DB GROUP S.C.
· AUDYT · PRZETARGI · SZKOLENIA ·

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

AN.1720.4.2023

Raport i opinia z przeprowadzenia zadania audytowego nr 3/2023

Audyt bezpieczeństwa informacji

1.1. Zadanie audytowe nr 03/2023

1.2. Temat audytu:

Audyt bezpieczeństwa informacji w Starostwie Powiatowym w Nidzicy, w tym ochrony danych osobowych w 2023 r.

1.3. Cel i zakres audytu:

Celem kontroli była ocena systemu bezpieczeństwa informacji i ochrony danych w Starostwie Powiatowym w Nidzicy w 2023 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 niniejszego audytu został ustalony w Planie audytu na 2023 r.

Audyt obejmuje ocenę działań Starostwa 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

Audytor **pozytywnie ocenia** funkcjonujący w Starostwie Powiatowym w Nidzicy system bezpieczeństwa informacji i ochrony danych. Stwierdzono bowiem, że zgodnie z wymaganiami § 20

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

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, wdrożono i zapewniono prawidłowe działanie systemu zarządzania bezpieczeństwem informacji, tj. system zapewniał poufność, dostępność i integralność informacji, przy spełnieniu atrybutów autentyczności, rozliczalności, niezaprzeczalności i niezawodności.

Ustalono, że wdrożona w Starostwie polityka ochrony danych osobowych spełniała 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 Ochrony Danych wdrożonej w Starostwie zarządzeniem Nr Z/21/2019 Starosty Powiatu Nidzickiego z dnia 30 sierpnia 2019 r. Audyt wykazał, że w systemach informatycznych wykorzystywanych w Starostwie 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. Zgodnie z obowiązującymi wymogami prawa Starostwa powierzył w dniu 2 września 2019 r. pracownikowi Starostwa umową o pracę z dnia 2 września 2019 r. na 0,5 etatu Jarosławowi Komoszyńskiemu funkcję Inspektora Danych Osobowych w Starostwie Powiatowym w Nidzicy, a także zapewnił przeprowadzenie oceny przetwarzaniu danych osobowych dla wszystkich chronionych zasobów oraz możliwych zagrożeń.

Ustalono również, że w Starostwie 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. Starostwo wywiązał się z obowiązku prowadzenia rzetelnego i zaktualizowanego rejestru czynności przetwarzania danych osobowych, prowadzenia rejestru umów powierzenia przetwarzania danych osobowych, ze wskazaniem daty umowy, podmiotu przetwarzającego dane i kategorii osób których dane dotyczą, a także rejestru naruszeń przetwarzania danych osobowych. Przeprowadzono również analizę ryzyka.

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

W Starostwie przeprowadzono wg oświadczenia inspektora ochrony danych szkolenie w 2023 r. dla osób zaangażowanych w proces przetwarzania informacji w Starostwa z zakresu ochrony danych, stosownie do wymagań § 20 ust 2 pkt 6 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności.
Przeprowadzono w 2023 r. dla wybranych pracowników Starostwa szkolenia w zakresie zagrożenia bezpieczeństwa informacji w systemach informatycznych, skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich.
Zrealizowano tym samym rekomendację z poprzedniego audytu systemu bezpieczeństwa informacji (za 2022 r.)

Ponadto, w Starostwie podjęto działania w celu powołania w 2024 r. Inspektora Bezpieczeństwa Teleinformatycznego, stosownie do wymagań 52 ust. 1 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (tekst jedn.: Dz. U z 2019 r. poz. 742) oraz § 14 Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (tekst jedn.: Dz. U. z 2011 r. nr 159 poz. 948). W tym celu m.in. Starostwo Powiatowe w Nidzicy jest w trakcie uzgodnień z Państwowym Instytutem Badawczym NASK w celu pozyskania laptopa i telefonu do przetwarzania informacji niejawnych o klauzuli „zastrzeżone".

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

1.6. Nazwa i adres audytowanej jednostki:

Starostwo Powiatowe w Nidzicy, ul. Traugutta 23, 13-100 Nidzica

1.7. Termin przeprowadzenia badania: od 27.12.2023 r. 29.12.2023 r.

1.8. Okres objęty badaniem: 01.01.2023 r. do 29.12.2023 r.

1.9. 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.UE.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.

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

z 2012 r., poz. 526), zwane dalej *„rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności"*

- Zarządzenie Nr Z/21/2019Starosty Powiatu Nidzickiego z dnia 30 sierpnia 2021 r. w sprawie wprowadzenia polityki ochrony danych osobowych w Starostwie Powiatowym w Nidzicy

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,

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

2. Formalno-prawne aspekty systemu bezpieczeństwa informacji w Starostwie Powiatowym w Nidzicy

Zarządzenie Nr Z/21/2019 Starosty Powiatu Nidzickiego z dnia 30 sierpnia 2021 r. w sprawie wprowadzenia polityki ochrony danych osobowych w Starostwie Powiatowym w Nidzicy wprowadzono politykę ochrony danych osobowych w Starostwa Powiatowego w Nidzicy. Zarządzenie zostało wydane na podstawie art.24ust.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.UE.L.2016.119)

2.1.1Polityka bezpieczeństwa informacji

- W Polityce ochrony danych osobowych przyjętej ww. zarządzeniem 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 Polityce 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

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

- 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 Ochrony Danych Osobowych spełniała 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 Starostwie standardy systemu uwzględniają postanowienia norm PN-ISO/IEC 27001, PN-ISO/IEC 27005,

2.1. 2 Przeprowadzenie analizy ryzyka

Stosownie do wymagań § 20 ust 2 pkt 3 rozporządzenia w sprawie Krajowych Ram Interoperacyjności w Starostwie przeprowadzano okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Audyt wykazał, że w Starostwie zarchiwizowano rzetelną dokumentację potwierdzającą przeprowadzenie okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji (raport z szacowania ryzyka utraty bezpieczeństwa informacji), tj. m.in. tabelę szacowania ryzyka, przykłady podatności, przykłady zagrożeń (nadużycie uprawnień, kradzież nośników, nieautoryzowane użycie urządzeń) oraz tryb postępowania.

Audytor nie wnosi zastrzeżeń do prawidłowości i rzetelności przeprowadzonej analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz metod minimalizujących to ryzyko.

3. Wykaz systemów informatycznych służących do przetwarzania danych osobowych

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

a. System Response Księgowość i Finanse autorstwa firmy ZETO SOFTWARE Sp. z o.o. wspomagający realizację zadań finansowo - księgowych Starostwa i Powiatu.

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

b. System informatyczny Besti@ - system do zarządzania budżetem Starostwa. Program umożliwia sporządzenie budżetu, zmian budżetu, sprawozdań budżetowych oraz wysłanie sprawozdań do Regionalnej Izby Obrachunkowej z siedzibą w Olsztynie.
c. System Response Księgowość i Finanse autorstwa firmy ZETO SOFTWARE Sp. z o.o. służący do obsługi kadr i płac w Starostwie.
d. System Pojazd i Kierowca w Wydziale Komunikacji do rejestracji pojazdów.
e. System Płatnik tworzony przez Asseco Poland S.A. wspomagający dział kadr i płac w zakresie elektronicznej wysyłki dokumentów ubezpieczeniowych do Zakładu Ubezpieczeń Społecznych (ZUS).
f. System EWOPIS autorstwa firmy GEOBID sp. z o. o.
g. System Strateg
h. System operacyjny MS Windows.

Oprogramowanie 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 wdrożonej w Starostwie zarządzeniem Nr Z/21/2019 Starosty Powiatu Nidzickiego z dnia 30 sierpnia 2019 r. w sprawie wprowadzenia polityki ochrony danych osobowych w Starostwie Powiatowym w Nidzicy. Ustalono m.in., że w w/w systemach informatycznych wykorzystywanych w Starostwie 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.

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

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.

3.1. W Starostwie spełniono standardy zabezpieczenia danych poprzez wdrożenie środków ochrony, takich jak:

1. **Środki fizyczne,** tj. m.in. Budynek Starostwa przy ul. ul. Traugutta 23, 13-100 Nidzica 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 za wyjątkiem 4 kopiarek oraz 2 niszczarek, 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

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

Zrealizowano tym samym rekomendację z poprzedniego audytu systemu bezpieczeństwa informacji (za 2022 r.)

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

Audyt wykazał, że w Starostwie podjęto działania w celu powołania w 2024 r. Inspektora Bezpieczeństwa Teleinformatycznego, stosownie do wymagań 52 ust. 1 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (tekst jedn.: Dz. U z 2019 r. poz. 742) oraz § 14 Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (tekst jedn.: Dz. U. z 2011 r. nr 159 poz. 948). W tym celu m.in. Starostwo Powiatowe w Nidzicy jest w trakcie uzgodnień z Państwowym Instytutem Badawczym NASK w celu pozyskania laptopa i telefonu do przetwarzania informacji niejawnych o klauzuli „zastrzeżone".

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. Szkolenia osób zaangażowanych w proces przetwarzania informacji

Starostwo wywiązało się z obowiązków przeprowadzenia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień związanych z zagrożeniem bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji oraz stosowanie środków zapewniających bezpieczeństwo informacji

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

UWAGI, REKOMENDACJE, ZALECENIA:

1. Analiza ważności licencji na oprogramowanie służące do przetwarzania danych osobowych.

Pouczenie

DB Group s.c.
ul. Popiełuszki 7/8
10-695 Olsztyn
tel. 502 610 282
NIP 7393737 042, REGON 280379420

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 Starostę

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

Podpis kierownika jednostki

STAROSTA
Marcin Paliński