OSO.1720.4.2019

OSO
24.09.2019
pm

Starostwo Powiatowe w Nidzicy
Wpłynęło dnia
2019 -09- 23
13807
L.dz. zał. podpis

AUDYT I WYCENA
Consulting Group Sp. z o.o.
we're making audit easier

AUDYT I WYCENA Consulting Group Sp. z o.o.
ul. Chmielna 2 lok. 31, 00-020 Warszawa
tel. (22) 299 58 30 Fax. (22) 266 09 11
NIP: 831-162-66-22 REGON: 101039946

RAPORT

z zadania audytowego pn.:

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

Nidzica, dnia 23.09.2019r.

Omówiono na posiedzeniu
Zarządu Powiatu w dniu 26.09.2019r.

Spis treści

I. WSTĘP – dane podstawowe.

W dniach 19 sierpnia – 23 września 2019r. firma AUDYT I WYCENA Consulting Group Sp. z o.o., z siedzibą w Warszawie, przy udziale Doroty Brandeburg - Audytora wewnętrznego, uprawnienia na podstawie art. 286, ust. 1 pkt. 1-4, 5) ppkt. d) Ustawy o finansach publicznych, przeprowadziła audyt pod nazwą: *„Audyt bezpieczeństwa informacji w Starostwie Powiatowym w Nidzicy, w tym ochrony danych osobowych".*

Audyt przeprowadzono w siedzibie Zamawiającego – Starostwie Powiatowym w Nidzicy.

Cel audytu.

Podstawowym celem audytu jest dostarczenie Staroście Powiatu Nidzickiego racjonalnego zapewnienia, że bezpieczeństwo informacji jest realizowane zgodnie z przepisami prawa, a wewnętrzna organizacja jednostki oraz przyjęte mechanizmy kontroli gwarantują prawidłowe wypełnianie obowiązków oraz zgodność w zakresie obowiązujących przepisów prawa.

Celem audytu jest ocena bezpieczeństwa danych osobowych oraz informacji przetwarzanych przy użyciu systemów teleinformatycznych, w tym sposobu zarządzania bezpieczeństwem informacji, z minimalnymi wymaganiami dla systemów teleinformatycznych określonych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247 t.j. z dnia 2017.12.05). Ponadto, celem audytu jest ocena bezpieczeństwa danych osobowych, zgodnie z Ustawą z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U.2018.1000) i Rozporządzeniem Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016r. 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. Urz. UE L 119 z 4.05.2016r.).

Uzyskanie racjonalnego zapewnienia w przedmiotowym obszarze funkcjonalnym ma charakter sprawdzenia bezpośredniego – badanie dokumentacji oraz sprawdzenia pośredniego – badanie działającego w jednostkach systemu kontroli zarządczej.

Zadaniem audytu jest również zdiagnozowanie istniejących problemów i nieprawidłowości – w przypadku ich stwierdzenia, celem audytu jest przedstawienie uwag i wniosków dotyczących zapewnienia zgodności postępowania.

Standardy audytu.

Audyt przeprowadzony został zgodnie z ***Międzynarodowymi Standardami Praktyki Zawodowej Audytu Wewnętrznego*** (Komunikat Ministra Rozwoju i Finansów z dnia 16 grudnia 2016r., Dz. Urz. MRIF poz. 28).

Podjęte czynności i zastosowane techniki przeprowadzenia audytu.

Dla przeprowadzenia badania obszaru objętego audytem, podjęto działania i zastosowano następujące techniki:

1. Badanie audytowi zgodne z przyjętą ankietą.
2. Przegląd przyjętej dokumentacji w zakresie wprowadzenia polityki bezpieczeństwa wraz z załącznikami.
3. Przegląd zabezpieczeń technicznych i organizacyjnych wprowadzonych w Starostwie.
4. Przyjęcie ustnych wyjaśnień od Informatyka zatrudnionego w Starostwie Powiatowym w Nidzicy – Pana Piotra Iwanickiego.

II. DZIAŁANIA AUDYTOWE.

Wszelkiego rodzaju informacje, w tym dane osobowe przetwarzane w Starostwie Powiatowym w Nidzicy jako jeden z zasobów każdej organizacji, podlegają ochronie. Informacje nie będące informacją publiczną, powinny być zabezpieczone przed nieuprawnionym dostępem, niezmiennością, szkodzeniem, utratą lub zniszczeniem. Ponadto przetwarzane dane powinny być dostępne dla upoważnionych osób zawsze wtedy, gdy występuje taka potrzeba. Brak właściwego zabezpieczenia danych, dla których minimalne wymagania zostały określone w rozdziałach III i IV Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247 t.j. z dnia 2017.12.05), poza naruszeniem przepisów w/w rozporządzenia może skutkować:

a) naruszeniem wymaganej przepisami prawa ochrony danych osobowych,

b) trudnościami w zarządzaniu jednostką ze względu na brak wiarygodnych i rzetelnych informacji dotyczących jej działalności, w tym informacji o stanie finansowym oraz innych ewidencjonowanych zasobach,
c) nieprawidłowościami w przekazywanych na zewnątrz sprawozdaniach i raportach.

W konsekwencji brak lub nieprawidłowości w zarządzaniu bezpieczeństwem danych osobowych i przetwarzaniem informacji naraża jednostkę, a w szczególności jej kierownika, na:

a) sankcje wymienione w Rozdziale VIII Rozporządzenia RODO,
b) sankcje wymienione w Rozdziale 11 Ustawy o ochronie danych osobowych (Dz.U.2018.1000),
c) sankcje wymienione w Ustawie z dnia 29 września 1994r. o rachunkowości (Dz.U.2018.395 t.j. z dnia 2018.02.20),
d) odpowiedzialność dyscyplinarną, z tytułu niewykonywania należyte kontroli w zakresie wykonywania zadań związanych z bezpieczeństwem informacji, w tym danych osobowych.

III. USTALENIA SZCZEGÓŁOWE AUDYTU.

Kryteria.

Zgodnie z powyżej przywołanymi aktami prawnymi każdy 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. Oznacza to, że wszelkie informacje przewarzane przez podmioty realizujące zadania publiczne, do których należy również Starostwo Powiatowe w Nidzicy, powinny być chronione i zabezpieczone w celu zapewnienia ich:

- integralności – ochrona danych mająca na celu zapewnienie dokładności i kompletności informacji oraz metod ich przetwarzania,
- dostępności – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów, wtedy gdy jest to potrzebne,
- poufności – zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym.

Wskazana ochrona powinna być realizowana na poziomie zabezpieczeń fizycznych, chroniących przed dostępem do pomieszczeń, sprzętu komputerowego, jak też zabezpieczających przed wypadkami losowymi, takimi jak np. pożar, powódź, przepięcia w sieci elektrycznej. Drugi poziom ochrony informacji powinien występować w obszarze logicznym, tj. zabezpieczenie dostępu na poziomie systemów informatycznych, danych stanowisk komputerowych czy też serwera, czyli zabezpieczenia wbudowane w wykorzystywane oprogramowanie komputerowe.

Stan faktyczny.

Opis stanu faktycznego audytowanego obszaru został podzielony na cztery podstawowe obszary, zaprezentowane poniżej. W oparciu o przeprowadzone czynności audytowe we wskazanym obszarze audytu, sformułowano następujące spostrzeżenia:

I. Formalne regulacje dotyczące ochrony danych.

W Starostwie Powiatowym w Nidzicy Zarządzeniem Nr Z/21/2019 Starosty Nidzickiego z dnia 30 sierpnia 2019r. w sprawie wprowadzenia Dokumentacji systemu zarządzania bezpieczeństwem informacji (polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych) w Starostwie Powiatowym w Nidzicy, przyjęte i wdrożone zostały formalnie do stosowania takie dokumenty jak:

- Polityka bezpieczeństwa informacji,
- Polityka bezpieczeństwa danych osobowych,
- Instrukcja zarządzania systemem informatycznym,
- Procedura realizacji praw osób, których dane dotyczą,
- Procedura przeprowadzania szacowania ryzyka i oceny skutków,
- Procedura zarządzania incydentami,
- Procedura zarządzania zmianą.

Elementy bezpieczeństwa informacji są zawarte także w oświadczeniach osób upoważnionych do przetwarzania danych osobowych, które są przez nich podpisywane po odbyciu przeszkolenia w zakresie stosowania środków technicznych i organizacyjnych przy przetwarzaniu danych osobowych.

Wymienione wyżej dokumenty stanowiące Politykę bezpieczeństwa informacji w Starostwie Powiatowym w Nidzicy opracowane zostały na podstawie Ustawy z dnia 10.05.2018r. o ochronie danych osobowych, Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016r. 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 Rozporządzenia Rady Ministrów z dnia 12.04.2012r. w sprawie Krajowych Ram Interoperacyjności, minimum wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Zawierają one wiele istotnych elementów związanych z ustanowieniem i zarządzaniem systemem bezpieczeństwa, takich jak: zarządzanie kontrolą dostępu, unikanie zagrożeń związanych z przetwarzaniem danych zapisanych na nośnikach papierowych jak i w systemach informatycznych, ochroną pomieszczeń, w których zlokalizowane są przetwarzane dane, ochroną przed zagrożeniami z sieci zewnętrznej, w tym ochroną antywirusową.

W Starostwie Powiatowym w Nidzicy ważnym elementem kontroli dostępu do przetwarzanych informacji, odpowiadających wymogom Krajowych Ram Interoperacyjności, są również:

a) Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.
b) Wykaz zbiorów danych osobowych.
c) Wykaz miejsc przetwarzania danych osobowych.
d) Opis struktury zbiorów osobowych.
e) Sposób przepływu danych pomiędzy systemami.
f) Ewidencja osób upoważnionych do przetwarzania danych osobowych.
g) Plany budynku.

Wprowadzona Zarządzeniem Nr Z/21/2019 Starosty Nidzickiego z dnia 30 sierpnia 2019r. zawiera dodatkowe dokumenty, które „wychodzą" naprzeciw wymogom, wynikającym z rozporządzenia RODO i (zaktualizowanej) ustawy o ochronie danych osobowych. W szczególności są to:

a) Powołanie (upoważnienie) Inspektora ochrony danych wraz z zakresem obowiązków.
b) Rejestr czynności przetwarzania.
c) Procedura realizacji praw osób, których dane dotyczą.
d) Procedura przeprowadzania szacowania ryzyka i oceny skutków.
e) Procedura zarządzania incydentami.
f) Zgłoszenia naruszenia ochrony danych osobowych (PUODO).

Zarządzeniem Nr Z/22/2019 Starosty Nidzickiego z dna 2 września 2019r. powołano Inspektora Ochrony Danych w Starostwie Powiatowym w Nidzicy oraz jednostkach organizacyjnych powiatu, a także dokonano zgłoszenia tego faktu do Urzędu Ochrony Danych Osobowych, zgodnie z wymaganym wzorem – Zawiadomienie o odwołaniu

dotychczasowego i wyznaczeniu nowego inspektora ochrony danych. Dokument podpisano podpisem elektronicznym i złożono w UODO w dniu 6 września 2019r.

Podczas działań audytowych stwierdzono, iż pracownicy Starostwa Powiatowego w Nidzicy, zostali przeszkoleni z zakresu zagadnień ochrony danych osobowych. Szkolenia odbyły się w dniu 11 marca 2019r. oraz 21 czerwca 2019r., co potwierdzają listy obecności na szkoleniach.

Całość Dokumentacji, przytoczonej powyżej, spełnia wymogi wynikające z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

II. Ochrona fizyczna.

III. Ochrona logiczna.

IV. Pozostałe środki ochrony bezpieczeństwa danych.

c) Powołanie Inspektora Ochrony Danych (IOD) i przydzielenie mu zadań, określonych w pkt. 7.2 Polityki bezpieczeństwa informacji.

Analiza ryzyka dla audytu bezpieczeństwa informacji wskazuje następujące czynniki ryzyka:

- nieuprawniony dostęp do danych, a przede wszystkim danych osobowych,
- zniszczenie posiadanych informacji,
- nieuprawniona i nieodwracalna zmiana informacji,
- nierzetelności i niejasność posiadanych informacji.

Potencjalne skutki zaistnienia w/w czynników ryzyka:

- naruszenie przepisów ustawy o ochronie danych osobowych i rozporządzenia RODO, co w konsekwencji skutkować może nałożeniem kar przewidzianych w tychże aktach prawnych,
- nierzetelna i niejasna sprawozdawczość,
- trudności w zarządzaniu jednostką.

Analiza przyczyn i skutków uchybień.

W oparciu o zebrane wyniki badania audytowego stwierdza się istnienie i funkcjonowanie formalnie zdefiniowanego systemu zarządzania bezpieczeństwem danych osobowych, który obejmują swoim zakresem działania wynikające z obecnie obowiązującego systemu prawnego – Ustawy z dnia 10 maja 2018r. o ochronie danych osobowych i 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), zwanym dalej RODO. Nie stwierdzono nieprawidłowości.

IV. REKOMENDACJE.

Biorąc pod uwagę specyfikę funkcjonowania administracji publicznej na szczeblu samorządu terytorialnego, a w szczególności zakres przetwarzanych informacji będących w dyspozycji i ich wykorzystanie, wydaje się że wiele ze zidentyfikowanych w trakcie audytu elementów zarządzania bezpieczeństwem informacji, jest adekwatnych i efektywnych. Stosowany obecnie system zarządzania bezpieczeństwem informacji spełnia swoje zadania w zakresie zapewnienia właściwej ochrony.

Po wykonaniu czynności audytowych stwierdzam, iż system bezpieczeństwa informacji, w tym bezpieczeństwa danych osobowych, w Starostwie Powiatowym w Nidzicy funkcjonuje w sposób skuteczny i adekwatny.

Zaleca się, aby Inspektor Ochrony Danych w Starostwie Powiatowym w Nidzicy, systematycznie dokonywał czynności sprawdzających funkcjonowanie sytemu bezpieczeństwa danych osobowych oraz na bieżąco prowadził szkolenia nowych pracowników, a także aktualizował rejestry, w tym załączniki do Polityki Bezpieczeństwa Informacji.

Nie stwierdzono uchybień o charakterze systemowym.

Nie wydano rekomendacji w zakresie objętym audytem.

Dorota Brandeburg

Audytor wewnętrzny

Nidzica, dnia 23.09.2019r.