

Raport i opinia z przeprowadzenia zadania audytowego nr B AW 3/12/2021

Audyt bezpieczeństwa informacji

1.1. Zadanie audytowe nr B AW 3/12/2021

1.2. Temat audytu:

Audyt bezpieczeństwa informacji w Urzędzie Miasta Bartoszyce w 2021 r

1.3. Cel i zakres audytu:

Celem kontroli była ocena systemu bezpieczeństwa informacji i ochrony danych w Urzędzie Miasta Bartoszyce w 2021 r., w szczególności:

- spełnienie standardów związanych z bezpieczeństwem informacji, stosownie do wymogów rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz normy PN-EN ISO/IEC 270001:2017 Systemy zarządzania bezpieczeństwem informacji ,
- spełnienie standardów związanych z ochroną danych osobowych, w tym zasad ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO), technicznych sposobów zapewnienia bezpieczeństwa informacji, w tym m.in. politykę haseł, procedur zarządzania w przypadku naruszenia ochrony danych osobowych, zabezpieczenia zasobów lokalnych, fizycznego bezpieczeństwa danych, wewnętrznego bezpieczeństwa danych,
- realizacja i nadzór nad przestrzeganiem standardów systemu bezpieczeństwa informacji oraz przepisów o ochronie danych osobowych,

Zakres niniejszej kontroli został ustalony w Planie audytu na 2021 r.

Audyt obejmuje ocenę działań Urzędu w zakresie opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Cel i zakres zadania audytowego został określony na podstawie przeprowadzonej analizy ryzyka.

1.4. Opinia audytora

Audyt pozytywnie ocenia funkcjonujący w Urzędzie Miasta Bartoszyce system bezpieczeństwa informacji i ochrony danych. Ustalono, że wdrożona w Urzędzie Polityka Bezpieczeństwa przetwarzania danych osobowych, Instrukcja zarządzania systemem informatycznym oraz pozostałe zasady i instrukcje określone Zarządzeniem nr 103/2019 Burmistrza Miasta Bartoszyce z 30 maja 2019 r. spełniały wymagania określone pkt 78 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Przewidziane w Polityce środki polegały m.in. na przestrzeganiu zasad przetwarzania danych osobowych umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń. Ponadto, oprogramowanie i urządzenia służące do przetwarzania danych osobowych spełniały wymagania przewidziane w przepisach prawa, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz Polityki Bezpieczeństwa, Instrukcja zarządzania systemem informatycznym wdrożonych Zarządzeniem nr 103/2019 Burmistrza Miasta Bartoszyce z 30 maja 2019 r. Audyt wykazał, że w systemach informatycznych wykorzystywanych w Urzędzie zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł, a dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony był za pomocą uwierzytelniania z wykorzystaniem hasła natomiast komputery z dostępem do obsługi Systemu Rejestrów Państwowych zabezpieczone są z pomocą dwuskładnikowego uwierzytelniania z wykorzystaniem hasła oraz karty procesorowej oraz kodu PIN. Audyt wykazał, że w Urzędzie prawidłowo i rzetelnie prowadzonych jest rejestr czynności przetwarzania danych w urzędzie oraz rejestr umów powierzenia danych, także rejestru naruszeń przetwarzania danych osobowych.

Zgodnie z obowiązującymi wymogami prawa zarządzeniem nr 71/2019 z 8 kwietnia 2019 r. Burmistrz powierzył pracownikowi Urzędu - Darii Butkiewicz - funkcję Inspektora Danych Osobowych w Urzędzie Miasta Bartoszyce i w Straży Miejskiej, a także zapewnił przeprowadzenie oceny przetwarzaniu danych osobowych dla wszystkich chronionych zasobów oraz możliwych zagrożeń.

Ustalono również, że w Urzędzie przeprowadza się inwentaryzację sprzętu komputerowego, która odbywa się poprzez coroczny przegląd stanowisk komputerowych. Zapewniono również, aby oprogramowanie służące przetwarzaniu informacji było legalne oraz posiadało środki ochrony przez zastosowanie np. firewall, m.in. licencje na systemy dziedzinowe wykupywane są na dany rok kalendarzowy.

W Urzędzie przeprowadzono również 18 listopada 2021 r. szkolenie pracowników urzędu w zakresie zagrożenia bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji, stosownie do wymagań § 20 ust 2 pkt 6 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności.

1.5. Podmiot przeprowadzający audyt wewnętrzny

Sebastian Bentkowski – audytor wewnętrzny z firmy DB Group s.c. w Olsztynie, ul. Popiełuszki 7/8, 10-695 Olsztyn, NIP 739-37-37-042,

przy udziale pracownika Urzędu Miasta Bartoszyce Darii Butkiewicz

1.6. Nazwa i adres audytowanej jednostki:

Urząd Miasta Bartoszyce, ul. Bohaterów Monte Cassino 1 11-200 Bartoszyce

Termin przeprowadzenia badania: od 01.12.2021 r. 27.12.2021 r.

1.7. Okres objęty badaniem: 01.01.2021 r. do 31.12.2021 r.

1.8. Podstawy prawne kontrolowanej działalności:

- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 2020 r., poz. 346 ze zm.), zwana dalej „ustawą o informatyzacji”,
- 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 - Dz.U.U.E.L.2016.119), zwane dalej „Rozporządzenie RODO”,
- 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 2012 r., poz. 526), zwane dalej „rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności”
- Zarządzenie nr 103/2019 Burmistrza Miasta Bartoszyce z 30 maja 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa przetwarzania danych osobowych, Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta Bartoszyce, Zasady zabezpieczenia pomieszczeń Urzędu Miasta Bartoszyce, Instrukcje postępowania w sytuacji naruszenia ochrony danych osobowych oraz Instrukcję oceny skutków przetwarzania dla ochrony danych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (...), wydane na podstawie 18 ustawy o informatyzacji, stanowi w § 18 m.in., że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

- zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;



- podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
- zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
- zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
- zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
- ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
- zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,

2. Formalno-prawne aspekty systemu bezpieczeństwa informacji w Urzędzie Miasta Bartoszyce

2.1. Zarządzeniem nr 103/2019 Burmistrza Miasta Bartoszyce z 30 maja 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa przetwarzania danych osobowych, Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta Bartoszyce, Zasady zabezpieczenia pomieszczeń Urzędu Miasta Bartoszyce, Instrukcje postępowania w sytuacji naruszenia ochrony danych osobowych oraz Instrukcję oceny skutków przetwarzania dla ochrony danych, określono standardy polityki ochrony danych osobowych w Urzędzie Miasta Bartoszyce. Zarządzenie zostało wydane na podstawie art.24 ust.1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - Dz.U.U.E.L.2016.119)



2.1.1 Polityka bezpieczeństwa informacji

W Polityce Bezpieczeństwa przetwarzania danych osobowych oraz pozostałych instrukcjach i regulaminach przyjętych ww. zarządzeniem Nr 103/2019 r. zawarto informacje dotyczące m.in. :

- zasad i sposobu przeprowadzenia analizy ryzyka w zakresie ochrony danych, opis sposobu przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych oraz plan postępowania z ryzykiem, w tym zobowiązanie Administratora do monitorowania zagrożeń
- zasad postępowania w zakresie udzielania upoważnień do przetwarzania danych osobowych,
- Procedury postępowania z incydentami zawierającą zbiór typowych naruszeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opis sposobu reagowania na nie w celu minimalizacji skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości
- zapewnienia wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania,
- zasad przeprowadzania szkoleń z zakresu ochrony danych osobowych
- prowadzenia rejestru czynności przetwarzania przez Administratora,

W zarządzeniu nr 103/2019 określono także m.in. role osób w systemie przetwarzania danych osobowych, zasady przetwarzania, rolę zgody, zasady wypełniania obowiązku informacyjnego, wypełniania praw podmiotów danych, niszczenia dokumentacji, zasad korzystania ze sprzętu.

Dokumentacja zawierała również:

- opis zabezpieczeń fizycznych i sprzętowych
- procedury nadawania uprawnień do przetwarzania danych osobowych
- stosowane metody i środki uwierzytelniania,
- zasady zarządzania oprogramowaniem,
- zasady likwidacji i serwisu sprzętu komputerowego,
- zasady zabezpieczenia systemu informatycznego, stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

W ocenie audytora wdrożona Polityka Bezpieczeństwa przetwarzania danych osobowych, Instrukcja zarządzania systemem informatycznym w Urzędzie Miasta Bartoszyce, Zasady zabezpieczenia pomieszczeń Urzędu Miasta Bartoszyce, Instrukcje postępowania w sytuacji naruszenia ochrony danych osobowych oraz Instrukcje oceny skutków przetwarzania dla ochrony

danych spełniały wymagania określone pkt 78 rozporządzenia o ochronie danych, tj. zawierały postanowienia zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Przewidziane w Polityce środki polegały m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń.

Stwierdzono również, że opracowane w Urzędzie standardy systemu uwzględniają postanowienia norm PN-ISO/IEC 27001, PN-ISO/IEC 27005.

2. Wykaz systemów informatycznych służących do przetwarzania danych osobowych

W wyniku czynności audytowych ustalono, że badanym okresie w Urzędzie funkcjonowały systemy informatyczne w ramach których przetwarzano dane osobowe, tj. m.in.

- a. System Elektronicznego Obiegu Dokumentów EDICTA do obsługi scentralizowanego przetwarzania zadań i procesów obiegu dokumentacji w Urzędzie Miasta Bartoszyce.
- b. System PUMA Księgowość i Finanse autorstwa firmy ZETO SOFTWARE Sp. z o.o. wspomagający realizację zadań finansowo - księgowych urzędu.
- c. System informatyczny Besti@ - system do zarządzania budżetem Urzędu Miasta Bartoszyce. Program umożliwia sporządzenie budżetu, zmian budżetu, sprawozdań budżetowych oraz wysłanie sprawozdań do Regionalnej Izby Obrachunkowej z siedzibą w Olsztynie.
- d. System Cmentarz I, II, służący administrowaniu miejscami cmentarnymi
- e. Aplikacja AZP umożliwiająca bieżące administrowanie dokumentacją dotyczącą Umowy Ubezpieczenia (grupowe ubezpieczenie na życie) zawartą z TUnŻ "WARTA" S.A.
- f. System Podatki i Opłaty Lokalne PUMA autorstwa firmy ZETO SOFTWARE Sp. z o.o. służący do identyfikowania, pobierania i ewidencjonowania podatków i opłat wnoszonych do urzędu.
- g. System Kadrowo - Płacowy System PUMA autorstwa firmy ZETO SOFTWARE Sp. z o.o. służący do obsługi kadr i płac w urzędzie.
- h. System Płatnik tworzony przez Asseco Poland S.A. wspomagający dział kadr i płac w zakresie elektronicznej wysyłki dokumentów ubezpieczeniowych do Zakładu Ubezpieczeń Społecznych (ZUS)
- i. System PUMA autorstwa firmy ZETO SOFTWARE Sp. z o.o. obsługujący bazę ewidencji ludności (rejestr mieszkańców).
- j. System PUMA moduł Nieruchomości służący rejestracji transakcji sprzedaży, najmu, dzierżawy nieruchomości
- k. Urząd Gminy posiada zdalny dostęp w ramach projektu pl.ID dostęp do Systemu Rejestrów Państwowych (SRP) realizowany za pośrednictwem dedykowanego łącza



tunelowanego, a dostęp do danych jest realizowany za pośrednictwem certyfikatów wydawanych przez Ministerstwo Spraw Wewnętrznych.

- l. W Systemie Rejestrów Państwowych (SRP) prowadzone są rejestry publiczne: Rejestr PESEL, Rejestr Dowodów Osobistych, Rejestr Stanu Cywilnego, Rejestr Danych Kontaktowych
- m. System operacyjny MS Windows.

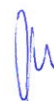
Oprogramowanie służące do przetwarzania danych osobowych spełnia wymagania przewidziane w przepisach prawa, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz wdrożonej w Urzędzie zarządzeniem nr 103/2019 Burmistrza Miasta Bartoszyce z 30 maja 2019 r. Polityki Bezpieczeństwa przetwarzania danych osobowych, Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta Bartoszyce. Ustalono m.in., że w w/w systemach informatycznych wykorzystywanych w Urzędzie zastosowano:

- systemowe mechanizmy wymuszające okresową zmianę haseł natomiast komputery z dostępem do obsługi Systemu Rejestrów Państwowych zabezpieczone są z pomocą dwuskładnikowego uwierzytelniania z wykorzystaniem hasła oraz karty procesorowej oraz kodu PIN.;
- środki umożliwiające określenia praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
- standardy dot. haseł, tj.:
 - hasło składa się, z co najmniej ośmiu znaków;
 - hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały, itp.) i nie może być sekwencją kolejnych znaków klawiatury.
- wymienione powyżej systemy (z wyjątkiem SRP, którego bazy danych znajdują się w MSW oraz MS Windows) pracują w oparciu o programy bazodanowe
- Bazy danych są zlokalizowane na serwerze bazodanowym, który stoi w wydzielonym pomieszczeniu, tzw. serwerowni.
- W celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych i urządzeń znajdujących się serwerowni, dostęp do niej mają tylko osoby uprawnione.

Ustalono również, że serwerownia jest wyposażona w urządzenie zabezpieczające przed zanikiem i gwałtownymi skokami napięcia w sieci energetycznej (UPS)-

Dostęp do baz danych znajdujących się na serwerze bazodanowym w serwerowni jest możliwy poprzez:

- Systemy informatyczne przetwarzające dane osobowe posiadające swoją bazę danych. Każdy użytkownik wymienionych powyżej programów posiada unikatowy login i hasło, które go



jednoznacznie identyfikują w danym programie. Hasła dostępu do programów podlegają cyklicznym zmianom (zmiana hasła musi być przeprowadzana co najmniej raz na rok).


- programy zainstalowane na serwerze bazodanowym wyposażone są w narzędzia służące do wykonywania kopii zapasowych a także zarządzania bazą danych. Dostęp do tego oprogramowania ma tylko administrator.

W celu podniesienia bezpieczeństwa danych i zapobieżenia ewentualnej ich utracie regularnie wykonywana jest zapasowa kopia użytkowanych baz danych. Backup baz danych odbywa się za pomocą narzędzi dostępnych w oprogramowaniu bazodanowym oraz dedykowanym oprogramowaniu. Kopie baz danych są zapisywane na dyskach serwerowych oraz cyklicznie na zewnętrznych dyskach:

W świetle powyższych ustaleń audytor stwierdza, że zapewniono bezpieczeństwo informacji w systemach informatycznych, stosownie do wymagań określonych w § 20 ust 2 pkt 9 i 12 rozporządzenia w sprawie Krajowych Ram Interoperacyjności.

2.1. W Urzędzie spełniono standardy zabezpieczenia danych poprzez wdrożenie środków ochrony, takich jak:

- 1.—Środki fizyczne,** tj. m.in. Urząd Miasta Bartoszyce, ul. Bohaterów Monte Cassino 1 11-200 Bartoszyce posiada wejścia wyposażone w drzwi z zamkami patentowymi, wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej, urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach biurowych – ograniczono dostęp osób nieupoważnionych. Wszystkie pomieszczenia biurowe, w których przetwarza się dane osobowe chronione są poprzez zastosowanie drzwi drewnianych z zamkami mechanicznymi, zamontowano system alarmowy oraz okratowano okna na pierwszej kondygnacji.
- 2.—Zabezpieczenia sprzętowe:** do likwidacji zbędnych dokumentów papierowych zawierających dane osobowe zastosowano niszczarki o podwyższonej klasie niszczenia, systemy informatyczne przetwarzające dane osobowe są zainstalowane na komputerach przyłączonych do sieci LAN oraz na samodzielnych stanowiskach niepodłączonych do LAN, dostęp do komputerów przetwarzających dane osobowe jest chroniony poprzez hasła na systemie operacyjnym i hasła aplikacji, lokalna sieć komputerowa ma połączenie z siecią publiczną Internet w sposób zapewniający kontrolę przepływu danych pomiędzy LAN a Internetem, dane są filtrowane za pomocą właściwych urządzeń, wybrane komputery na których przetwarzane są dane osobowe są zabezpieczone przed utratą danych na skutek zaniku napięcia: UPS podtrzymuje pracę urządzeń w przypadku zaniku zasilania, laptopy posiadają własną baterię wewnętrzną.
- 3.—Środki ochrony w ramach oprogramowani systemu:** Konfiguracja systemu umożliwia użytkownikom dostęp do danych osobowych tylko za pośrednictwem aplikacji; zabronione jest instalowanie narzędzi programowych umożliwiających dostęp do baz danych z pominięciem aplikacji, systemy operacyjne komputerów mają zdefiniowane prawa dostępu do zasobów systemu dla poszczególnych użytkowników oraz system ich autoryzacji poprzez



identyfikatory i hasła, dostęp do systemów sieciowych jest chroniony poprzez system identyfikatorów i haseł użytkowników, zainstalowany program antywirusowy posiada funkcje skanera zasobów dyskowych, monitora systemu, skanera poczty elektronicznej oraz funkcje, która umożliwia wykrywanie i blokowanie niepożądanych procesów w systemie, systemy operacyjne są aktualizowane poprzez instalowanie Serwis Pack'ów i update'ów systemu

Audytora stwierdza, że zastosowane środki bezpieczeństwa informacji spełniają wymagania określone w § 20 ust 2 pkt 7, 9 i 12 rozporządzenia w sprawie Krajowych Ram Interoperacyjności.

4.—Obowiązki Administratora/Inspektora Danych Osobowych

Burmistrz Miasta Bartoszyce zarządzeniem nr 71/2019 z 8 kwietnia 2019 r. powierzył pracownikowi Urzędu - Darii Butkiewicz - funkcję Inspektora Danych Osobowych w Urzędzie Miasta Bartoszyce. Do zadań Inspektora należy informowanie i doradzanie Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz monitorowanie ich przestrzegania oraz działanie jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Powyższym zarządzeniem Burmistrz Miasta powierzył Karolowi Puszkiewiczowi funkcję administratora Systemu Informatycznego w Urzędzie Miasta Bartoszyce. Do zadań Administratora Systemu Informatycznego należy w szczególności:

- współpraca z Inspektorem Ochrony danych w zakresie zapewnienia bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.
- formułowanie w uzgodnieniu z administratorem danych i/lub osobami, do których administrator delegował zarządzenie uprawnieniami oraz Inspektorem Ochrony danych sposobu określenia uprawnień w systemach informatycznych.
- realizacja decyzji administratora danych osobowych (osób upoważnionych) odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania w środowisku IT.

Burmistrz wywiązał się również z obowiązku zamieszczenia na stronie internetowej Urzędu informacji na temat systemu przetwarzania danych osobowych, w tym m.in. zamieszczono klauzulę informacyjną dla klientów Urzędu

Audyt wykazał, że w Urzędzie prawidłowo i rzetelnie prowadzonych jest rejestr czynności przetwarzania danych w urzędzie oraz rejestr umów powierzenia danych

W Urzędzie przeprowadzono również 18 listopada 2021 r. szkolenie pracowników urzędu w zakresie zagrożenia bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji, stosownie do wymagań § 20 ust 2 pkt 6 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności

Audyt stwierdza, że spełniono standard określony w § 20 ust 2 pkt 3 i 6 rozporządzenia w sprawie Krajowych Ram Interoperacyjności.

5.—Inwentaryzacja sprzętu i oprogramowania

Zgodnie z obowiązkami wynikającymi z § 20 ust 2 pkt 2 rozporządzenia w sprawie Krajowych Ram Interoperacyjności zapewniono przeprowadzenie inwentaryzacji sprzętu komputerowego, służącego przetwarzaniu informacji. W ramach corocznie wykonywanego przeglądu stanowisk komputerowych uaktualniano zmiany powstałe na poszczególnych stanowiskach komputerowych (np. wymiana sprzętu).

6.—Pozostałe ustalenia

Audyt wykazał, że Urząd wywiązał się z obowiązku:

- a. Prowadzenia rejestru czynności przetwarzania danych osobowych – rejestr zawierał rzetelne i aktualne informacje nt czynności i celu przetwarzania, kategorii osób których dane dotyczą oraz kategorii danych osobowych, planowany termin usunięcia poszczególnych danych, a także opis technicznych i organizacyjnych środków bezpieczeństwa.
- b. Prowadzenia rejestru naruszeń przetwarzania danych osobowych, ze wskazaniem rodzaj naruszenia, okoliczność naruszenia, skutki naruszenia oraz podjęte działania zaradcze.
- c. Prowadzenia rejestru umów powierzenia przetwarzania danych osobowych, ze wskazaniem daty umowy, podmiotu przetwarzającego dane i kategorii osób których dane dotyczą.
- d. Urząd wywiązała się również z obowiązku zamieszczenia na stronie internetowej Urzędu informacji na temat systemu przetwarzania danych osobowych, w tym m.in. zamieszczono klauzulę informacyjną.

UWAGI, REKOMENDACJE, ZALECENIA:

Wobec braku stwierdzenia nieprawidłowości odstąpiono od formułowania zaleceń pokontrolnych

Pouczenie

Audytowany może zgłosić audytorowi na piśmie, w terminie 7 dni wnieść pisemne zastrzeżenia dotyczące wstępnych wyników audytu wewnętrznego.

W przypadku nieuwzględnienia zgłoszonych zastrzeżeń uzasadnienie i opinia audytora zostanie umieszczona w ostatecznej wersji sprawozdania jako „stanowisko audytora wewnętrznego”.

Audytowany, w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania, ustala sposób i termin realizacji zaleceń oraz wyznacza osoby odpowiedzialne za realizację zaleceń, powiadamiając o tym na piśmie audytora i Burmistrza.



W przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko kierownikowi jednostki i audytorowi wewnętrznemu.

Podpis audytora wewnętrznego

PRZES DB Group s.c.

Sebastian Bentkowski

Podpis kierownika jednostki

BURMISTRZ

Piotr Petrykowski