostek nie wywiązało się z obowiązku zgłoszenia do rejestracji GIODO wszystkich prowadzonych zbiorów danych osobowych wbrew przepisom art. 40 ustawy o ochronie danych osobowych. Zgodnie z art. 53 tej ustawy, niezgłoszenie do rejestracji zbioru danych zagrożone było sankcją karną, natomiast od 25 maja 2018 r., w myśl RODO, wymagane jest tylko prowadzenie rejestru czynności przetwarzania danych w jednostce (zniesiono obowiązek rejestracji zbiorów oraz zlikwidowano sankcje karne za jego niedopełnienie). Brak zgłoszenia w poszczególnych jednostkach dotyczył od jednego do 17 zbiorów, co stanowiło od 2% do nawet 71%[44] prowadzonych zbiorów danych osobowych.

Przykłady

W Urzędzie Gminy Milejczyce do rejestracji przez GIODO nie zgłoszono 17[45] (z 33) zbiorów danych osobowych (dane rozpoczęto w nich przetwarzać przed 2016 rokiem). Wójt wyjaśnił, że nie miał świadomości, że pracownicy nie dokonali zgłoszenia. Faktycznie jednak obowiązek zgłaszania rejestracji zbiorów danych osobowych spoczywa na ADO, którego zadania wykonywał Wójt.

Prezydent Miasta Suwałki prowadził bez wymaganej rejestracji dwa zbiory danych osobowych, zawierające dane wrażliwie: [1] od 20 czerwca 2014 r.

41 Urzędy miejskie w: Michałowie, Suwałkach i Wysokiem Mazowieckiem.

42 Dz. U. Nr 243 poz.1449.

43 GOPS w: Dobrzyniewie Dużym, Rudce i Sztabinie, MGOPS w: Czarnej Białostockiej, Krynkach i Suchowoli, MOPS w Siemiatyczach i Zambrowie, OPS w Ciechanowcu, starostwa powiatowe w: Białymstoku, Hajnówce, Kolnie, Łomży i Zambrowie, urzędy gmin w: Klukowie, Milejczycach, Sidrze i Szudziałowie, urzędy miejskie w: Kleszczelach, Michałowie, Nowogrodzie, Suwałkach, Szczuczynie i Szepietowie.

44 MGOPS w Suchowoli.

45 Do rejestracji nie zgłoszono następujących zbiorów: „Zwrot podatku akcyzowego na paliwo", „Rejestr Vat", „Wnioski do gminnej komisji rozwiązywania problemów alkoholowych", „Ewidencja zezwoleń na sprzedaż napojów alkoholowych", „Gospodarka odpadami komunalnymi", „Podział i rozgraniczenia nieruchomości", „Zezwolenia na zajęcie pasa drogowego prowadzenie robót, umieszczenie urządzeń infrastruktury technicznej", „Wycinka drzew i krzewów", „Sprzedaż nieruchomości, użytkowanie wieczyste", „Decyzje o środowiskowych uwarunkowaniach zgody na realizację przedsięwzięcia", „Wnioski o nadanie numeru porządkowego", „Gospodarka wodna", „Skargi i wnioski", „Wnioski o udzielenie informacji publicznej", „Oświadczenia majątkowe", „Rejestr sołtysów", „Kancelaria i elektroniczny obieg dokumentów".

do 22 grudnia 2017 r. zbiór Karta Dużej Rodziny[46], zawierający m.in. informacje o znacznym i umiarkowanym stopniu niepełnosprawności, w tym o okresie, na jaki wydano orzeczenie o niepełnosprawności, informacje o umieszczeniu dziecka w pieczy zastępczej, orzeczenie sądu o odebraniu lub ograniczeniu władzy rodzicielskiej; [2] od 3 stycznia 1997 r. do 29 grudnia 2017 r. zbiór Ewidencja osób kierowanych na leczenie odwykowe, w którym gromadzono m.in. informacje o stanie zdrowia, nałogach, orzeczenia sądowe wydane w postępowaniu sądowym lub administracyjnym. Prezydent wyjaśnił, że nie miał świadomości, że te zbiory nie były zarejestrowane oraz że w latach 2015–2016 co najmniej trzykrotnie pisemnie zwracał się do naczelników wydziałów o zgłaszanie wszystkich zbiorów zawierających dane osobowe do GIODO lub do rejestru wewnętrznego oraz że ABI co najmniej dwukrotnie przeprowadził szkolenie w tym zakresie. Oba zbiory zostały w trakcie kontroli zarejestrowane w GIODO.

Powszechnym było nieaktualizowanie zbiorów w rejestrze GIODO

W prawie wszystkich skontrolowanych jednostkach (w 28[47] z 31) nie wywiązywano się również z określonego w art. 41 ust. 2 i 3 ustawy o ochronie danych osobowych, obowiązku aktualizacji w rejestrze GIODO danych dotyczących zbiorów już zarejestrowanych[48]. W konsekwencji rejestr ten nie zawierał aktualnych informacji o zakresie danych faktycznie gromadzonych w zbiorach prowadzonych w poszczególnych jednostkach lub o zaprzestaniu prowadzenia danego zbioru. W 17[49] jednostkach brak zgłoszeń aktualizacji dotyczył zbiorów, w których przetwarzane były dane wrażliwe, o których mowa w art. 27 ustawy o ochronie danych osobowych.

Przykład

Burmistrz Kleszczel (ADO), nie zgłosił GIODO zmian danych rejestracyjnych sześciu[50] zbiorów danych osobowych, mimo że zakres przetwarzanych w nich danych osobowych w latach 2016–2018 (do 6 lutego) był szerszy od wskazanego w rejestrze GIODO. Przetwarzane przez pracowników Urzędu dane obejmowały oprócz danych zgłoszonych do rejestracji także m.in.: nazwisko rodowe; nazwiska rodziców; numer aktu urodzenia; stan cywilny; status wyborczy; informacje o rozwodzie; datę i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko; imię i nazwisko osoby przysposabiającej dziecko; zmianę nazwiska dziecka; daty rozwiązania poprzedniego małżeństwa, rozwodu, zgonu współmałżonka; numer aktu zgonu. Zgodnie z art. 41 ust. 2 i ust. 3 ustawy o ochronie danych osobowych,

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

[47] GOPS w: Boćkach, Dobrzyniewie Dużym, Rudce i Sztabinie, MGOPS w: Czarnej Białostockiej, Krynkach i Suchowoli, MOPR w Suwałkach, MOPS w: Siemiatyczach, Supraślu i Zambrowie, OPS w Ciechanowcu, starostwa powiatowe w: Białymstoku, Hajnówce, Kolnie, Łomży i Zambrowie, urzędy gmin w: Jaświłach, Klukowie, Milejczycach i Szudziałowie, urzędy miejskie w: Bielsku Podlaskim, Kleszczelach, Michałowie, Suwałkach, Szczuczynie, Szepietowie i Wysokiem Mazowieckiem.

[48] Od 25 maja 2018 r. RODO nie przewiduje obowiązku rejestracji zbiorów danych osobowych oraz ich aktualizacji w rejestrze GIODO.

[49] GOPS w: Boćkach, Dobrzyniewie Dużym, Rudce i Sztabinie, MGOPS w: Czarnej Białostockiej, Krynkach i Suchowoli, MOPR w Suwałkach, MOPS w: Siemiatyczach, Supraślu i Zambrowie, Starostwo Powiatowe w Białymstoku, urzędy gmin w Jaświłach i Szudziałowie, urzędy miejskie w: Bielsku Podlaskim, Kleszczelach i Suwałkach.

[50] Akta stanu cywilnego, Ewidencja członków formacji obrony cywilnej (Ochrona ludności), Ewidencja rejestracji pojazdów, Ewidencja wniosków w sprawie dodatków mieszkaniowych, Gospodarka nieruchomościami (Rejestr umów dzierżawy na grunty zasobu gminy), Rejestr Mieszkańców.

zmiana w zbiorze danych powinna być zgłoszona w terminie 30 dni od dnia jej dokonania, a w przypadku danych wrażliwych – przed dokonaniem zmiany w zbiorze. Burmistrz Kleszczel wyjaśnił, że było to wynikiem przeoczenia. W trakcie kontroli NIK (9 lutego 2018 r.) dokonano aktualizacji danych rejestracyjnych jednego[51] z tych sześciu zbiorów.

W 12 jednostkach pracownicy przetwarzali dane bez upoważnienia ADO

W 12 (z 31) jednostkach pracownikom umożliwiono dostęp i przetwarzanie danych w zbiorach danych osobowych, chociaż nie posiadali upoważnienia, wydanego przez ADO. Sytuacja taka dotyczyła od jednej do 25[52] osób, którym umożliwiono dostęp do kilku odrębnych zbiorów danych osobowych. Wyjątkiem był Urząd Miejski w Szepietowie, w którym trzem pracownikom nieposiadającym upoważnień wydanych przez ADO umożliwiono w tym samym czasie dostęp do jednego ze zbiorów. Nieposiadanie upoważnienia stanowiło naruszenie art. 37 ustawy o ochronie danych osobowych i zgodnie z art. 51 tej ustawy było zagrożone sankcją karną. Od 25 maja 2018 r. RODO, w art. 29, normuje obowiązki osób przetwarzających dane z upoważnienia lub na polecenie ADO, ale nie wskazuje sankcji karnych za nieprzestrzeganie tych regulacji.

Kierownicy aż 19 (z 31) jednostek nie wywiązali się z – określonego w art. 39 ust. 1 ustawy o ochronie danych osobowych – obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, która zawierać powinna określone tym przepisem elementy i być aktualna[53]. Nieprawidłowości w tym zakresie dotyczyły głównie nieujęcia w niej danych wszystkich osób, którym zostały nadane upoważnienia bądź niezawarcia informacji o zakresie nadanych im upoważnień oraz identyfikatorów w systemach informatycznych.

Przykłady

W GOPS w Dobrzyniewie Dużym w ewidencji nie wskazano zakresu upoważnienia oraz identyfikatora w systemie informatycznym osób upoważnionych, a także nie ujęto informacji o siedmiu pracownikach Powiatowego Urzędu Pracy w Białymstoku, którym udzielono upoważnienia do przetwarzania danych osobowych pochodzących z GOPS. Kierownik GOPS wyjaśniła, że wynika to z niezaktualizowania polityki bezpieczeństwa oraz ujęcia na odrębnej liście (stanowiącej część porozumienia z PUP w Białymstoku) upoważnień udzielonych pracownikom tej jednostki.

W Urzędzie Gminy Milejczyce nie prowadzono ewidencji osób upoważnionych. Wójt Gminy wyjaśnił, że było to wynikiem braku wystarczającej wiedzy w zakresie wymagań dotyczących ochrony danych osobowych.

Tylko w 13 jednostkach powołano ABI

Jedynie w 13[54] jednostkach skorzystano z możliwości powołania ABI, określonej w art. 36a ust. 1 ustawy o ochronie danych osobowych, mimo że regulacje wewnętrzne (polityka bezpieczeństwa lub instrukcja zarządzania systemem informatycznym) przewidywały wyznaczenie takiej

[51] Akta stanu cywilnego.

[52] Starostwo Powiatowe w Łomży.

[53] RODO nie przewiduje już takiej ewidencji. Wprowadza zaś obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, obejmującego inny zakres danych.

[54] GOPS w Narewce, MGOPS w Krynkach, MOPS w Zambrowie, starostwa powiatowe w: Białymstoku, Hajnówce i Łomży, urzędy gmin w Jaświłach i Klukowie, urzędy miejskie w: Bielsku Podlaskim, Michałowie, Suwałkach, Szczuczynie i Wysokiem Mazowieckiem.

osoby w 24[55] skontrolowanych jednostkach[56]. Regulacje te określały również katalog zadań przewidzianych do realizacji przez osobę na tym stanowisku. Najczęściej było to: opracowanie, aktualizacja i nadzorowanie przestrzegania obowiązujących zasad bezpieczeństwa danych osobowych, prowadzenie rejestru osób upoważnionych do przetwarzania danych, prowadzenie postępowań w przypadku naruszenia bezpieczeństwa przetwarzania danych, nadzór nad przestrzeganiem przez pracowników zasad ochrony danych, organizowanie szkoleń dla pracowników wykorzystujących systemy informatyczne do przetwarzania danych, wdrażanie systemu informatycznego. Niewyznaczenie osób do pełnienia obowiązków ABI powodował, że wymienione zadania nie były realizowane wcale lub wykonywano je w niewielkim stopniu.

Jedynie czterech ABI wywiązało się w pełni ze swoich obowiązków

W jednostkach, w których powołano ABI wystąpiły przypadki nierealizowania przez nich zadań ustawowych, do których byli zobowiązani na podstawie art. 36a ust. 2 ustawy o ochronie danych osobowych i wskazanych w dokumentacji wewnętrznej. Taka sytuacja miała miejsce w dziewięciu[57] z 13 jednostek. Najczęstsze zaniedbania ze strony ABI dotyczyły m.in.: nieprowadzania lub prowadzenia w sposób nierzetelny rejestru przetwarzanych zbiorów danych[58], nieprzeprowadzania kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, niesporządzania dla ADO sprawozdań w tym zakresie, a także nieaktualizowania dokumentacji opisującej przetwarzanie danych osobowych.

Przykład

W MGOPS w Krynkach ABI nie opracowywał planu sprawdzeń oraz nie przeprowadzał sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, o których mowa w §§ 3–5 rozporządzenia w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (wymóg przeprowadzenia sprawdzeń wynika też z art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych). ABI wyjaśnił, że nie opracowano planu sprawdzeń z uwagi na nadmiar obowiązków służbowych wykonywanych przez ABI. Ponadto ABI nie prowadził rejestru, o którym mowa w art. 36a ust. 2 pkt 2 powołanej ustawy, zawierającego wykaz zbiorów danych osobowych przetwarzanych w tej jednostce – jak wyjaśnił ABI – z powodu przeoczenia spowodowanego nadmiarem wykonywanych obowiązków. Na stanowisko ABI została powołana jedna z pracownic Ośrodka, realizująca jednocześnie szereg zadań związanych z pomocą społeczną.

[55] GOPS w: Dobrzyniewie Dużym, Narewce i Rudce, MGOPS w Krynkach i Suchowoli, MOPR w Suwałkach, MOPS w Siemiatyczach i Zambrowie, OPS w Ciechanowcu, starostwa powiatowe w: Białymstoku, Hajnówce, Kolnie, Łomży i Zambrowie, urzędy gmin w Jaświłach, Klukowie, Milejczycach i Sidrze, urzędy miejskie w: Bielsku Podlaskim, Michałowie, Nowogrodzie, Suwałkach, Szczuczynie i Wysokiem Mazowieckiem.

[56] Od 25 maja 2018 r. RODO likwiduje stanowisko ABI. W jego miejsce należy powołać Inspektora Ochrony Danych.

[57] MGOPS w Krynkach, MOPS w Zambrowie, starostwa powiatowe w Hajnówce i Łomży, urzędy gmin w Jaświłach i Klukowie, urzędy miejskie w: Bielsku Podlaskim, Michałowie i Szczuczynie.

[58] Od 25 maja 2018 r. wprowadza się obowiązek prowadzenia rejestru czynności przetwarzania wewnątrz jednostki.

W 14 jednostkach ADO nie wywiązywali się ze swoich obowiązków

W przypadku niepowołania ABI ustawa o ochronie danych osobowych nakłada na ADO dodatkowe obowiązki określone w art. 36a ust 2 pkt 1 tej ustawy. W blisko połowie (14[59]) skontrolowanych jednostek zadania te nie były realizowane. ADO nie dokonywali sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz nie nadzorowali opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 powołanej ustawy[60]. Na dokumentację tę, opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, zgodnie z § 3 ust 1 rozporządzenia w sprawie dokumentacji i warunków technicznych, składają się: polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Szczegółowe wymagania wobec tych dokumentów zostały określone w §§ 4 i 5 ww. rozporządzenia. Dotyczą one m.in. określenia: [1] miejsc, w których przetwarzane są dane osobowe; [2] środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych; [3] procedury nadawania uprawnień do przetwarzania; [4] procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; [5] sposobu, miejsca i okresu przechowywania kopii zapasowych baz danych. Dokumenty te zostały opracowane we wszystkich skontrolowanych jednostkach, ale np. w Urzędzie Miejskim w Kleszczelach dopiero 28 grudnia 2017 r., tj. w trakcie kontroli NIK.

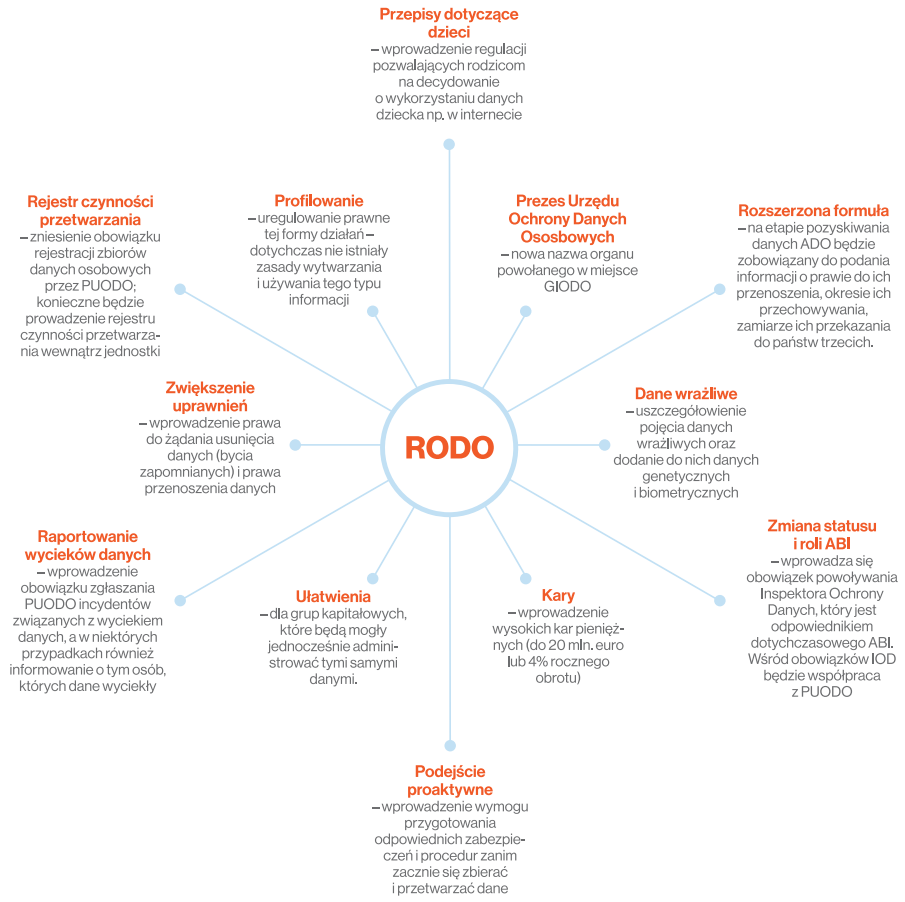
RODO

Główne zmiany, jakie niesie za sobą wprowadzenie z dniem 25 maja 2018 r. przepisów RODO, obrazuje poniższy diagram.

[59] GOPS w Boćkach i Dobrzyniewie Dużym, MGOPS w Czarnej Białostockiej, MOPS w Siemiatyczach, OPS w Ciechanowcu, starostwa powiatowe w: Kolnie, Łomży i Zambrowie, urzędy gmin w: Klukowie, Milejczycach i Sidrze, urzędy miejskie w: Kleszczelach, Nowogrodzie i Szepietowie.

[60] Od 25 maja 2018 r. obowiązek wdrożenia, poddawania przeglądom oraz uaktualniania środków technicznych i organizacyjnych zapewniających właściwe przetwarzania danych osobowych, wynika z art. 24 RODO.

Diagram nr 5
Zmiany wprowadzane RODO



Źródło: Opracowanie własne NIK na podstawie przepisów RODO i ustawy o ochronie danych osobowych.

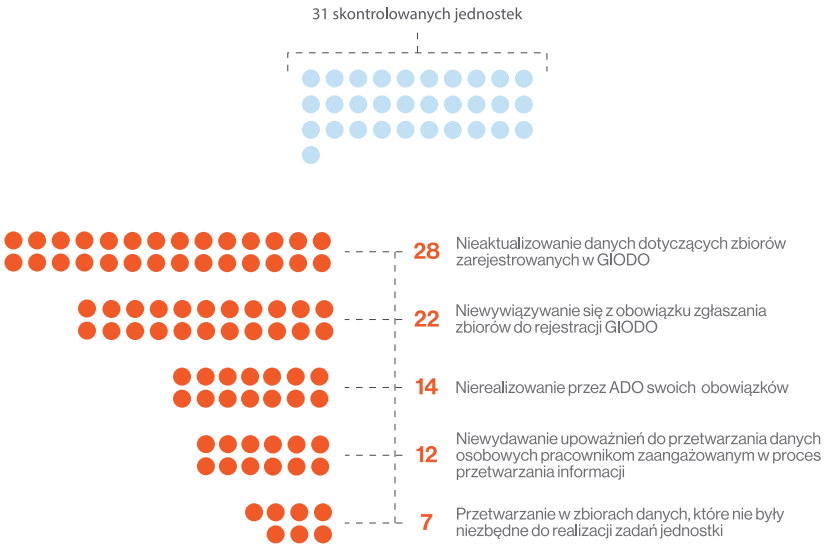
Tylko w sześciu jednostkach część pracowników przeszkolono w związku z RODO

Pomimo zmian w zakresie przetwarzania danych osobowych, wynikających z RODO, działania polegające na zapoznaniu się z nowymi przepisami dotyczącymi ochrony danych osobowych zostały podjęte jedynie w sześciu[61] z (31) jednostek. Wybrani pracownicy tych jednostek (głównie ABI) w latach 2017 i 2018 wzięli udział w szkoleniach, których tematyka dotyczyła zmian w ochronie danych osobowych, jakie zostaną wprowadzone w związku z wejściem w życie ww. rozporządzenia.

[61] GOPS w Dobrzyniewie Dużym i Sztabinie, MOPR w Suwałkach, urzędy miejskie w: Bielsku Podlaskim, Kleszczelach i Suwałkach.

Diagram nr 7

Najczęściej występujące nieprawidłowości związane z ochroną danych osobowych



Źródło: Opracowanie własne na podstawie wyników kontroli NIK.

6. ZAŁĄCZNIKI

6.1. Metodyka kontroli i informacje dodatkowe

Cel główny kontroli

Celem głównym kontroli było ustalenie, czy elektroniczne zasoby informacyjne w jednostkach samorządu terytorialnego są właściwie chronione.

Cele szczegółowe

Celami szczegółowymi w jednostkach objętych kontrolą było ustalenie, czy:

- przyjęte rozwiązania dotyczące dostępu do poszczególnych systemów informatycznych i usług sieciowych zabezpieczały przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych,
- opracowano wymaganą dokumentację i procedury dotyczące ochrony danych,
- sposób przechowywania oraz zabezpieczenia danych odpowiadał przepisom oraz przyjętym procedurom i zapewniał ich ochronę,
- przetwarzane dane mieściły się w ramach uprawnień wynikających z przepisów oraz zadań, do jakich jednostka została powołana.

Zakres podmiotowy

Kontrolą objęte zostały trzy starostwa powiatowe, 11 urzędów gmin (w tym jeden urząd miasta na prawach powiatu) oraz 11 ośrodków pomocy społecznej (w tym jeden w mieście na prawach powiatu).

Przy wyborze podmiotów do kontroli uwzględniono zakres oraz aktualność informacji zawartych w rejestrze zbiorów danych osobowych oraz w rejestrze ABI prowadzonym przez GIODO. Kontrolą objęte zostały jednostki, które zgłosiły GIODO do zarejestrowania relatywnie małą liczbę zbiorów danych osobowych w porównaniu z pozostałymi podmiotami tego rodzaju. Kolejnym czynnikiem był fakt powołania lub niepowołania ABI w danej jednostce. Przy wyborze podmiotów brano również pod uwagę teren, na którym działa dana jednostka (wiejski, wiejsko-miejski, miejski), aby wybrana do kontroli grupa była reprezentatywna i jak najbardziej oddawała rzeczywisty stan badanej działalności w województwie podlaskim.

Kryteria kontroli

Kontrolę we wszystkich jednostkach prowadzono na podstawie art. 2 ust. 2 ustawy o NIK. Kryteriami kontroli były: legalność i rzetelność.

Okres objęty kontrolą

Kontrolą objęto okres od 1 stycznia 2016 r. do czasu zakończenia czynności kontrolnych oraz działania wcześniejsze, jeśli miały związek z przedmiotem kontroli. Kontrole rozpoczęto 2 listopada 2017 r., a zakończono 27 lutego 2018 r.

Wnioski pokontrolne

Wyniki kontroli przedstawiono w 25 wystąpieniach pokontrolnych, w których sformułowano 225 wniosków pokontrolnych. Wg stanu na 18 lipca 2018 r. 136 z nich zostało zrealizowanych, 80 było w trakcie realizacji, a dziewięciu nie zrealizowano.

W wystąpieniach do kierowników jednostek objętych kontrolą wnioskowano głównie o:

- nadanie użytkownikom komputerów uprawnień w systemach operacyjnych odpowiadających ich zakresom obowiązków (odebranie uprawnień administratorów systemu operacyjnego);
- przeprowadzanie okresowych analiz utraty integralności, dostępności lub poufności informacji oraz corocznych audytów wewnętrznych w tym zakresie;

- zapewnienie skutecznego monitorowania dostępu do zasobów informacyjnych oraz zapewnienie skutecznej ochrony fizycznej posiadanej infrastruktury informatycznej;
- wywiązanie się z obowiązków dotyczących rejestracji i aktualizacji danych w rejestrze prowadzonym przez GIODO oraz wydawanie upoważnień pracownikom przetwarzającym dane w tych zbiorach;
- zapewnienie szkoleń, o których mowa w 20 ust. 2 pkt 6 rozporządzenia KRI, wszystkim pracownikom zaangażowanym w proces przetwarzania informacji,
- aktualizację dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych oraz realizację zadań z niej wynikających;
- gromadzenie bieżących informacji o posiadanym sprzęcie i oprogramowaniu służącym do przetwarzania danych, obejmujących ich rodzaj i konfigurację oraz zapewnienie jego aktualizacji.

Do jednego z wystąpień pokontrolnych kierownik jednostki (Starosta Powiatu Białostockiego) złożył sześć zastrzeżeń, z których jedno zostało uwzględnione w części, a pozostałe oddalono. Dotyczyły one głównie oceny kontrolowanej działalności.

Pozostałe informacje

Do kontroli wykorzystano metodykę określoną w podręczniku kontroli systemów informatycznych dla najwyższych organów kontroli, opracowanym przez INTOSAI Working Group on IT Audit (WGITA) i zatwierdzonym przez XXI Międzynarodowy Kongres Najwyższych Organów Kontroli w Pekinie w październiku 2013 roku.

W każdej z jednostek objętych kontrolą do oceny, czy przyjęte rozwiązania dotyczące dostępu do poszczególnych systemów informatycznych i usług sieciowych zabezpieczały przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych, wykorzystywano opinię biegłego w dziedzinie bezpieczeństwa systemów informatycznych.

Kontrola była poprzedzona kontrolą rozpoznawczą przeprowadzoną od stycznia do kwietnia 2017 roku w sześciu j.s.t. (dwóch starostwach powiatowych, dwóch gminach oraz dwóch ośrodkach pomocy społecznej) z terenu województwa podlaskiego[62].

Wykaz jednostek kontrolowanych

Lp.	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej	Ocena kontrolowanej działalności
1.	GOPS w Boćkach	Barbara Tołoczko	negatywna
2.	GOPS w Dobrzyniewie Dużym	Agata Krupska	negatywna
3.	GOPS w Narewce	Elżbieta Potoniec	pozytywna mimo stwierdzonych nieprawidłowości

[62] Kontrola R/17/001 *„Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim”*, którą objęto: GOPS w Rudce, MGOPS w Krynkach, starostwa powiatowe w Hajnówce i Kolnie, Urząd Gminy Jaświły, Urząd Miejski w Michałowie. We wszystkich zastosowano opisową ocenę ogólną kontrolowanej działalności.

Lp.	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej	Ocena kontrolowanej działalności
4.	GOPS w Sztabinie	Dorota Barbara Salik	negatywna
5.	MGOPS w Czarnej Białostockiej	Agnieszka Dyda	negatywna
6.	MGOPS w Suchowoli	Barbara Pikus	negatywna
7.	MOPR w Suwałkach	Leszek Lewoc	pozytywna mimo stwierdzonych nieprawidłowości
8.	MOPS w Siemiatyczach	Ewa Romaniuk	negatywna
9.	MOPS w Supraślu	Małgorzata Ostrowska	negatywna
10.	MOPS w Zambrowie	Janina Komorowska	negatywna
11.	OPS w Ciechanowcu	Marzena Kryńska	negatywna
12.	Starostwo Powiatowe w Białymstoku	Antoni Pełkowski	negatywna
13.	Starostwo Powiatowe w Łomży	Elżbieta Parzych	negatywna
14.	Starostwo Powiatowe w Zambrowie	Robert Maciej Rosiak	pozytywna mimo stwierdzonych nieprawidłowości
15.	Urząd Gminy w Klukowie	Piotr Uszyński	negatywna
16.	Urząd Gminy w Milejczycach	Jerzy Iwanowiec	negatywna
17.	Urząd Gminy w Sidrze	Jan Hrynkiewicz	negatywna
18.	Urząd Gminy w Szudziałowie	Tadeusz Tokarewicz	negatywna
19.	Urząd Miasta Bielsk Podlaski	Jarosław Borowski	pozytywna mimo stwierdzonych nieprawidłowości
20.	Urząd Miasta Wysokie Mazowieckie	Jarosław Siekierko	pozytywna mimo stwierdzonych nieprawidłowości
21.	Urząd Miejski w Kleszczelach	Aleksander Sielicki	negatywna
22.	Urząd Miejski w Nowogrodzie	Grzegorz Andrzej Palka	pozytywna mimo stwierdzonych nieprawidłowości
23.	Urząd Miejski w Suwałkach	Czesław Renkiewicz	pozytywna mimo stwierdzonych nieprawidłowości
24.	Urząd Miejski w Szczuczynie	Artur Kuczyński	pozytywna mimo stwierdzonych nieprawidłowości
25.	Urząd Miejski w Szepietowie	Robert Lucjan Wyszyński	negatywna

6.2. Analiza stanu prawnego

1. Kluczowe uwarunkowania w odniesieniu do urządzeń i systemów informatycznych wykorzystywanych do przetwarzania danych zostały określone w rozporządzeniu KRI oraz rozporządzeniu w sprawie dokumentacji oraz warunków technicznych. Rozporządzenie KRI wskazuje m.in. wymogi w zakresie zarządzania bezpieczeństwem informacji. Przepisy tego rozporządzenia zobowiązują podmioty realizujące zadania publiczne do opracowania, ustanowienia, wdrożenia, monitorowania i dokonywania przeglądów systemu zarządzania bezpieczeństwem informacji. Zgodnie z § 23 rozporządzenia KRI, systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie ww. rozporządzenia, tj. 31 maja 2012 r., należało dostosować w powyższym zakresie, nie później niż w dniu ich pierwszej istotnej modernizacji. Systemy informatyczne nabywane po tej dacie obligatoryjnie podlegają wymogom rozporządzenia KRI.

W myśl przepisów rozporządzenia KRI, jednostka, aby zabezpieczyć swoje dane powinna zastosować podejście systemowe, w ramach którego będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji. System Zarządzania Bezpieczeństwem Informacji[63] określa wymagania oraz zasady inicjowania, wdrażania, utrzymania i poprawy zarządzania bezpieczeństwem informacji w jednostce oraz zawiera najlepsze praktyki celów stosowania zabezpieczeń w następujących obszarach zarządzania bezpieczeństwem informacji: [1] polityka bezpieczeństwa informacji, [2] organizacja bezpieczeństwa informacji, [3] zarządzanie aktywami, [4] bezpieczeństwo osobowe, [5] bezpieczeństwo fizyczne i środowiskowe, [6] zarządzanie systemami i sieciami, [7] kontrola dostępu, [8] uzyskiwanie, rozwój i utrzymanie systemów informacyjnych, [9] zarządzanie incydentami związanymi z bezpieczeństwem informacji, [10] zarządzanie ciągłością działania, [11] zgodność.

Zgodnie z § 20 ust. 3 rozporządzenia KRI, obowiązki, o których mowa w § 20 ust. 1 i 2, uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem; PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Stosownie do załącznika A PN-ISO/IEC 27001:2014-12:

1. Zbiór polityk bezpieczeństwa informacji powinien być opracowany, zatwierdzony przez kierownictwo, opublikowany i zakomunikowany pracownikom (pkt 5.1.1).

[63] Na podstawie normy PN-EN ISO/IEC 27002:2017.

2. Polityki bezpieczeństwa informacji należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne (pkt 5.1.2).
3. Wszyscy pracownicy urzędu powinni przejść stosowne kształcenie i szkolenie uświadamiające oraz regularnie otrzymywać aktualizacje polityk i procedur związanych z ich stanowiskiem pracy (pkt 7.2.2).
4. Wszystkie aktywa powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany spis wszystkich aktywów informatycznych. Aktualna inwentaryzacja m.in. sprzętu informatycznego powinna także zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie odtworzenie po katastrofie lub innym zdarzeniu losowym (pkt 8.1.1).
5. Przydzielanie i wykorzystywanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować. Ma to na celu uniemożliwienie użytkownikom systemów informatycznych niebędących pracownikami służb informatycznych w jednostce samodzielnej instalacji oprogramowania na komputerach służbowych. Powszechną praktyką w tym zakresie jest nieprzyznawanie praw administracyjnych do systemu operacyjnego (pkt 9.2.3).
6. Kopie zapasowe należy regularnie wykonywać i testować zgodnie z ustaloną polityką kopii zapasowych (pkt 12.3.1).

Z kolei zarządzanie uprawnieniami użytkowników, zgodnie z załącznikiem A normy PN-ISO/IEC 27001:2007, pkt 9.2.1, powinno być realizowane w oparciu o formalną procedurę rejestrowania i wyrejestrowywania użytkowników. Procedura taka winna opisywać obowiązki zarówno komórki IT, jak i kierownictwa jednostki. Kierownicy poszczególnych komórek organizacyjnych decydują o uprawnieniach pracowników, a w przypadku zmian zadań realizowanych przez pracownika winni bezzwłocznie, pisemnie występować o zmianę uprawnień w systemie IT.

Rada Ministrów uchwałą nr 52/2017 z dnia 27 kwietnia 2017 r. przyjęła Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Ich celem głównym jest zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych. Obowiązanymi do realizacji Krajowych Ram są członkowie Rady Ministrów oraz organy i jednostki organizacyjne im podległe lub przez nich nadzorowane.

Bezpieczeństwo informacji, co też zostało podkreślone w podręczniku kontroli systemów IT oznacza, że muszą być spełnione trzy zasadnicze wymagania: poufność – czyli zapewnienie, że informacje są dostępne tylko dla osób uprawnionych do dostępu (odpowiednie nadanie uprawnień w systemie IT powoduje, że każdy użytkownik ma dostęp tylko do danych dla niego przeznaczonych); integralność – zagwarantowanie dokładności i kompletności informacji oraz metod ich przetwarzania (pewność, że odczytywana informacja, np. mail nie został zmodyfikowany w trakcie

przesyłania do odbiorcy bez wiedzy i zgody nadawcy); dostępność – czyli zapewnienie upoważnionym użytkownikom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami (np. posiadanie dostępu do danych w każdym czasie). Ponadto, jak wskazano w podręczniku kontroli systemów IT, bezpieczeństwo informacji polega również na minimalizowaniu ekspozycji na zagrożenia w oparciu o zarządzanie ryzykiem we wszystkich obszarach modelu ładu informatycznego. Niewdrożenie i niemonitorowanie procesów łagodzenia ryzyka w jednym obszarze może spowodować szkody w całej organizacji.

2. Stosownie do art. 47 Konstytucji RP, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Ponadto w art. 51 ust. 1–4 Konstytucji RP określono, że:

- nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby,
- władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym,
- każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, a ograniczenie tego prawa może określić ustawa,
- każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą,
- zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Przepisy regulujące zasady przetwarzania danych osobowych wprowadzone zostały do polskiego ustawodawstwa ustawą o ochronie danych osobowych, która (jak wskazano na stronie internetowej GIODO[64]) wzorowana była w znacznej mierze na zasadach ustanowionych Dyrektywą 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[65].

W art. 1 ustawy o ochronie danych osobowych wskazano, że każdy ma prawo do ochrony dotyczących go danych osobowych, a przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą lub dobro osób trzecich w zakresie i trybie określonym tą ustawą. Ponadto wprowadzono w niej zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Obowiązek stosowania ustawy o ochronie danych osobowych został nałożony zarówno na organy państwowe, organy samorządu terytorialnego, państwowe i komunalne jednostki organizacyjne, jak również podmioty niepubliczne realizujące zadania publiczne, osoby fizyczne i osoby prawne oraz jednostki organizacyjne niebędące osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych (art. 3).

64 http://www.giodo.gov.pl/pl/484

65 Dz.U. UE.L.1995.281.31.

W rozumieniu art. 6 tej ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Ustawa o ochronie danych osobowych określa zasady zabezpieczenia danych oraz odpowiedzialność za ich przestrzeganie. Obowiązki z tego zakresu nałożone zostały na ADO, którym – w myśl art. 7 pkt 4 tej ustawy – jest organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.

- Stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1).
- Prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz środki zapewniające ochronę danych (art. 36 ust. 2). Szczegółowe regulacje w tym zakresie zawiera rozporządzenie w sprawie dokumentacji oraz warunków technicznych, zgodnie z którym na ww. dokumentację składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Ponadto wymagana ono przyjęcia odpowiednich poziomów bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, uwzględniających kategorie przetwarzanych danych oraz zagrożenia.
- Zgłaszanie zbiorów danych do rejestracji GIODO (art. 40).

Art. 27 ustawy o ochronie danych osobowych określa katalog danych „wrażliwych", których przetwarzanie jest zabronione lub ograniczone. Należą do nich: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

W związku z możliwością powołania ABI przez ADO, w ustawie określono wymagania wobec osoby mogącej pełnić tę funkcję oraz zakres jej obowiązków. Tryb i sposób realizacji zadań ABI oraz sposób prowadzenia rejestru zbiorów danych został wskazany w rozporządzeniu w sprawie sposobu prowadzenia rejestru zbiorów danych oraz w rozporządzeniu w sprawie trybu i sposobu realizacji zadań przez ABI.

Nieprzestrzeganie przepisów dotyczących ochrony danych osobowych wiąże się z sankcjami karnymi, tj. karą grzywny, ograniczenia wolności lub nawet jej pozbawienia. I tak np.: zgodnie z art. 49 ustawy o ochronie danych osobowych (obowiązującej do 25 maja 2018 r.), kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2, natomiast jeżeli przetwarzanie dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech. **Odpowiedzialność karna za wszystkie ww. czyny została utrzymana także w obowiązującym od 25 maja 2018 r. porządku prawnym, tj. art. 107 nowej ustawy o ochronie danych osobowych.**

Z kolei art. 51 oraz 52 ustawy o ochronie danych osobowych (obowiązujące do 25 maja 2018 r.) wskazywały, że kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2, a kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. **Od 25 maja 2018 r. przepisy nowej ustawy o ochronie danych osobowych nie przewidują sankcji karnych za udostępnienie lub umożliwienie dostępu do danych osobom nieupoważnionym, jak również naruszenie obowiązku zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.**

Ponadto zgodnie z obowiązującym do 25 maja 2018 r. art. 53 ustawy o ochronie danych osobowych, karze grzywny, karze ograniczenia wolności albo pozbawienia wolności do roku podlegał również każdy kto, będąc do tego obowiązany, nie zgłaszał do rejestracji zbioru danych. **Nowa ustawa o ochronie danych osobowych znosi obowiązek rejestracji zbiorów oraz nie przewiduje sankcji karnych w tym zakresie.**

Od 25 maja 2018 r. w krajach członkowskich UE bezpośrednio obowiązuje RODO, częściowo odmiennie normujące zagadnienia ochrony danych osobowych.

Wprowadzone zmiany dotyczą m.in. obowiązkowego wyznaczenia przez organ lub podmiot publiczny inspektora ochrony danych, którego zadania są częściowo odmienne od zadań ABI (art. 37–39 rozporządzenia). W miejsce kilku dotychczas wymaganych ewidencji i rejestrów wprowadzono jeden rejestr czynności przetwarzania (art. 30).

Inaczej określono też obowiązki związane z bezpieczeństwem ochrony danych osobowych, akcentując konieczność indywidualnej oceny skutków przetwarzania dla ochrony tych danych, jeszcze przed rozpoczęciem takiego przetwarzania (art. 35).

Rozszerzono uprawnienia osób fizycznych, których dane są przetwarzane i powiązano je z odpowiednimi obowiązkami podmiotów przetwarzających dane (art. 5–22), w szczególności prawo do sprzeciwu lub prawo do usunięcia danych (bycia zapomnianym). Administrator powinien zgłaszać stwierdzone naruszenia ochrony danych osobowych zarówno organowi nadzorczemu (od 25 maja 2018 r. PUODO), jak i zawiadamiać o nich osoby fizyczne, których naruszenia dotyczą (art. 32 i 34 rozporządzenia).

Rozporządzenie przewiduje też doprecyzowanie szeregu wymogów dotyczących ochrony przetwarzania danych w komunikatach organu nadzorczego, publikowanych na jego stronie internetowej czy w zatwierdzanych przez ten organ kodeksach postępowania lub wiążących regułach korporacyjnych.

Organom nadzorczym oprócz zadań edukacyjnych i informacyjnych przyznano także uprawnienia władcze, jak np. uprawnienia naprawcze w zakresie prowadzonych postępowań (art. 58) i prawo nakładania administracyjnych kar pieniężnych (art. 83).

Wprowadzono także nową ustawę o ochronie danych osobowych (wraz z aktami wykonawczymi), normującą głównie status, zadania i uprawnienia PUODO, w nawiązaniu do przepisów RODO.

6.3 Wykaz aktów prawnych dotyczących kontrolowanej działalności

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, ze zm.)
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).
3. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570).
4. Ustawa z 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524, ze zm.).
5. Rozporządzenie 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 (Dz. U. z 2017 r. poz. 2247).
6. Rozporządzenie 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 do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)
7. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. poz. 745).
8. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych osobowych (Dz. U. Nr 229, poz. 1536).
9. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. poz. 1934).
10. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 04.05.2016 s. 1)

6.4. Wykaz podmiotów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Minister Cyfryzacji
8. Minister Spraw Wewnętrznych i Administracji
9. Senacka Komisja Samorządu Terytorialnego i Administracji Państwowej
10. Sejmowa Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
11. Sejmowa Komisja do Spraw Kontroli Państwowej
12. Sejmowa Komisja Samorządu Terytorialnego i Polityki Regionalnej
13. Sejmowa Komisja Administracji i Spraw Wewnętrznych
14. Prezes Urzędu Ochrony Danych Osobowych
15. Wójtowie gmin, burmistrzowie i prezydenci miast
16. Starostowie powiatów
17. Kierownicy ośrodków pomocy społecznej