Sprawozdanie
z audytu
nr 2/2018
w zakresie
systemu zarządzania
bezpieczeństwem informacji/danych
teleinformatycznych
i kontroli zarządczej
w Szkole Podstawowej w Pogorzeli

Termin audytu:	30.11.2018 r.
Data sprawozdania:	6.02.2019 r.
Audytor:	Adrian Chodubski CGAP, MF

Wstęp

Tematem zadania zapewniającego była ocena *„Systemu zarządzania bezpieczeństwem informacji/danych teleinformatycznych i kontroli zarządczej w Szkole Podstawowej w Pogorzeli"*. Zadanie audytowe zostało przeprowadzone zgodnie z rocznym planem pracy na rok 2018 – poz. 2, na podstawie Umowy zawartej pomiędzy Gminą Gołdap, a Aesco Group Sp. z o.o. W ramach czynności audytowych przeprowadzono wizytę audytową w dniu 30 listopada 2018 r. Audyt przeprowadził Adrian Chodubski, CGAP no. 1318 MF 1700/2005 – audytor spełniający wymogi o których mowa w art. 286 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Celem działań było przeprowadzenie audytu systemu zarządzania bezpieczeństwem informacji/danych teleinformatycznych i kontroli zarządczej w Szkole Podstawowej w Pogorzeli (Dalej: SP lub Szkoła). Zadanie audytowe przeprowadzone zostało w oparciu o program zadania z dnia 14 listopada 2018 r. Zakres audytu obejmował ocenę regulacji wewnętrznych Szkoły w zakresie systemu kontroli zarządczej oraz systemu zarządzania bezpieczeństwem informacji.

W trakcie czynności audytowych przeprowadzono wywiady z p. – Moniką Taudul - Dyrektorem SP w Pogorzeli oraz z p. Joanną Knych – inspektorem ochrony danych.

Ustalenia z audytu

Stwierdzono, iż regulacje wewnętrzne dot. systemu kontroli zarządczej w Szkole w Pogorzeli określone zostały w Regulaminie Kontroli Zarządczej, stanowiącym załącznik Nr 2 do Zarządzenia Nr 1 /2015/2016 Dyrektora Szkoły Podstawowej w Pogorzeli z dnia 15 września 2015 r. Regulacje wewnętrzne jednostki stanowią uzupełnienie ramowych zasad określonych na poziomie Urzędu Miejskiego w Gołdapi[1].

W zakresie funkcjonowania środowiska wewnętrznego placówki pracownicy Szkoły podpisali oświadczenia o zapoznaniu się z postanowieniami Kodeksu Etyki Pracowników Szkoły oraz

[1] Zarządzenie Nr 113/IV/11 w sprawie określenia zasad przeprowadzania kontroli zarządczej w Urzędzie Miejskim w Gołdapi i jednostkach organizacyjnych Gminy Gołdap oraz zasad jej koordynacji z dnia 12 kwietnia 2011 r.

zobowiązali się do stosowania jego postanowień. Ponadto w Szkole opracowano i wdrożono system delegowania uprawnień dla pracowników Szkoły.

Oświadczenia o stanie kontroli zarządczej

W wyniku przeprowadzonych czynności audytowych stwierdzono, iż na poziomie Szkoły wprowadzono praktykę opracowywania oświadczenia o stanie kontroli zarządczej, w treści określonej przepisami rozporządzenia wykonawczego[2]. W ramach czynności audytowych weryfikacji poddano dokumentację opracowywania oświadczeń za lata 2017-2018. Szkoła wskazywała, iż w jednostce w poddanym weryfikacji okresie w wystarczającym stopniu funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza. Dokumenty, zatwierdzane przez Dyrektora szkoły, przekazywane były w ramach systemu składania oświadczeń cząstkowych do Urzędu Miejskiego w Gołdapi, w celu opracowania oświadczenia o stanie kontroli zarządczej Burmistrza Gminy Gołdap. Audytor nie wnosi zastrzeżeń do badanego obszaru.

Samoocena systemu kontroli zarządczej i raporty ewaluacyjne

Szkoła w latach 2017-2018 dokonywała samooceny systemu kontroli zarządczej. Ocena dokonywana była na podstawie ankiet/ocen cząstkowych, dokonywanych przez pracowników Szkoły. Ponadto Szkoła corocznie opracowywała raporty z ewaluacji wewnętrznej. Badanie ankietowe przeprowadzone było każdorazowo na próbie uczniów, rodziców i nauczycieli. W okresie poddanym weryfikacji raporty opracowywane były przez Zespół, każdorazowo powołany przez Dyrektora Szkoły. Audytor nie wnosi zastrzeżeń do badanego obszaru

Zarządzanie ryzykiem

W wyniku przeprowadzonych czynności stwierdzono, iż Szkoła w latach 2014-2018 przeprowadziła ocenę ryzyka, zgodnie z metodologią określoną w regulacjach wewnętrznych Szkoły, tj:

[2] Rozporządzenie Ministra Finansów z dnia 2 grudnia 2010 r. w sprawie wzoru oświadczenia o stanie kontroli zarządczej (Dz.U. Nr 238, poz. 1581)

- obszar: Zapewnienie prawidłowego funkcjonowania jednostki - 8 ryzyk,
- obszar: Obsługa finansowo-księgowa – 4 ryzyka,
- obszar: Zasoby ludzkie - 3 ryzyka,
- obszar: Czynniki zewnętrzne – 4 ryzyka.

Ponadto jednostka zdefiniowała ryzyka w zakresie celów jednostki, określonych treści załącznika nr do Regulaminu kontroli zarządczej, w obszarze: realizacja podstawy programowej, zagrożenia wychowawcze, klasyfikacja, frekwencja.

Audytor podkreśla, iż modelowe podejście do budowy systemu sytemu kontroli zarządczej zakłada, iż kluczowym elementem systemu kontroli zarządczej jest proces zarządzania ryzykiem.

Proces zarządzania ryzykiem wdrożony w Szkole nie ma charakteru „iteracyjnego". Czynności związane z identyfikacją, oceną ryzyka przeprowadzane są w odstępach corocznych. W ramach procesu zarządzania ryzykiem na poziomie Szkoły nie dokonywano monitorowania wyników oceny ryzyka na przestrzeni poszczególnych lat oraz nie dokonywano weryfikacji środowiska wewnętrznego dokonanej oceny w ciągu roku kalendarzowego, w którym dokonano oceny ryzyka.

Stwierdzono, iż w ramach kart oceny ryzyka za lata 2017-2018 praktycznie nie uległy zmianie zarówno zdefiniowane czynniki ryzyka, jak również przypisane im wielkości prawdopodobieństwa oraz skutków. Audytor podkreśla, iż w ramach zdefiniowanych rejestrów ryzyka zdefiniowane są najczęściej przyczyny oraz skutki wystąpienia ryzyka, a nie zaś faktyczne ryzyka. W ramach wyników oceny ryzyka definiowane są typowe problemy, takie jak: awarie systemu informatycznego, nieterminowe przekazywanie informacji, itp. Ponadto w rejestrach ryzyka zauważalny jest trend definiowania zdarzeń zewnętrznych, na które właściciele ryzyka nie mają wpływu.

W ocenie audytora należy dokonać aktualizacji regulacji wewnętrznych w zakresie metodologii zarządzania ryzykiem, poprzez:

- wprowadzenie obowiązku okresowego monitorowania wyników oceny ryzyka, obejmującego dokonywanie w odstępach kwartalnych aktualizacji wyników oceny ryzyka (ocena pod kątem parametru prawdopodobieństwa oraz skutków),

- wprowadzenie mechanizmu definiowania ryzyka z wykorzystaniem metodologii „Bow-Tie", gdzie w procesie identyfikacji ryzyka definiowane są powiązane warz z nim przyczyny i skutki ryzyka.

Polityka Bezpieczeństwa i Instrukcja Zarządzania Systemem Przetwarzania Danych Osobowych w sposób tradycyjny oraz przy użyciu systemu informatycznego w Szkole

Stwierdzono, iż zasady zarządzania bezpieczeństwem informacji w Szkole zdefiniowano w treści Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Przetwarzania Danych Osobowych w sposób tradycyjny oraz przy użyciu systemu informatycznego w Szkole Podstawowej w Pogorzeli[3]. Obowiązki inspektora ochrony danych powierzone zostały p. Joannie Knych

Stwierdzono, iż w Szkole prowadzony jest rejestr wydanych upoważnień do przetwarzania danych osobowych, zgodny ze wzorem określonym w załączniku nr 2 do Polityki Bezpieczeństwa Informacji w SP w Pogorzeli. Dokument na dzień audytu obejmował 20 pozycji, w tym rejestr aktywnych upoważnień dla 17 osób. Wszyscy pracownicy Szkoły, w tym pracownicy gospodarczy podpisali oświadczenia o zachowaniu poufności i zapoznaniu się z przepisami PBI, obowiązującymi w Szkole.

W kontekście obowiązujących na dzień audytu przepisów stwierdzono, iż spełnione zostały wymogi bezpieczeństwa fizycznego w zakresie dostępu do pokoju nauczycielskiego, gdzie dostęp ograniczony jest poprzez mechanizm cyfrowy drzwi wejściowych. Dostęp do pomieszczenia mają wyłącznie osoby uprawnione, posiadające breloki zbliżeniowe. Ponadto częściowo spełnione zostały wymogi bezpieczeństwa fizycznego w zakresie dostępu do pomieszczenia dyrektora oraz inspektora ochrony danych/sekretarza, gdzie dostęp mają wyłącznie osoby wskazane powyżej osoby. Personel sprzątający ma dostęp do pomieszczenia wyłącznie w obecności uprawnionych osób. Dostęp do pomieszczenia mają wyłącznie osoby wskazane powyżej, posiadające klucze. Pomieszczenie Dyrektora oraz Sekretarza Szkoły znajduje się na parterze budynku. Audytor zwraca uwagę, iż w oknie pomieszczenia brak jest

[3] Zmiany w prowadzone aneksem Nr 1/2018 do Polityki Bezpieczeństwa z dnia 15 maja 2018 r., poprzez aktualizację załącznika nr 5 i wprowadzenie rodzaju danych i struktury zbiorów

zainstalowanej kraty zabezpieczające, co niesie za sobą wysokie ryzyko dostępu z zewnątrz osób nieuprawnionych.

Biorąc pod uwagę fakt, iż w pomieszczeniu Dyrektora i Sekretarza Szkoły przechowywane są kluczowe dokumenty dot. funkcjonowania podmiotu, w ocenie audytora należy wprowadzić rozwiązania minimalizujące ryzyko nieuprawnionego dostępu poprzez zainstalowanie zabezpieczenia zewnętrznego okna pomieszczenia. W przedmiotowym obszarze wydano zalecenie.

Stwierdzono, iż kopie zapasowe, które tworzone są w odstępach 3-miesiecznych, przechowywane są w metalowej, ogniotrwałej szafie pancernej, znajdującej się w pomieszczeniu Dyrektora i Sekretarza Szkoły.

Szkoła dokonała inwentaryzacji rodzajów dokumentacji i dostosowała wstępnie klasyfikacje dokumentacji w korelacji z Jednolitym Rzeczowym Wykazem Akt. Dokumentacja przechowywana jest w sposób uniemożliwiający dostęp osobom nieuprawnionym. Niszczenie dokumentacji papierowej odbywa się z wykorzystaniem niszczarki. W przypadku uszkodzeń mechanicznych nośników danych dane odzyskiwane są za pośrednictwem formy zewnętrznej.

Dokumentacja w formie papierowej przechowywana jest pomieszczeniu Dyrektora i Sekretarza Szkoły. Dokumentacja w formie elektronicznej przechowywana jest na dysku wspólnym do którego dostęp mają wyłącznie uprawnione osoby. System informatyczny wymusza cykliczną zmianę haseł. Zasady tworzenia haseł obejmują małe litery i duże litery oraz znaki specjalne. W okresie poddanym weryfikacji nie stwierdzono przypadków naruszenia danych osobowych.

Stwierdzono, iż do dnia przeprowadzenia audytu opracowano w dniu 14 maja 2018 r. rejestr czynności, obejmujący m.in. cele przetwarzania danych, kategorie osób których dane dotyczą, kategorie odbiorców którym dane mogą być ujawniane, itp. Audytor podkreśla, iż zakres informacji rejestru powinien zostać dostosowany do zakresu informacyjnego określonego w treści załącznika nr 18 projektu Polityki Bezpieczeństwa Danych Osobowych

w Szkole Podstawowej w Pogorzeli. Stwierdzono, iż każdy pracowników Szkoły posiadał upoważnienie do przetwarzania danych osobowych.

W ramach czynności audytowych w trybie czynności doradczych audytor w dniu 16 grudnia 2018 r. zgłosił uwagi do projektu Polityki Bezpieczeństwa Danych Osobowych w Szkole Podstawowej w Pogorzeli, w szczególności w obszarze zakresu upoważnienia do przetwarzania danych osobowych, zasad zgłaszania naruszeń ochrony danych osobowych, rejestru kategorii czynności przetwarzania danych.

Do dnia przeprowadzenia czynności audytowych przygotowano i przedstawiono nowy projekt wdrożenia zasad przetwarzania danych osobowych, dostosowanych kompleksowo do wymogów zapisów Rozporządzenia RODO[4] oraz zapisów nowej ustawy o chronię danych osobowych[5], przy czym nie został on jeszcze formalnie wdrożony.

W przedmiotowym obszarze wydano zalecenie.

Podsumowanie

Na podstawie przeprowadzonych czynności audytowych audytor wydaje ocenę pozytywną nt. systemu zarządzania bezpieczeństwem informacji/danych teleinformatycznych i kontroli zarządczej w Szkole Podstawowej w Pogorzeli.

Audytor wskazuje, iż niezbędne jest dostosowanie zasad zarządzania bezpieczeństwem informacji do nowych rozwiązań legislacyjnych. Stosowane w ramach audytowanego obszaru mechanizmy kontrolne, wynikające z funkcjonujących regulacji częściowo minimalizują możliwość materializacji zagrożeń mogących mieć istotny, negatywny wpływ na realizację celów i zadań Szkoły.

W audytowanym obszarze funkcjonuje adekwatny, skuteczny i efektywny system kontroli zarządczej, z zastrzeżeniami wskazanymi w treści sprawozdania.

[4] 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) (Tekst mający znaczenie dla EOG) *OJ L 119, 4.5.2016, p. 1–8.*

[5] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000).

Zalecenia

Lp.	Treść	Termin	Ryzyko
1	Należy dokonać formalnego wdrożenia zasad przetwarzania danych osobowych, dostosowanych kompleksowo do wymogów wynikających z treści 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 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.	30 czerwca 2019 r.	Ryzyko o charakterze wysokim (💣💣💣)
2	Należy wprowadzić rozwiązania minimalizujące ryzyko nieuprawnionego dostępu do pomieszczenia Dyrektora oraz Sekretarza Szkoły, poprzez zainstalowanie zabezpieczenia zewnętrznego okna pomieszczenia (np. zewnętrznej kraty).	31 marca 2019 r.	Ryzyko o charakterze niskim (💣)
3	W ocenie audytora należy dokonać aktualizacji regulacji wewnętrznych w zakresie metodologii zarządzania ryzykiem, poprzez: - wprowadzenie obowiązku okresowego monitorowania wyników oceny ryzyka, obejmującego dokonywanie w odstępach kwartalnych aktualizacji wyników oceny ryzyka (ocena pod kątem parametru prawdopodobieństwa oraz skutków), - wprowadzenie mechanizmu definiowania ryzyka z wykorzystaniem metodologii „Bow-Tie", gdzie w procesie identyfikacji ryzyka definiowane są powiązane warz z nim przyczyny i skutki ryzyka.	31 marca 2019 r.	Ryzyko o charakterze średnim (💣💣)
	Skala ryzyka: 💣 niskie, 💣💣 średnie, 💣💣💣 wysokie, ? krytyczne		

Adrian [illegible]
Audytor wewnętrzny
CGAP nr. 1318 MF 1700/2005

Zapoznałem się ze sprawozdaniem:	Zapoznałem się ze sprawozdaniem:
DYREKTOR Szkoły Podstawowej w Pogorzeli mgr Monika Wojtala-Taudul 07.02.2019 r.	BURMISTRZ GOŁDAPI Tomasz Luto
Dyrektor SP w Pogorzeli (data i podpis)	Burmistrz Gminy Gołdap (data i podpis)