

**Sprawozdanie
z audytu
nr 3/2018
w zakresie
systemu zarządzania
bezpieczeństwem informacji/danych
teleinformatycznych
i kontroli zarządczej
w Środowiskowym Domu
Samopomocy
„Słoneczny Dom” w Gołdapi**

Termin audytu:	20.12.2018 r.
Data sprawozdania:	14.02.2019 r.
Audytory:	Adrian Chodubski CGAP, MF



Wstęp

Tematem zadania zapewniającego była ocena „Systemu zarządzania bezpieczeństwem informacji/danych teleinformatycznych i kontroli zarządczej w Środowiskowym Domu Samopomocy „Słoneczny Dom” w Gołdapi”. Zadanie audytowe zostało przeprowadzone zgodnie z rocznym planem pracy na rok 2018 – poz. 3, na podstawie Umowy zawartej pomiędzy Gminą Gołdap, a Aesco Group Sp. z o.o. W ramach czynności audytowych przeprowadzono wizytę audytową w dniu 20 grudnia 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 środowiskowym Domu Samopomocy „Słoneczny Dom” w Gołdapi (Dalej: ŚDS). Zadanie audytowe przeprowadzone zostało w oparciu o program zadania z dnia 17 grudnia 2018 r. Zakres audytu obejmował ocenę regulacji wewnętrznych ŚDS w zakresie systemu kontroli zarządczej oraz systemu zarządzania bezpieczeństwem informacji.

W trakcie czynności audytowych przeprowadzono wywiady z p. – Sebastianem Liwak - inspektorem ochrony danych ŚDS.

Ustalenia z audytu

Stwierdzono, iż regulacje wewnętrzne dot. systemu kontroli zarządczej w ŚDS określone zostały w treści Zarządzenia Nr 6/ŚDS/2016 z dnia 19 grudnia 2016 r. dotyczącego wprowadzenia regulaminu kontroli zarządczej. W treści procedury określono:

- listę ryzyk występujących w jednostce,
- wzór kwestionariusza samooceny systemu kontroli zarządczej,
- wzór oświadczenia o stanie kontroli zarządczej.

Oświadczenia o stanie kontroli zarządczej

W wyniku przeprowadzonych czynności audytowych stwierdzono, iż na poziomie ŚDS wprowadzono praktykę opracowywania oświadczenia o stanie kontroli zarządczej, w treści



określonej przepisami rozporządzenia wykonawczego¹. W ramach czynności audytowych weryfikacji poddano dokumentację opracowywania oświadczeń za lata 2017-2018. ŚDS wskazywał, iż w jednostce w poddanym weryfikacji okresie w wystarczającym stopniu funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza. Dokumenty, zatwierdzane przez Dyrektora ŚDS, przekazywane były w ramach systemu składania oświadczeń częściowych 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

ŚDS w latach 2017-2018 przeprowadzał samoocenę systemu kontroli zarządczej. W okresie poddanym weryfikacji ocena systemu kontroli zarządczej dokonywana była wyłącznie przez Dyrektora ŚDS. W ocenie audytora niezbędne jest rozszerzenie katalogu osób dokonujących oceny systemu kontroli zarządczej. System kontroli zarządczej obejmuje całość procesów występujących w jednostce, zarówno w zakresie zadań merytorycznych, określonych w Statucie jednostki², jak również w zakresie zadań obsługowych komórek merytorycznych. Wskazana powyżej różnorodność zadań jednostki determinuje potrzebę oceny elementów systemu kontroli zarządczej przez wszystkich pracowników jednostki realizujących cele i zadania ŚDS, na różnych poziomach jego funkcjonowania. Audytor podkreśla, iż model systemu kontroli zarządczej opracowany został m.in. w oparciu o założenia modelu systemu kontroli wewnętrznej COSO II „Zarządzanie ryzykiem korporacyjnym – Zintegrowana Struktura Ramowa”. Według tego modelu kluczowe elementy systemu, w tym proces zarządzania ryzykiem, *„realizowany jest przez zarząd, kierownictwo lub inny personel przedsiębiorstwa”*. W związku z powyższym w ocenie audytora należy dokonać zmiany praktyki przeprowadzania procesu samooceny kontroli zarządczej, poprzez zaangażowanie w proces oceny wszystkich pracowników komórek merytorycznych i obsługowych ŚDS. W dokumentacji dot. procesu samooceny kontroli zarządczej stwierdzono brak kwestionariusza samooceny za rok 2018. W dokumentacji stwierdzono projekt dokumentu,

¹ Rozporządzenie Ministra Finansów z dnia 2 grudnia 2010 r. w sprawie wzoru oświadczenia o stanie kontroli zarządczej (Dz.U. Nr 238, poz. 1581)

² zgodnie z zapisami § 6 Statutu Środowiskowego Domu Samopomocy „Słoneczny Dom” w Gołdapi



bez oznaczenia daty jego sporządzenia oraz oznaczenia okresu którego dotyczy. W ocenie audytora należy dołączyć do dokumentacji dot. samooceny kontroli zarządczej arkusz oceny za rok 2018. W przedmiotowym obszarze wydano zalecenia.

Zarządzanie ryzykiem

W wyniku przeprowadzonych czynności stwierdzono, iż ŚDS w latach 2017-2018 przeprowadził ocenę ryzyka, zgodnie z metodologią określoną w regulacjach wewnętrznych jednostki.

Wyniki oceny ryzyka przedstawiono w treści protokołu z posiedzenia Zespołu ds. analizy ryzyka z dnia 13 stycznia 2017 r. Stwierdzono, iż zidentyfikowane ryzyka oraz poddane ocenie ryzyka zostały ujęte w rejestrze celów i ryzyka, który jest załącznikiem do protokołu.

Wyniki oceny ryzyka przedstawiono w treści protokołu z posiedzenia Zespołu ds. analizy ryzyka z dnia 17 stycznia 2018 r. Stwierdzono, iż zidentyfikowane ryzyka oraz poddane ocenie ryzyka zostały ujęte w rejestrze celów i ryzyka, który jest załącznikiem do protokołu.

Audytorka 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 ŚDS nie ma charakteru „iteracyjnego”. Czynności związane z identyfikacją, oceną ryzyka przeprowadzane są w odstępach corocznych. W ramach procesu zarządzania ryzykiem na poziomie ŚDS 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 wyników oceny ryzyka za lata 2017-2018 praktycznie nie uległy zmianie zarówno zdefiniowane czynniki ryzyka, jak również przypisane im wielkości prawdopodobieństwa oraz skutków. Audytorka 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 wraz z nim przyczyny i skutki ryzyka. W przedmiotowym obszarze wydano zalecenie.

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 ŚDS zdefiniowano w treści Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Środowiskowym Domu Samopomocy „Słoneczny Dom” w Gołdapi³. Obowiązki inspektora ochrony danych powierzone zostały p. Sebastianowi Liwak⁴.

Stwierdzono, iż w ŚDS prowadzony jest rejestr wydanych upoważnień do przetwarzania danych osobowych. Według danych na dzień 20 grudnia 2018 r. upoważnienia wydano szesnastu osobom. Stwierdzono, iż każda z osób posiada nadany identyfikator z przypisanym zakresem uprawnień⁵.

Stwierdzono, iż na poziomie ŚDS prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, w sposób umożliwiający prawidłową identyfikację historii i prawidłowości przetwarzania danych osobowych. Ponadto jednostka prowadzi ewidencję podmiotów którym powierzono przetwarzanie danych osobowych⁶.

³ Zarządzenie Nr 9 z dnia 24 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Środowiskowym Domu Samopomocy „Słoneczny Dom” w Gołdapi

⁴ Zarządzenie Nr 8/ŚDS/2018 Dyrektora Środowiskowego Domu Samopomocy „Słoneczny Dom w Gołdapi z dnia 21 maja 2018 r. w sprawie wyznaczenia Inspektora Ochrony Danych w Środowiskowym Domu Samopomocy „Słoneczny Dom” w Gołdapi

⁵ Zakres uprawnień obejmuje: Pełny dostęp/Brak dostępu/Przeglądanie/Wprowadzanie/Modyfikowanie/Kasowanie/Archiwizowanie.

⁶ Rejestr podmiotów którym powierzono dane osobowe (świadczenie usług hostingowych, realizacja zadań w zakresie BHP i ppoż).



Stwierdzono, iż dokumentacja przechowywana jest w pomieszczeniach do tego wyznaczonych. Na stanowiskach pracy mogą być dostępne jedynie dokumenty dotyczące danej sprawy/uczestnika. W jednostce stosowana jest „zasada czystego biurka”.

Stwierdzono, iż w ŚDS dokonano inwentaryzacji zbiorów danych, gdzie zdefiniowano dziewięć zbiorów danych⁷.

W zakresie dokumentacji regulujących Politykę Ochrony Danych Osobowych jednostki audytor zgłasza uwagi do zapisów załącznika nr 9 do Polityki, tj. do „Instrukcji Zarządzania Systemami Informatycznymi”. W ocenie audytora należy doprecyzować w treści Instrukcji:

- zasady korzystania z zewnętrznych nośników danych, w szczególności nośników danych zawierających dane medyczne. Obecnie dokumentacja medyczna przechowywana jest w jednostce wyłącznie w formie papierowej w zamkniętych szafach. Należy rozważyć dookreślenie zapisów definiujących zasady przechowywania dokumentacji medycznej również w formie elektronicznej,
- zasady monitorowania ruchu sieciowego, ze szczególnym uwzględnieniem klauzul informacyjnych o stosowaniu monitoringu sieciowego. W przypadku braku decyzji o dookreśleniu zasad tego monitoringu należy rozważyć możliwość rezygnacji z tej formy zabezpieczeń funkcjonujących w jednostce.

W przedmiotowym obszarze wydano zalecenia.

W zakresie dokumentacji Polityki Ochrony Danych Osobowych, w ocenie audytora, należy rozważyć wprowadzenie dokumentu dot. rejestru kategorii czynności przetwarzania, określającego wykaz zbiorów danych osobowych prowadzonych przez procesora, tj. przez podmiot, któremu dane są powierzane. Na dzień realizacji czynności audytowych ŚDS nie pełni roli „procesora”, jednakże stan obecny nie wyklucza możliwości przetwarzania danych w imieniu administratorów danych w przyszłości. W przedmiotowym obszarze wydano zalecenie.

⁷ Kandydaci do pracy, Pracownicy, Członkowie rodzin pracowników, Wynagrodzenia, Dane do przelewów bankowych, Uczestnicy SDS, Multimedia, Monitoring, ZFŚS



Podsumowanie

Na podstawie przeprowadzonych czynności audytowych audytor wydaje ocenę pozytywną nt. systemu zarządzania bezpieczeństwem informacji/danych teleinformatycznych i kontroli zarządczej w Środowiskowym Domu Samopomocy „Słoneczny Dom” w Gołdapi.

Audytor wskazuje, iż funkcjonujące regulacje minimalizują możliwość materializacji zagrożeń mogących mieć istotny, negatywny wpływ na realizację celów i zadań ŚDS.

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

Zalecenia

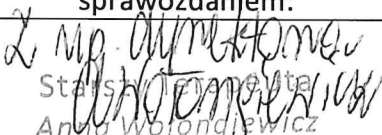
Lp.	Treść	Termin	Ryzyko
1	Należy dokonać zmiany praktyki przeprowadzania procesu samooceny kontroli zarządczej, poprzez zaangażowanie w proces oceny wszystkich pracowników komórek merytorycznych i obsługowych ŚDS.	Na bieżąco	Ryzyko o charakterze niskim (●)
2	Należy dołączyć do dokumentacji dot. samooceny kontroli zarządczej arkusz oceny za rok 2018.	Na bieżąco	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 wraz z nim przyczyny i skutki ryzyka.	30 czerwca 2019	Ryzyko o charakterze średnim (●●)
4	W ocenie audytora należy doprecyzować w treści Instrukcji Zarządzania Systemem Informatycznym: - zasady korzystania z zewnętrznych nośników danych, w szczególności nośników danych zawierających dane medyczne, - zasady monitorowania ruchu sieciowego, ze	30 czerwca 2019	Ryzyko o charakterze średnim (●□□)

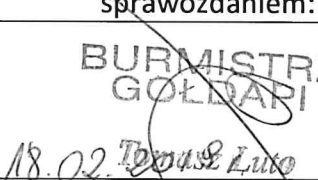
Sprawozdanie nr 3/2018 – Urząd Miejski w Gołdapi

System zarządzania bezpieczeństwem informacji/danych teleinformatycznych i kontroli zarządczej w Środowiskowym Domu Samopomocy „Słoneczny Dom” w Gołdapi

	szczególnym uwzględnieniem klauzul informacyjnych o stosowaniu monitoringu sieciowego lub rozważenie rezygnacji z tej formy zabezpieczeń.		
5	Należy rozważyć wprowadzenie dokumentu dot. rejestru kategorii czynności przetwarzania, określającego wykaz zbiorów danych osobowych prowadzonych przez procesora, tj. przez podmiot, któremu dane są powierzane.	Na bieżąco	Ryzyko o charakterze niskim (●)
Skala ryzyka: ● niskie, ●● średnie, ●●● wysokie, □ krytyczne			

Adrian Cichociński
Chotulski
Audytor wewnętrzny
C&A P m. 1318 MF 1700/2005

Zapoznałem się ze sprawozdaniem:
 Anna Woźniakiewicz 18.02.2018
Dyrektor ŚDS „Słoneczny Dom” w Gołdapi (data i podpis)

Zapoznałem się ze sprawozdaniem:
 BURMISTRZ GOŁDAP 18.02.2018
Burmistrz Gminy Gołdap (data i podpis)

Środowiskowy Dom Samopomocy
„Słoneczny Dom” w Gołdapi
tel. 87 307 00 10, 790 771 621
ul. 1-go Maja 21; 19-500 Gołdap
NIP: 847-161-32-32; REGON: 281515781