Rzeszów, dnia 30 kwietnia 2018 r.

Urząd Miasta i Gminy Czarne
ul. Moniuszki 12
77-330 Czarne

AW.Cz.1.2018

Egz. Nr 1

Sprawozdanie
z zadania audytowego przeprowadzonego na rzecz Urzędu Miasta i Gminy w Czarne

Temat: *Funkcjonowanie systemu bezpieczeństwa teleinformatycznego w Urzędzie Miasta i Gminy w Czarnem.*

Audytor wewnętrzny:

Marek Żuczek

Zadanie audytowe przeprowadzono zgodnie z międzynarodowymi standardami audytu wewnętrznego

Rzeszów 2018

Zadanie audytowe zostało przeprowadzone zgodnie z planem audytu wewnętrznego na 2018 rok w Urzędzie Miasta i Gminy w Czarnem.

Audytor wewnętrzny postanowił objąć zadaniem audytowym następujące obszary ryzyka:

1. Adekwatność i aktualność regulacji wewnętrznych w zakresie dotyczącym ochrony danych osobowych;
2. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
3. Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
4. Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
5. Ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
6. Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.

Termin, w którym przeprowadzono zadanie audytowe: marzec/kwiecień 2018 r.

Badany okres:

2015-2018.

Kryteria oceny:

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1], zwana dalej „ustawą";
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany

[1] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, t. jedn., Dz. U. z 2016 r. poz. 922.

informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[2], zwane dalej „rozporządzeniem";

- 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 służące do przetwarzania danych osobowych[3];
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez Administratora Bezpieczeństwa Informacji[4];
- Zarządzenie Nr 338/09 Burmistrza Gminy Czarne z dnia 17.04.2009 r. *„w sprawie ochrony danych osobowych w Urzędzie Miasta i Gminy w Czarnem, wprowadzenia dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy teleinformatyczne służące do przetwarzania danych osobowych.";*
- „Instrukcja w sprawie trybu postępowania przy przetwarzaniu danych osobowych podlegających ochronie w Urzędzie Miasta i Gminy w Czarnem" – stanowiąca załącznik nr 1 do Zarządzenia Nr 338/09;
- „Polityka Bezpieczeństwa Ochrony Danych Osobowych", zwana dalej „polityką bezpieczeństwa Urzędu Miasta i Gminy w Czarnem" - stanowiąca załącznik nr 2 do Zarządzenia Nr 338/09;
- „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji" - stanowiąca załącznik nr 3 do Zarządzenia Nr 338/09;
- „Instrukcja postępowania w przypadku naruszenia bezpieczeństwa danych osobowych" - stanowiąca załącznik nr 4 do Zarządzenia Nr 338/09;
- „Polityka zarządzania oprogramowaniem Urzędu Miasta i Gminy w Czarnem" - stanowiąca załącznik nr 5 do Zarządzenia Nr 338/09;

---

[2]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, t. jedn., Dz. U. z 2016 r. poz 113,

[3]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 służące do przetwarzania danych osobowych, Dz. U. z 2004 r. Nr 100 poz. 1024.

[4] Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez Administratora Bezpieczeństwa Informacji, Dz. U. z 2015 r. poz. 745.

- Zarządzenie Nr 0050.170.2013 Burmistrza Czarnego z dnia 31 grudnia 2013 zmieniające zarządzenie w sprawie ochrony danych osobowych w Urzędzie Miasta i Gminy w Czarnem, wprowadzenia dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy teleinformatyczne służące do przetwarzania danych osobowych.";

Zakres przedmiotowy zadania audytowego:

Zakresem przedmiotowym zadania audytowego objęto:

- analizę systemu zarządzania bezpieczeństwem informacji,
- kwestię podziału obowiązków osób zaangażowanych w zarządzanie bezpieczeństwem informacji, oraz
- kwestię ochrony danych osobowych.

Podjęte działania i zastosowane techniki przeprowadzania zadania audytowego:

W trakcie zadania audytowego została przeprowadzona rozmowa z Burmistrzem Miasta i Gminy w Czarnem pełniącym jednocześnie funkcję Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji, który został powołany w dniu 18 października 1999 r. (został również wymieniony jak ABI/ASI w Zarządzeniu Burmistrza Gminy Czarne nr 338/09 z dnia 17 kwietnia 2009 r. – funkcja pełniona do dnia 30 czerwca 2015 r.) – tj. osobami bezpośrednio zaangażowanymi w proces zarządzania bezpieczeństwem informacji w badanym okresie. Sporządzono listę pytań kontrolnych, przeprowadzono testy zgodności i testy przeglądowe.

Celem zadania audytowego było zapewnienie Burmistrza, że:

1. obowiązujące w Urzędzie mechanizmy kontrolne i schematy działania dotyczące ochrony danych osobowych są zgodne z przepisami powszechnie obowiązującego prawa;
2. funkcjonujący w Urzędzie system bezpieczeństwa informacji gwarantuje optymalną ochronę informacji przed nieautoryzowanym dostępem;
3. zastosowane w systemie mechanizmy zarządzania informacją, jak również mechanizmy kontroli zarządczej, są adekwatne do znaczenia audytowanych procesów w ramach funkcjonowania całej jednostki.

Tło informacyjne:

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych w art. 36 ust. 2 nakłada na administratora danych osobowych obowiązek prowadzenia dokumentacji, stanowiącej opis sposobu przetwarzania danych oraz środków technicznych i organizacyjnych, stosowanych przez administratora, które mają zapewnić ochronę odpowiednią do zagrożeń oraz kategorii danych, tą ochroną objętych. Jak precyzuje 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 służące do przetwarzania danych osobowych, na dokumentację składają się dwa podstawowe akty, które powinien opracować administrator. Są to:

- polityka bezpieczeństwa;
- instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

Dokumentacja przetwarzania danych osobowych winna być prowadzona w formie papierowej, a za jej wdrożenie odpowiada administrator danych.

Polityka bezpieczeństwa to wewnętrzna regulacja wdrażana w danym podmiocie, zawierająca katalog reguł i zasad postępowania oraz działań, które mają być podjęte bądź są podejmowane w celu zapewnienia prawidłowego i rzetelnego procesu zarządzania informacją spersonalizowaną i jej należytej ochrony. Z założenia polityka bezpieczeństwa odnosi się do całokształtu zagadnień, związanych z ochroną danych osobowych w danej organizacji. Jej kompleksowy charakter przejawia się m.in. w konieczności uregulowania w niej problematyki zabezpieczania danych przetwarzanych tradycyjnie, a także danych przetwarzanych w systemach informatycznych. Minimalny zakres informacji, które powinny się znaleźć w polityce wyznacza ww. rozporządzenie, wymagając od administratora stworzenia:

- wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

- opisu struktury zbiorów danych, wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- sposobu przepływu danych pomiędzy poszczególnymi systemami;
- określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Powyższe elementy mają gwarantować prawidłową identyfikację zasobów informacyjnych, zagrożeń dla bezpieczeństwa informacji oraz obszarów i sposobu przetwarzania danych wewnątrz danego podmiotu. Ponadto, prowadzą do wypracowania jednolitych reguł postępowania z informacją, a także z jej nośnikami oraz wszelkimi urządzeniami stosowanymi w przypadku przetwarzania danych.

Drugi kluczowy dokument, czyli instrukcja zarządzania systemem informatycznym, z oczywistych względów powinna być tworzona tylko przez tych administratorów danych, którzy dane przetwarzają w systemach informatycznych. W dzisiejszych czasach taka sytuacja zachodzi niemalże zawsze. Podobnie jak w przypadku polityki, tak i w przypadku instrukcji, rozporządzenie wyznacza minimalny poziom regulacji, zobowiązując do opisania w omawianym dokumencie:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym (ponadto, wskazać należy osobę odpowiedzialną za te czynności);
- stosowanych metod i środków uwierzytelnienia oraz procedur związanych z ich zarządzaniem i użytkowaniem;
- procedur rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemu;
- procedur tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
- sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;
- sposobu zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- instrukcję postępowania w sytuacji naruszenia bezpieczeństwa informacji;
- sposobu odnotowywania informacji o odbiorcach danych, którym dane zostały udostępnione, a także o dacie i zakresie udostępnienia;

- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Art. 39 ustawy przesądza o konieczności prowadzenia, poza wymienioną dokumentacją, również ewidencji osób upoważnionych do przetwarzania danych. W ewidencji odnotować należy imię i nazwisko osoby upoważnionej, datę nadania, zakres upoważnienia oraz datę jego cofnięcia, a także identyfikator, jeśli dane przetwarzane są w systemie informatycznym.

Opracowanie wskazanych trzech dokumentów jest obowiązkiem każdego administratora danych osobowych, o ile przetwarza dane także w systemie informatycznym. Pamiętać jednak należy, że najistotniejszym zadaniem administratora jest wdrożenie przygotowanej dokumentacji tak, by zagwarantować efektywne wykonywanie zapisów, przewidzianych w dokumentacji przetwarzania danych osobowych.

Prawidłowe administrowanie danymi osobowymi w organizacjach jest obecnie o tyle ważne, że wzrasta świadomość społeczna w tematyce ochrony danych osobowych, a ich nieuprawnione ujawnienie powoduje poważne konsekwencje zarówno dla całej organizacji, jak i – indywidualnie – względem osób odpowiedzialnych.

Tematyka ta jest również częstym przedmiotem kontroli dokonywanej w jednostkach. Zgodnie ze sprawozdaniem z działalności Generalnego Inspektora Ochrony Danych Osobowych (dalej „GIODO") za rok 2015, opublikowanym na stronie internetowej, GIODO przeprowadził w 2015 r. łącznie 175 kontroli (w 2012 r. – 165, 2013 r. -173, 2014 r. – 175). Większość kontroli, jak wskazuje GIODO w sprawozdaniu, prowadzona była na zlecenie Departamentu Skarg i Legislacji oraz Departamentu Rejestracji Zbiorów Danych Osobowych Biura GIODO. Rosnąca aktywność kontrolerów GIODO związana jest w dużej mierze ze wzrostem świadomości osób, których dane dotyczą – do biura GIODO wpływa coraz więcej skarg i coraz więcej z nich wnoszonych jest skutecznie. Jak wskazano w sprawozdaniu GIODO, coraz częściej skarżący przywołują w skargach okoliczności, stanowiące naruszenia przepisów o ochronie danych osobowych, implikując tym samym podjęcie przez GIODO środków kontrolnych przewidzianych w ustawie o ochronie danych osobowych. W roku 2015 złożono aż 2256 skarg związanych z naruszeniem przepisów o ochronie danych osobowych, czyli np. o 377 skargi więcej niż w roku 2013. Postępowania zainicjowane skargami, a także te wszczęte przez GIODO z urzędu, doprowadziły do wydania 647 decyzji, co stanowi wzrost w stosunku do 2014 r., kiedy to wydano w tym zakresie 548 decyzji. Można się spodziewać, że z roku na rok liczba zarówno kontroli, jak i wydawanych po nich decyzji, będzie wzrastać. Nie ulega wątpliwości, że rosnąca liczba kontroli, a także coraz wyższy poziom świadomości

podmiotów, których dotyczą dane, powodują, że administratorzy danych osobowych powinni dokładać jeszcze większych starań, by przetwarzać je zgodnie z zasadami: legalności, celowości, adekwatności, merytorycznej poprawności oraz ograniczenia czasowego. Ponadto, powinni dbać o należytą realizację obowiązków informacyjnych i rejestracyjnych, a także pamiętać, by wdrażać zarówno zabezpieczenia fizyczne, informatyczne, jak i organizacyjno-prawne przetwarzanych przez siebie danych osobowych.

Opis stanu faktycznego:

Tab. nr 1 Test - dokumentacja systemu zarządzania bezpieczeństwem informacji.

Kryterium: Dokumentacja systemu zarządzania bezpieczeństwem informacji.					
Sposób przeprowadzenia czynności audytowych: - Analiza aktów wewnętrznych dot. bezpieczeństwa informacji. - Uzyskiwanie wyjaśnień i informacji od osób odpowiedzialnych za prawidłowe funkcjonowanie systemu bezpieczeństwa informacji oraz od innych pracowników urzędu. - Zapoznawanie się z dokumentami służbowymi na podstawie których można będzie dokonać ustalenia stanu faktycznego, np. zakresy obowiązków pracowników, plany szkoleń, protokoły z przeprowadzonych szkoleń, wykaz pracowników zapoznanych z aktami wewnętrznymi dot. bezpieczeństwa informacji, itp.					
TREŚĆ PYTANIA		**ODPOWIEDZI**		**DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"**	**UWAGI**
		TAK	**NIE**		
1.	Czy określono zasady zarządzania bezpieczeństwem informacji przetwarzanych w jednostce ? Jeśli tak to: a) czy opracowano politykę bezpieczeństwa informacji? b) czy opracowano politykę bezpieczeństwa danych osobowych? c) czy opracowano dokumentację zarządzania systemem informatycznym służącym do przetwarzania danych osobowych? d) czy opracowano instrukcję postępowania w sytuacji naruszenia bezpieczeństwa informacji? e) czy Burmistrz formalnie zatwierdził ww. dokumentację? f) czy zakomunikowano	Tak Tak Tak Tak Tak Tak		Zarządzeniem nr 338/09 z dnia 17.04.2009 r. Burmistrza Gminy Czarne wdrożono dokumenty wewnętrzne stanowiące załączniki do ww. Zarządzenia tj. Instrukcja w sprawie trybu postępowania przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy w Czarnem; Politykę bezpieczeństwa ochrony danych osobowych; Instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji; Instrukcję postępowania w przypadku naruszenia bezpieczeństwa danych osobowych; politykę zarządzania oprogramowaniem. Dokumentacja została	

	dokumentację pracownikom? g) czy i w jaki sposób zapewnia się, że pracownicy zapoznali się z dokumentacją bezpieczeństwa informacji i potwierdzili obowiązek jej przestrzegania? h) czy procedury wewnętrzne są tworzone w oparciu o przepisy prawa w zakresie bezpieczeństwa informacji?	Tak		zatwierdzona przez osobę umocowaną, czyli Burmistrza Miasta i Gminy Czarne. Dokumentacja została podana do wiadomości każdemu z pracowników Urzędu – każdy z pracowników zapoznanie się z dokumentacją poświadczył własnoręcznym podpisem. W dokumentacji wskazana jest podstawa prawna, w oparciu o którą tworzono dokumentację w zakresie bezpieczeństwa informacji.	
2.	Czy polityka bezpieczeństwa informacji zawiera: a) definicje, zakres oraz znaczenie bezpieczeństwa informacji? b) cele i zadania bezpieczeństwa informacji? c) zasady zarządzania informacją? d) nawiązania do regulacji prawnych? e) zakresy obowiązków związanych z zarządzaniem bezpieczeństwem? f) określenie stosowanych zabezpieczeń z uwzględnieniem analizy ryzyka? g) odniesienia do dokumentów uzupełniających?	Tak Tak Tak Tak Tak Tak	Nie	W dokumentacji zawarto stosowne definicje. Zostały zawarte w Załączniku nr 1 do ww. Zarządzenia nr 338/09. Zostały zawarte w dokumentacji dotyczącej ochrony danych osobowych	Z rozmowy przeprowadzonej z ADO wynika, iż pracownicy mają zamykać na klucz szafy w których przechowywane są dokumenty zawierające dane osobowe, stosować zasadę czystego biurka, stanowiska komputerowe usytuowane są w sposób nie pozwalający na „podglądnięcie ekranu" przez osoby postronne, pokoje w przypadku nieobecności pracowników są zamykane na klucz a ten zabierany ze sobą.
3.	Czy polityka bezpieczeństwa danych osobowych zawiera? a) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe? b) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych? c) opis struktury zbiorów danych	Tak Tak		Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe stanowi załącznik A do Polityki Bezpieczeństwa Ochrony Danych Osobowych U M i G Czarne Wykaz zbiorów danych wraz z wykazem programów stanowi załącznik B do ww. Polityki Bezpieczeństwa Opis struktury danych osobowych stanowi załącznik C	

	wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi? d) sposób przepływu danych pomiędzy poszczególnymi systemami? e) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych?	Tak Tak Tak		do ww. Polityki Bezpieczeństwa. Jest opisana w dodatkowej dokumentacji. Jest opisana w dodatkowej dokumentacji	
4.	Czy dokumentacja zarządzania systemem informatycznym reguluje zasady przetwarzania danych osobowych w zakresie: a) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności? b) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem? c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu? d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania? e) sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych? f) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie	Tak Tak Tak Tak Tak Tak		Zasady opisane zostały w Rozdziale II Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji stanowiącą załącznik nr 3 do Zarządzenia nr 338/09 Burmistrza Gminy Czarne z dnia 17 kwietnia 2009 r. Rozdział III ww. Instrukcji. Rozdział IV ww. Instrukcji Rozdział V ww. Instrukcji Rozdział VI ww. Instrukcji Rozdział VII ww. Instrukcji Rozdział VIII ww. Instrukcji Rozdział IX ww. Instrukcji	

	nieuprawnionego dostępu do systemu informatycznego? g) sposób realizacji wymogów odnotowania informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j. t. Dz. U. z 2002 r., poz. 926 z późn. zm.), którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia? h) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych?	Tak Tak			
5.	Czy instrukcja postępowania w sytuacji naruszenia bezpieczeństwa informacji zawiera: a) zasady reagowania na incydent? b) obowiązki Administratora Bezpieczeństwa Informacji? c) zasady raportowania z incydentu i ewidencjonowanie incydentów? d) zasady analizy incydentu?	Tak Tak Tak Tak		Każdy pracownik placówki, który stwierdzi naruszenie bezpieczeństwa danych, niezwłocznie powiadamia o tym ABI, który - po dokładnej analizie incydentu - podejmuje stosowne kroki naprawcze. Następnie ABI sporządza raport z naruszenia bezpieczeństwa danych osobowych.	
6.	Ponadto czy dokumentacja zawiera: a) wymagania szkoleniowe? b) procedury kontrolne? c) procedury postępowania w przypadku naruszenia ochrony informacji? d) czy dokumentacja nie zawiera szczegółowych rozwiązań technicznych dotyczących stosowanych zabezpieczeń? e) czy dokumentacja napisana jest językiem prostym i zrozumiałym dla wszystkich jej odbiorców?	Tak Tak Tak Tak	Nie	Pracownicy są zobowiązani do ścisłego przestrzegania przepisów prawa oraz wewnętrznych zarządzeń i instrukcji regulujących przetwarzanie danych osobowych W instrukcji Postępowania w przypadku naruszenia bezp. danych osobowych wskazano procedury postępowania w przypadku naruszenia ochrony informacji. W dokumentacji wyszczególniono w jaki sposób powinny być zabezpieczone zbiory danych bez wskazania szczegółowych programów/urządzeń zabezpieczających zbiory danych.	W dokumentacji brak jest informacji o procedurze kontrolnej.
7.	Czy dokumentacja przetwarzania danych osobowych zawiera także: a) decyzję o wyznaczeniu	Tak		Pismem z dnia 18 października 1999 r. został wyznaczony ABI ponadto został wymieniony w	

	Administratora Bezpieczeństwa Informacji? b) upoważnienia do przetwarzania danych? c) ewidencję osób upoważnionych do przetwarzania danych? d) zbiór oświadczeń osób zapoznanych z dokumentacją oraz zobowiązanie do stosowania jej wymogów? e) listę osób przeszkolonych z zasad przetwarzania danych osobowych? f) oświadczenia pracowników o zachowaniu w tajemnicy danych osobowych? g) umowy o powierzeniu przetwarzania danych?	Tak Tak Tak Tak	Nie	Zarządzeniu nr 338/09 z dnia 17 kwietnia 2009 r. Burmistrza Miasta i Gminy Czarne w sprawie w sprawie ochrony danych osobowych w U M i G w Czarnem został wyznaczony Administrator Bezpieczeństwa Informacji, nie został zgłoszony do GIODO. Sprawdzono upoważnienia wszystkich pracowników, są one przechowywane w segregatorach oznaczonych jako „OCHRONA DANYCH OSOBOWYCH", oraz są dołączone do akt osobowych zatrudnionych pracowników. Każdy z pracowników podpisuje oświadczenia o zapoznaniu się z przepisami dot. przetwarzania danych osobowych oraz o zachowaniu w tajemnicy wszelkich informacji dot. przetwarzania danych. W § 21 Polityki Bezpieczeństwa Ochrony Danych Osobowych wskazano formę powierzenia przetwarzania oraz określono obowiązki jakie musi spełnić podmiot.	W Urzędzie nie została sporządzona oddzielna lista osób zapoznanych z dokumentacją, każdy z pracowników zapoznanie się z dokumentacją poświadcza własnoręcznym podpisem na dokumentacji.
8.	Czy kierownictwo wspiera działania w zakresie bezpieczeństwa informacji w całej organizacji, w tym: a) w jaki sposób demonstrowane są cele, kierunki działania, zaangażowanie? (np. czy mówi się o tym na naradach, czy jest to temat powracający na który kierownictwo zwraca uwagę?) b) jakie działania służą utrzymaniu właściwej świadomości problematyki bezpieczeństwa w organizacji? (np. kontrole, szkolenia)	TAK Nie		Burmistrz pełniący funkcję ADO w trakcie prowadzonych narad z podległym kierownictwem zwraca uwagę na uświadamianie pracowników o odpowiedzialności związanej z przetwarzaniem danych osobowych. W miesiącu kwietniu 2018 r. ma zostać przeprowadzona wyrywkowa kontrola stanowisk pracy w zakresie ochrony danych osobowych. W miesiącu maju 2018 r. ma odbyć się szkolenie w związku z rozpoczęciem obowiązywania od dnia 25 maja 2018 roku RODO (GDPR), czyli nowego unijnego rozporządzenie dotyczące ochrony danych osobowych.	

Uchybienia:

1. Administrator Bezpieczeństwa Informacji nie został zgłoszony do GIODO, w aktach osobowych pracownika oraz w Zarządzeniu nr 338/09 Burmistrza Gminy Czarne z dnia 17 kwietnia 2009 r. jest zapis o wyznaczaniu pracownika na stanowisko ABI – w związku z niedopełnieniem obowiązku zgłoszenia ABI po dniu 30 czerwca 2015 r., w jednostce rolę Administratora Danych Osobowych pełni Burmistrz.

Rekomendacje:

Ustawa o ochronie danych osobowych nie określa obowiązku ani formy „powołania" ABI-ego. Art. 36a ustawy w ustępie 1 wskazuje jedynie, że: Administrator Danych Osobowych może powołać Administratora Bezpieczeństwa Informacji. Jeśli wolą Administratora Danych jest powołanie ABI-ego, to brak ograniczenia ustawowego umożliwia powołanie go na różnej podstawie w tym na podstawie jednostronnych oświadczeń woli Administratora Danych Osobowych lub w drodze umów. Przed wyjaśnieniem poszczególnych możliwości powołań wyjaśnić należy, że ABI musi bezpośrednio podlegać kierownikowi jednostki organizacyjnej lub Administratorowi Danych Osobowych. Jest to bardzo ważna kwestia, gdyż umożliwia ona niezależne oraz nieskrępowane funkcjonowanie w ramach struktury organizacji. Powołanie może zostać dokonane albo w formie postanowienia zawartego w umowie (o pracę, zlecenia) albo w formie oświadczenia woli (decyzja/zarządzenie kierownika jednostki - forma preferowana przez audytora). Audytor wewnętrzny wskazuje, że fakt powołania ABI-ego w jednostce udokumentowany był pisemnie, jednakże w związku z nowelą ustawy o ochronie danych osobowych z dnia 1 stycznia 2015 r. Administrator Bezpieczeństwa Informacji powołany przed dniem wejścia nowych przepisów, zgodnie z przepisami przejściowymi powinien zostać zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych do 30 czerwca 2015 r. Jeśli nie zostanie On zgłoszony i zarejestrowany, to po dniu 30 czerwca 2015 r. automatycznie przestanie pełnić swoją funkcję i jego zadania przejmuje administrator danych. Postępowanie takie ma to znaczenie, gdyż forma pisemna gwarantuje transparentność i nie pozostawia niejasności w kwestii obowiązków spoczywających na tak powołanym ABI oraz służy celom dowodowym. Należy także zaznaczyć, że kontrolerzy GIODO (w razie kontroli) również zażądają okazania dokumentu powołania i zgłoszenia ABI-ego.

Zatem w przypadku ponownego powołania Administratora Bezpieczeństwa Informacji przez Administrator Danych Osobowych fakt ten – ze względów dowodowych – powinien zostać udokumentowany na piśmie jak również w dokumentacji winien znaleźć się dowód

zgłoszenia i rejestracji ABI-ego przez GIODO. Dlatego audytor zaleca, by stosownym pisemnym zarządzeniem Burmistrza Miasta i Gminy Czarne w przypadku powołania Administratora Bezpieczeństwa Informacji; w zarządzeniu tym wskazany został zakres obowiązków ABI-ego. Należy również pamiętać o tym, że w razie powołania ABI-ego fakt ten trzeba w terminie 30 dni zgłosić do rejestracji GIODO a następnie zostanie on wpisany do ogólnokrajowego, jawnego rejestru ABI. W przypadku nie powołania stanowiska Administratora Bezpieczeństwa Informacji obowiązki te stają się obowiązkami Administratora Danych Osobowych. ADO wykonuje więc następujące obowiązki przypisane ABI: przeprowadzanie wewnętrznych kontroli, nadzór nad dokumentacją i szkolenia. Przepisy w tej kwestii nie przesądzają, jak ADO powinien wykonywać te obowiązki. Zatem ADO może zdecydować, że sam będzie realizował zadania, może również powierzyć to innej osobie, bez powoływania jej na ABI. Może także wyznaczyć cały zespół, odpowiedzialny za ochronę danych. Warto, by ADO pamiętał, że niezależnie od tego jaki model wybierze, to on odpowiada za realizację ustawowych zadań. Powierzenie obowiązków innym, nie zwalnia ADO z odpowiedzialności.

Uchybienia:

2. urząd nie realizuje regulacji dotyczącej procedury kontrolnej;

Rekomendacje:

Jednym z obowiązków Administratora Bezpieczeństwa Informacji - jeśli jest powołany - jest sprawowanie kontroli wewnętrznej nad ochroną przetwarzanych danych osobowych w jednostce. Wytyczne w tym zakresie określa rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez Administratora Bezpieczeństwa Informacji. Rozporządzenie to wyróżnia dwie formy sprawowania kontroli: sprawdzenie oraz *stricte* sprawowanie nadzoru. Sprawdzenie to weryfikacja zgodności przetwarzania danych osobowych z przepisami ustawy. Zdaniem audytora – w Polityce Bezpieczeństwa muszą pojawić się oraz być realizowane – odpowiadające wytycznym rozporządzenia – zasady przeprowadzania sprawdzeń, ich planowania oraz ich częstotliwość (nie częściej niż raz na kwartał, nie rzadziej niż raz na rok). Z kolei samo sprawowanie nadzoru przez Administratora Bezpieczeństwa Informacji obejmuje weryfikację aktualności dokumentacji ochrony danych osobowych, a także badanie zgodności ze stanem faktycznym przewidzianych w dokumentacji środków technicznych i organizacyjnych oraz ogólnych

zasad i obowiązków określonych w dokumentacji. Tryb przeprowadzania tych wszystkich działań kontrolnych powinien być nie tylko szczegółowo opisany w Polityce Bezpieczeństwa, wraz z podaniem częstotliwości przeprowadzania danych procedur, ale także – z taką właśnie częstotliwością realizowany. Z czynności kontrolnych należy sporządzać protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne, dołącza się go do dokumentacji ochrony danych osobowych. Wzór protokołu kontroli lub czynności sprawdzających powinien znaleźć się w Polityce Bezpieczeństwa. W badanej jednostce w związku z brakiem powołanego ABI-ego po dniu 30 czerwca 2015 r. winny być wykonywane przez Administratora Danych Osobowych.

Uchybienia:

3. w dokumentacji brak jest regulacji, dotyczących wymagań szkoleniowych pracowników.

Rekomendacje:

Zapoznać pracowników z przepisami można na dwa sposoby. Sposób pierwszy polega na przekazaniu im treści aktów prawnych oraz dokumentacji dotyczącej polityki bezpieczeństwa (sposób zastosowany przez jednostkę). Jest to działanie proste i bardzo tanie, jednak – zdaniem audytora – w praktyce zupełnie się nie sprawdza. Przepisy dotyczące ochrony danych osobowych są bowiem skomplikowane i trudne w interpretacji nawet dla pracowników działów prawnych. Należy pamiętać o tym, że tzw. „czynnik ludzki" jest przyczyną największej ilości incydentów, związanych z naruszeniem danych osobowych. Wysoka świadomość pracowników jest z kolei najskuteczniejszym sposobem zabezpieczenia informacji. Z powyższych względów audytor wewnętrzny zaleca bardziej kompleksowe podejście do szkolenia pracowników. W jednostce w chwili obecnej brak jest Administrator Bezpieczeństwa Informacji zatem obowiązek realizacji cyklicznych szkoleń pracowników spoczywa na Admiratorze Danych bądź osobie przez niego wskazanej. Jednostka może również skorzystać z usług trenera zewnętrznego, który cyklicznie będzie przeprowadzał szkolenia pracowników. W trakcie szkolenia należy skupić się na najważniejszych aspektach – po szkoleniu pracownicy powinni wiedzieć, do kogo mogą zgłosić się z problemami z zakresu ochrony danych osobowych, powinni znać też podstawowe definicje, być świadomi tego, że przetwarzają dane osobowe. Bardzo ważna jest również świadomość odpowiedzialności, która łączy się z faktem przetwarzania danych osobowych. W sytuacji,

kiedy jednostka wybierze optymalny dla siebie sposób prowadzenia szkoleń, powinien on zostać opisany w Polityce Bezpieczeństwa i być realizowany w praktyce.

Pomimo stwierdzonych powyżej uchybień, system kontroli zarządczej w badanym obszarze jest na poziomie akceptowalnym.

Tab. nr 2 Test - zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Sposób przeprowadzenia czynności audytowych:

- Analiza aktów wewnętrznych dot. bezpieczeństwa informacji.
- Uzyskiwanie wyjaśnień i informacji od osób odpowiedzialnych za prawidłowe funkcjonowanie systemu bezpieczeństwa informacji oraz od innych pracowników jednostki.
- Zapoznawanie się z innymi dokumentami służbowymi, na podstawie których można będzie dokonać ustalenia stanu faktycznego w badanym zakresie.

	TREŚĆ PYTANIA	*ODPOWIEDZI*		*DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"*	*UWAGI*
		TAK	NIE		
1.	Czy w regulacjach wewnętrznych są zapisy dotyczące przeprowadzania przeglądu dokumentacji bezpieczeństwa w jednostce?	Nie			Dokumentacja wdrożona w 2009 r., nie była aktualizowana.
2.	Czy w regularnych odstępach czasowych i przez kogo wykonywany jest przegląd dokumentacji bezpieczeństwa celem zapewnienia, że pozostaje ona przydatna, adekwatna i skuteczna?	Nie			Przeglądu powinien dokonywać ABI.
3.	Czy obowiązki w zakresie opracowania, przeglądu i oceny dokumentacji bezpieczeństwa przypisane są określonym osobom? W jakich dokumentach?	Tak		Obowiązki opracowania polityki bezpieczeństwa, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych spoczywają na ABI.	

4.	Czy w latach 2015 - 2017 r aktualizowano dokumentację bezpieczeństwa? (podać datę ostatniej aktualizacji)	Nie		Urząd zamierza w tym roku opracować nową kompleksową dokumentację w zakresie polityki bezpieczeństwa.	Burmistrz Zarządzeniem nr 0050.170.2013 z dnia 31 grudnia 2013 r. wprowadził zmiany do załącznika B – wykazu zbiorów danych.
5.	Czy zmiany w dokumentacji bezpieczeństwa informacji zostały zatwierdzone przez kierownictwo jednostki?	Nie dotyczy			

Uchybienia:

1. w dokumentacji jednostki brak jest zapisów dotyczących przeprowadzania przeglądu dokumentacji w zakresie bezpieczeństwa informacji;

Rekomendacje:

Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych jest aktem wykonawczym do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Wprowadza ono liczne wymagania, między innymi obligując odpowiednie jednostki administracji publicznej do realizowania corocznych, wewnętrznych audytów bezpieczeństwa swojej infrastruktury IT, czy uczestniczenia w szkoleniach z obszaru bezpieczeństwa. Minimalne wymagania dotyczące bezpieczeństwa zapisane są w § 20 tego rozporządzenia, którego ust. 1 stanowi, że 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, rozliczalność, niezaprzeczalność i niezawodność. Dalej w rozporządzeniu określono, w jaki sposób należy organizować zarządzanie bezpieczeństwem informacji. W § 20 ust. 2 wskazano, że zarządzanie bezpieczeństwem informacji realizowane jest m.in. przez zapewnienie przez kierownictwo podmiotu publicznego aktualizacji regulacji

wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. Zdaniem audytora, najczęściej nie udaje się jednorazowe poprawne wdrożenie mechanizmów bezpieczeństwa – tj. jednokrotne przygotowanie odpowiednich procedur (tak jak zrobiła to audytowana jednostka), zabezpieczenie systemów, wprowadzenie odpowiednich mechanizmów monitoringu bezpieczeństwa itd. Zazwyczaj bezpieczeństwo zmienia się w czasie – zmieniają się technologie, wdrażamy nowe systemy, powstają nowe zagrożenia, może się również okazać, że przygotowane przez nas procedury po jakimś czasie nie są do końca skuteczne, optymalnie itd. Dlatego zaleca się okresowe przeglądy dokumentacji w zakresie bezpieczeństwa informacji i dostosowania jej do wewnętrznych procedur działania, do bieżącej sytuacji. Po dokonaniu takiego przeglądu należy sporządzić stosowny protokół z tej czynności i dołączyć go do dokumentacji jednostki w zakresie Polityki Bezpieczeństwa.

Biorąc pod uwagę uzyskane wyjaśnienia i informacje od Administratora Danych Osobowych, faktycznego przeglądu dokonuje On osobiście oraz zapewnienia, że jednostka zamierza w tym roku wprowadzić nową kompleksową dokumentację w zakresie bezpieczeństwa informacji, audytor wewnętrzny stwierdza, że system kontroli zarządczej w badanym obszarze jest na poziomie akceptowalnym.

Podsumowując: Audytor wewnętrzny, realizując zadanie zapewniające, stwierdził kilka uchybień. Były to m.in.: brak realizacji regulacji dotyczących procedury kontrolnej, brak decyzji/zarządzenia o powołaniu i zgłoszenia ABI-ego w związku z wygaśnięciem dotychczasowego powołania w związku nowelą ustawy o ochronie danych osobowych i przepisami przejściowymi, brak w dokumentacji regulacji, dotyczących wymagań szkoleniowych pracowników brak w dokumentacji jednostki zapisów dotyczących przeprowadzania przeglądu dokumentacji w zakresie bezpieczeństwa informacji. Audytor wskazuje ponadto na potrzebę przygotowania zapisów, dotyczących przeprowadzania przeglądu dokumentacji w zakresie bezpieczeństwa informacji oraz w zakresie potrzeb szkoleniowych dla pracowników. W tym zakresie wydano również stosowne rekomendacje, zalecając wdrożenie procedur kontrolnych w zakresie bezpieczeństwa informacji, ponowne pisemne powołanie ABI-ego i jego zgłoszenia do GIODO jeśli Administrator Danych Osobowych zechce powołać Administratora Danych Osbobwych oraz dokonywanie okresowych przeglądów dokumentacji, a także wdrożenie nowej kompleksowej/dostosowanej do obowiązujących przepisów prawa dokumentacji w zakresie polityki bezpieczeństwa. Powyższe uchybienia nie mają jednak wpływu na końcową pozytywną ocenę badanego

obszaru. Stwierdza się, że system kontroli zarządczej w jednostce funkcjonuje na poziomie akceptowalnym. Nie zauważono podwyższonego ryzyka mogącego stanowić zagrożenie dla realizacji celów stawianych przed systemem bezpieczeństwa informacji. Wdrożona przez jednostkę dokumentacja w zakresie bezpieczeństwa informacji nie jest wprawdzie kompleksowa i aktualna, ale spełnia minimalne wymogi wynikające z przepisów prawa. A – co ważne – jednostka zamierza w tym roku wdrożyć nową kompleksową dokumentację w zakresie polityki bezpieczeństwa.

Zgodnie z § 17 ust. 1 rozporządzenia Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu[5] audytor wewnętrzny po przeprowadzeniu czynności audytowych omawia z audytowanym wstępne wyniki audytu, w tym w szczególności ustalenia i propozycje zaleceń. Realizując dyspozycję tego przepisu audytor wewnętrzny w dniu 23.04.2018 r. przekazał audytowanemu drogą elektroniczną projekt sprawozdania, zawierający ustalenia oraz propozycje zaleceń. W tym samym dniu audytowany zaakceptował to sprawozdanie.

Z kolei § 19 ust. 1 tego rozporządzenia mówi, że kierownik komórki audytu wewnętrznego przekazuje sprawozdanie audytowanemu i kierownikowi jednostki; w przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko kierownikowi jednostki i audytorowi wewnętrznemu (ust. 3).

Sprawozdanie to sporządzono w dwóch jednobrzmiących egzemplarzach, które otrzymują:

1. Burmistrz Miasta i Gminy w Czarnem,
2. a/a

Audytor wewnętrzny
M. Żuczek
.....Marek Żuczek.....
(podpis audytora)

[5] Rozporządzenie Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu, Dz. U. z 2015 r. poz. 1480 ze zm.