zapoznałem się
PREZYDENT MIASTA
30 CZE. 2015
Janusz Gromek

zapoznałem się:
ZASTĘPCA PREZYDENTA
ds. społecznych
2015 -06- 19
H. Woźniak

BAK.1711.8.2015.I

Kołobrzeg 19-06-2015

SPRAWOZDANIE

z planowanej kontroli

przeprowadzonej w Gimnazjum nr 1 z Oddziałami Integracyjnymi im. Bolesława Chrobrego w Kołobrzegu

Jednostka kontrolowana:

Gimnazjum Nr 1 z Oddziałami Integracyjnymi im. Bolesława Chrobrego w Kołobrzegu, ul. Portowa 37, 78-100 Kołobrzeg.

Temat kontroli:

Analiza i ocena realizacji zadań związanych z bezpieczeństwem informacji, wynikających w szczególności z ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku, nr 101 poz. 926 ze zm.) oraz przepisów wykonawczych wydanych na podstawie art. 39 a w/w ustawy.

Kontrolę przeprowadził:

Krzysztof Mielnikiewicz – inspektor ds. kontroli - Biuro Audytu i Kontroli Urzędu Miasta Kołobrzeg, na podstawie upoważnienia Nr OR.0052.27.2015.II z dnia 23 marca 2015 roku wydanego przez Prezydenta Miasta Kołobrzeg.

Termin przeprowadzania czynności kontrolnych:

24 marzec - 17 kwiecień 2015 rok.

Okres objęty kontrolą:

Czynności kontrole przeprowadzono w oparciu o bieżącą działalność jednostki.

USTALENIA OGÓLNOORGANIZACYJNE.

1. Gimnazjum nr 1 z Oddziałami Integracyjnymi im. Bolesława Chrobrego w Kołobrzegu, zwane dalej szkołą jest jednostką organizacyjną Gminy Miasto Kołobrzeg działającą w formie jednostki budżetowej.
2. Szkoła została utworzone na podstawie uchwały Nr XXIV/311/04 Rady Miejskiej w Kołobrzegu z dnia 16 czerwca 2004 roku.
3. Zarządzeniem Nr 10 2009/2010 Dyrektora Gimnazjum Nr 1 z Oddziałami Integracyjnymi im. Bolesława Chrobrego w Kołobrzegu z dnia 24 listopada 2009 roku wprowadzono w jednostce politykę bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Gimnazjum nr 1 z Oddziałami Integracyjnymi w Kołobrzegu.
4. Zarządzeniem nr 17 2013/2014 Dyrektora Gimnazjum Nr 1 z Oddziałami Integracyjnymi im. Bolesława Chrobrego w Kołobrzegu z dnia 27 stycznia 2014 roku wprowadzono Regulamin Ochrony Danych Osobowych oraz Instrukcję zarządzania systemem

przetwarzania danych osobowych przy użyciu systemu informatycznego i w sposób tradycyjny w Gimnazjum nr 1 z Oddziałami Integracyjnymi im. Bolesława Chrobrego w Kołobrzegu.

5. Kierownikiem jednostki w okresie obejmującym czynności kontrolne była Pani Lidia Mikołajek, powołana na to stanowisko przez Prezydenta Miasta Kołobrzeg z dniem 01 września 2009 roku, która funkcję tą pełni do chili obecnej.

II. USTALENIA SZCZEGÓŁOWE.

Zakres kontroli:

Kontrolą objęto wdrożone przez Dyrektora Gimnazjum nr 1 z Oddziałami Integracyjnymi im. Bolesława Chrobrego w Kołobrzegu procedury, które związane są z pojęciem bezpieczeństwa informacji, jak również sposób ich funkcjonowania w jednostce.

III. WNIOSKI.

Na wstępie zaznaczyć należy, że przetwarzanie danych osobowych jest pojęciem dość szerokim, na które składa się wiele czynników o charakterze zarówno wewnętrznym, jak i zewnętrznym. Zgodnie z art. 7 ust. 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku, Nr 101, poz. 926, ze zm. – wersja obowiązująca w okresie, za który przeprowadzano czynności kontrolne) poprzez pojęcie przetwarzania danych należy rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Bez względu na formę jaką przybiera przetwarzanie danych, dane te powinny być poddane szczególnej ochronie na co składa się między innymi wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem o czym mowa w art. 7, ust. 2b cyt. ustawy. Za ochronę danych osobowych w kontrolowanej jednostce odpowiada Dyrektor szkoły, który jednocześnie pełni rolę administratora danych, któremu zostały ściśle określone ustawowe zadania. **Dokonując ogólnej oceny sposobu wdrożenia, jak i samego funkcjonowania mechanizmów, które mają zapewnić szeroko rozumianą ochronę informacji w kontrolowanej jednostce, kontrolujący wskazuje, że wprowadzono działania, które pomimo wniesionych uwag dają zapewnienie bezpieczeństwa danych.**

1. Jednym z zabezpieczeń uważanych za powszechną praktykę w zakresie bezpieczeństwa informacji jest przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji.
   W myśl § 36, ust. 3 przedmiotowej ustawy Dyrektor szkoły wyznaczył administratora bezpieczeństwa informacji (dalej ABI). W wyniku analizy poszczególnych obowiązków, które przypisano dla ABI stwierdzono, że nie „wpisują" się one w pełni w obowiązki, które

wynikają z art. 36, ust. 3 w nawiązaniu do art. 36 ust. 1 cyt. ustawy o ochronie danych osobowych.

Ponadto, jako nieprawidłowość uznano, że w wewnętrznych procedurach ograniczono się do pełnienia przez ABI obowiązków, w zakresie nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych, jak również w zakresie ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych szkoły. Zarówno w świetle przepisów prawa, jak i literaturze przedmiotu, obowiązki ABI odnoszą się do całego, szerokiego systemu ochrony danych osobowych, a nie tylko do systemów informatycznych. Ponadto zaleca się, aby wszelka odpowiedzialność związana z bezpieczeństwem informacji była wyraźnie zdefiniowana co w opinii kontrolującego zostało wykonane w dość ogólny sposób. Jako mankament uznano, że nie dokonano rozdzielenia funkcji ABI od ASI, a wręcz jest to jedna i ta sama osoba. Co prawda osoba ta bezpośrednio odpowiada przed Dyrektorem szkoły, niemniej jednak odpowiada ona przed samym sobą za wdrożone mechanizmy, wykonywanie określonych obowiązków. Ostatecznie jednak, mając na uwadze specyfikę jednostki nie uznano łączenia ww. funkcji w ramach jednej osoby za nieprawidłowość czy też uchybienie, aczkolwiek wskazano na potencjalne ryzyka z tym związane.

2. Zgodnie z § 3, § 4 i § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024), zwanego dalej rozporządzeniem wykonawczym, administrator danych obowiązany jest do opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa, jak również instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej "instrukcją". Wartym podkreślenia jest fakt, że żadne z wyżej wymienionych regulacji prawnych nie wskazują na szczegółowość tych dokumentów. Jak wynika z wytycznych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych (dalej GIODO) „dokument określający politykę bezpieczeństwa nie powinien mieć charakteru zbyt abstrakcyjnego, a zasady postępowania w niej określone powinny zawierać uzasadnienie wyjaśniające przyjęte standardy i wymagania". Powyższe wskazuje również, że ww. dokumentacja powinna być zrozumiała dla pracowników. Odnosząc się do samych zapisów polityki bezpieczeństwa, którą wdrożono w jednostce uwagi wniesiono do tego, że poszczególne jej uregulowania, jak i sama nazwa dokumentu ograniczają się jedynie do systemów informatycznych służących do przetwarzania danych osobowych, natomiast zgodnie z § 3 ust. 1 cyt. rozporządzenia na dokumentację o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem

informatycznym służącym do przetwarzania danych osobowych. Ponadto wskazano na zbyt ogólne i nieaktualne postanowienia w zakresie wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Istotnym jest, że funkcjonujący w jednostce dokument nie spełnia wymogi wskazane odpowiednio w § 4 ust. 3 i 4 cyt. rozporządzenia.

Analiza poszczególnych zapisów instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wykazała, iż spełnia ona, co do zasady, warunki określone w rozporządzeniu, aczkolwiek uznano je za zbyt ogólne i budzące wątpliwości sformułowania. Zdaniem kontrolującego poszczególne zapisy instrukcji wymagają doprecyzowania i jednoznacznego sformułowania i wskazania osób które odpowiadają za wykonywanie określonych czynności. Przy aktualizacji zapisów z pewnością należy mieć wskazówki GIODO dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

3. Kontrolujący dokonał sprawdzenia czy jednostka wywiązała się obowiązku wynikającego z art. 40 cyt. ustawy o ochronie danych osobowych. Z ww. przepisu wynika, że administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Stwierdzono, że w większości przypadków kontrolowana jednostka podlega zwolnieniu od rejestrowania zbiorów danych z uwagi na zapisy art. 43, ust. 1, pkt 4 i 8 cyt. ustawy. W ramach czynności kontrolnych dokonano sprawdzenia czy zbiory danych znajdują się w jawnym rejestrze zbiorów danych osobowych, który prowadzony jest przez Generalnego Inspektora Ochrony Danych Osobowych w myśl art. 42, ust. 1 cyt. ustawy. Ustalono, że w rejestrze nie zarejestrowano jakiegokolwiek zbioru danych Gimnazjum nr 1. Nie mniej przedstawiono korespondencję mailową z GIODO (urzędowe poświadczenia odbioru) - z której wynika, że do GIODO wpłynęły zgłoszenia dotyczące odpowiednio zbioru danych osobowych o nazwie „uczniowie posiadający orzeczenie o niepełnosprawności" oraz zbiór danych osobowych o nazwie „księga ewidencji dzieci i młodzieży podlegających obowiązkowi szkolnemu".
4. Zgodnie z zapisami art. 37 cyt. ustawy administrator danych ma obowiązek nadania upoważnień osobom, które dopuszczone zostały do przetwarzania danych osobowych. W zakresie tym, stwierdzono również, że poszczególne sformułowania odnoszą się tylko do obsługi systemów informatycznych. Wymieniony art. 37 cyt. ustawy o ochronie danych osobowych obejmuje wszystkie osoby, które przetwarzają dane osobowe niezależnie od sposobu przetwarzania danych osobowych (tradycyjnego czy też w systemie

informatycznym). Ważnym jest także, że nie można ograniczać się tylko do osób zatrudnionych w jednostce. Stosowne upoważnienie powinny posiadać również osoby, które czasowo wykonują czynności – np. serwisanci sprzętu osoby z którymi zawarto umowy cywilno-prawne, itd. Stwierdzono ponadto, że w wewnętrznych regulacjach (polityce oraz instrukcji) nie określono wzoru, jak również nie doprecyzowano kto ma prowadzić ewidencję o której mowa w art. 39 ust. 1 przedmiotowej ustawy. Postanowienia te ujęto w funkcjonującym, równolegle obok polityki bezpieczeństwa oraz instrukcji, Regulaminie Ochrony Danych Osobowych, który Dyrektor szkoły wprowadził Zarządzeniem Nr 17 2013/2014 z dnia 27 stycznia 2014 roku. Regulacje te powinny znaleźć się w postanowieniach polityki bezpieczeństwa, jak i instrukcji lub też dokumenty te powinny zawierać odnośnik do procedury jaką jest ww. regulamin.

Ustalono, że dokumentacja dotycząca upoważnień (zarówno ewidencja, jak i same upoważnienia, oświadczenia) prowadzona jest przez samodzielnego referenta, który wykonuje obowiązki z zakresu kadr i płac. Ponadto kontrolującemu przedstawiono ewidencję, która spełniała wymogi określone w 39 ust. 1 przedmiotowej ustawy o ochronie danych osobowych, mianowicie zawierała imię i nazwisko osoby upoważnionej, datę nadania i ustania, zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator w przypadku przetwarzania danych w systemie informatycznym. Do powyższego nie wniesiono uwag.

W jednostce nie jest prowadzona ewidencja osób, które zostały zapoznane z dokumentem – polityka bezpieczeństwa, co niezgodne jest z zapisami rozdziału 5 pkt. 2 polityki bezpieczeństwa. W jednostce zbierane są jednak stosowne oświadczenia z treści których między innymi wynika fakt potwierdzający zapoznanie się pracownika z wewnętrznymi regulacjami. Ponadto stwierdzono, że w jednostce nie jest prowadzona dokumentacja związanej z przeszkalaniem osób, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych. Co prawda z wewnętrznych regulacji nie wynika obowiązek dokumentowania tego typu czynności aczkolwiek kontrolujący stoi na stanowisku, że podejmowane działania w tym zakresie powinny być ewidencjonowane. Cykliczne szkolenia dla pracowników zarówno z obsługi urządzeń i programów oraz samymi regulacjami wewnętrznymi są działaniami jak najbardziej pożądanymi, które przede wszystkim wpływają na świadomość pracowników na temat istotności obszaru związanego z ochroną danych osobowych. Wskazać należy, że w regulacjach wewnętrznych (polityce bezpieczeństwa) nie doprecyzowano do czyich obowiązków należy przeszkalanie osób.

Biorąc pod uwagę zakres upoważnień należy zaznaczyć, że został on określony dla każdej osoby w sposób indywidualny (dot. pracowników administracji oraz kierownictwa szkoły). W przypadku nauczycieli, było im wydane upoważnienie tylko do przetwarzania

danych osobowych w dzienniku elektronicznym. Poszczególni nauczyciele uczestniczą również np. w pracach komisji rekrutacyjnej, jak również przetwarzają dane osobowe w formie papierowej, a nie tylko w dzienniku elektronicznym, chociażby wskazać można dane wynikające z orzeczeń o niepełnosprawności, dzienników zajęć rewalidacyjnych (prowadzone w sposób tradycyjny) itp. Jak stwierdzono w przypadku Komisji Rekrutacyjnej Dyrektor Zarządzeniem nr 20 2013/2014 z dnia 13 lutego 2014 roku w sprawie naboru kandydatów do klas pierwszych w roku szkolnym 2013/2014 wprowadził kryteria przyjmowania uczniów do klas pierwszych, jednocześnie powołując komisję rekrutacyjną. Co prawda zobowiązano komisję rekrutacyjną do zapoznania się i przestrzegania przepisów dotyczących rekrutacji oraz ochrony danych osobowych i ich przetwarzania, aczkolwiek nie zostały wydane odrębne upoważnienia do przetwarzania danych osobowych w tym celu. Ponadto zastrzeżenia wniesiono do upoważnień wydanych dla Sekretarza Szkoły oraz Głównej księgowej. Tak na prawdę ograniczono się do systemów komputerowych, a nie na całości zagadnień związanych z ochroną danych osobowych. Ww. osoby przetwarzają także dane osobowe w sposób tradycyjny, poza wykorzystaniem oprogramowania. Uwag nie wniesiono do upoważnień, które zostały wydane dla członków Komisji Zakładowego Funduszu Świadczeń Socjalnych.

5. Jednym z wymogów, jakie powinien zostać spełniony. jest ten wynikający z art. 39 ust. 2 przedmiotowej ustawy. Wprowadza on po stronie osób, które są upoważnione do przetwarzania danych osobowych, obowiązek zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczenia. Stwierdzono, że jednostka przyjęła do stosowania oświadczenia z treści którego wynika, że pracownik zapoznał się z przepisami ustawy o ochronie danych osobowych oraz polityką i instrukcją i zobowiązał się ich przestrzegania w trakcie pracy w szkole oraz zachowania w tajemnicy wszystkich danych osobowych do których ma dostęp w związku z zatrudnieniem – także po ustaniu stosunku zatrudnienia. Dodatkowo przedkładano oświadczenia, w których dana osoba zobowiązywała się do nieujawniania w żadnej postaci i treści informacji dotyczących danych osobowych oraz spraw pracowniczych szkoły z wyjątkiem sytuacji kiedy jest to niezbędne dla celów służbowych. Jednocześnie osoba ta przyjmowała do wiadomości, że nieprzestrzeganie powyższego obowiązku może powodować odpowiedzialność z tytułu ciężkiego naruszenia obowiązków pracowniczych. Ważnym w niniejszym zakresie jest również, że sama treść upoważnień do przetwarzania danych osobowych zawiera klauzulę z której wynika, że osoba upoważniona zobowiązuje się do zachowania w tajemnicy wszelkich informacji o których wiedzę powziął w trakcie przetwarzania danych osobowych na mocy upoważnienia. Jak wynika z powyższego, żadna z ww. form nie odnosi się do obowiązku zachowania tajemnicy w zakresie sposobu zabezpieczenia

danych, jaki funkcjonuje w jednostce – co wynika bezpośrednio z art. 39, ust. 2 cyt. ustawy. Ponadto wskazane jest, aby wprowadzić jedną formę dokumentacji, która wypełniała będzie obowiązki wynikające z art. 39 i nie gromadzenie 3 odrębnych dokumentów w tym samym zakresie.

6. Kontrolujący dokonał oceny sposobu prowadzenia ewidencji nośników instalacyjnych i oprogramowania wykorzystywanego w Gimnazjum Nr 1 w Kołobrzegu. Głównym celem przeprowadzonych czynności było przede wszystkim sprawdzenie czy jednostka wykorzystuje oprogramowanie do którego posiada prawa. Przeprowadzone czynności kontrolne dały zapewnienie, że jednostka posiada legalne oprogramowanie, o czym świadczyły dokumenty takie jak umowy, licencje oraz dokumentacja księgowa.
   W wyniku analizy treści polityki bezpieczeństwa stwierdzono jednak brak zapisów, które regulowałyby obszar związany z licencjami oraz oprogramowaniem wykorzystywanym w jednostce, przede wszystkim brak jest regulacji, które przypisywałyby odpowiedzialność w tym zakresie. Biorąc pod uwagę przedstawioną dokumentację do wglądu ustalono, że zasadnym byłoby wprowadzenie jednolitych zasad ewidencjonowania zarówno oprogramowania, licencji jak i samego sprzętu komputerowego, przy czym zaznaczyć należy, że nie dotyczy to ewidencji księgowej. Co prawda nie jest to wymóg wynikający wprost z regulacji prawnych, niemniej w literaturze przedmiotu jest to element pożądany. Zwrócono uwagę, że w jednostce nie funkcjonują inne zabezpieczenia sprzętu komputerowego przed instalacją niechcianego oprogramowania – możliwa jest instalacja z nośnika zewnętrznego czy też bezpośrednio z pliku z sieci Internet.
7. Jako jeden z elementów, które wprowadzono w jednostce jest ten dotyczący przeprowadzanych kontroli w zakresie poprawności zabezpieczeń i przestrzegania przyjętej polityki bezpieczeństwa w Gimnazjum nr 1. Takie kontrole przeprowadzane są przez ABI w ciągu roku na podstawie zatwierdzonego przez Dyrektora Szkoły planu kontroli.
8. Kontrolujący przeprowadził czynności kontrolne mające na celu ustalenie czy i w jaki sposób jednostka wykonuje czynności związane z wykonywaniem kopii bezpieczeństwa. Obowiązek ten wynika bezpośrednio z Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U z 2004 roku, Nr 100, poz. 1024.). Biorąc pod uwagę przeprowadzoną analizę samych zapisów wewnętrznych regulacji wskazać należy, że nie zawierają one w pełni postanowień zawartych w wytycznych GIODO. W instrukcji nie doprecyzowano sposobu sporządzania kopii zapasowych, np. czy są to kopie sporządzane są w sposób przyrostowy, czy całościowy. Nie podano także oprogramowania, które wykorzystywane

jest do tego typu czynności. Ponadto w instrukcji zaznaczono, że w przypadku awarii należy okresowo sprawdzać kopie pod kątem ich przydatności, co uznano za działanie niepożądane. Okresowe sprawdzanie kopii powinno odbywać się w sposób cykliczny (sprawdzenie kopii po wystąpieniu awarii może okazać się bezskuteczne), jak również co istotne tego typu czynności powinny być dokumentowane, czego nie potwierdzono. Ponadto nie wiadomym jest kto odpowiada za wykonywanie kopii, ich gromadzenie i weryfikację oraz nie doprecyzowano odpowiedzialności za niszczenie nośników danych po ustaniu ich użyteczności. Ponadto w instrukcji zapisano, że kopie okresowe są sporządzane na płytach CD/DVD – co w praktyce nie jest stosowane. Nie dookreślono również czasu przechowywania tego typu kopii.

9. Jednym z elementów, które składają się na bezpieczeństwo danych osobowych jest zabezpieczenie samego pomieszczenia, w którym znajdują się serwery jednostki - tzw. serwerowni. W wyniku przeprowadzonych oględzin, które przeprowadzono w obecności Informatyka stwierdzono, że w jednostce funkcjonują zarówno techniczne jak i logiczne zabezpieczenia dostępu do pomieszczenia serwerowni. Jako słabość zabezpieczenia serwerów od strony samego pomieszczenia wskazać należy, że panuje w nim odczuwalna wysoka temperatura. Stwierdzono, że w pomieszczeniu serwerowni znajduje się jedynie otwór od wentylacji grawitacyjnej. Ponadto zaznaczenia wymaga, że na urządzeniach na którym gromadzone są dane w tym kopie bezpieczeństwa umieszczone są również poza serwerownią. Dotyczy to urządzenia, które znajduje się w gabinecie Wicedyrektora jednostki. Należałoby rozważyć, aby wszystkie tego typu urządzenia, które pełnią funkcją serwerów znajdowały się w jednym pomieszczeniu, spełniającym podstawowe zasady bezpieczeństwa. Jako mankament należy uznać, że w serwerowni brak jest urządzeń systemu przeciwpożarowego, aczkolwiek szkoła posiada zawartą umowę na ochronę fizyczną obiektu oraz stały monitoring budynku, a w pobliżu serwerowni znajdują się gaśnice poddawane okresowym przeglądom.

   Zgodnie z wewnętrznymi regulacjami w jednostce prowadzony jest zeszyt wejść do serwerowni. Aby Informatyk mógł wejść do pomieszczenia serwerowni musi najpierw otrzymać klucze, które przechowywane są w sejfie. Nadmienić w tym zakresie należy, że w jednostce nie wdrożono w sposób formalny zasad wydawania i zdawania kluczy do pomieszczeń, jak również samego dostępu do budynku szkoły, które wymaga uprzedniego rozbrojenia alarmu. Analiza poszczególnych zapisów wykazała, że wejścia do serwerowni zdarzają się sporadycznie. W zakresie zabezpieczenia samego budynku oraz jego części stwierdzono, że kontrolowana jednostka zawarła umowy na całodobowe elektroniczne monitorowanie obiektu. Ponadto w jednostce funkcjonuje system telewizji obserwacyjnej (tzw. monitoring). Dyrektor szkoły zawarł umowę z firmą zewnętrzną na utrzymanie w całej gotowości sprawności eksploatacyjnej ww. monitoringu. Ponadto

przedstawiono kontrolującemu aktualną dokumentację dotyczącą wykonanych cyklicznych przeglądów stanu technicznego budynku jak i zabezpieczeń przeciwpożarowych (przeglądy gaśnic).

10. Kontrolujący w ramach czynności kontrolnych przeprowadził oględziny w obecności Dyrektora szkoły, których głównym celem było ustalenie sposobu zabezpieczenia pomieszczeń pracy i stanowisk roboczych przed nieuprawnionym dostępem do danych osobowych po zakończeniu pracy przez pracowników. W wyniku tych czynności stwierdzono, że same pomieszczenia były zabezpieczone przed niepożądanym dostępem, aczkolwiek w 2 przypadkach umożliwiony był dostęp do dokumentacji, w tym dokumentacji z tzw. danymi sensytywnymi z uwagi na niezabezpieczenie szaf. W 1 przypadku stwierdzono, że pracownik na tzw. zapleczu biblioteki pozostawił dzienniki zajęć rewalidacyjnych, zawierające dane osobowe uczniów oraz rodziców/opiekunów prawnych wraz z danymi tzw. sensytywnymi z uwagi na szczególny rodzaj prowadzonych zajęć.
11. W zakresie przeprowadzonych czynności kontrolnych polegających na weryfikacji sposobu zabezpieczenia poszczególnych stacji roboczych stwierdzono, że przyjęte do stosowania procedury wymagają uaktualnienia jak i doprecyzowania. Szczegółowe czynności na stacjach roboczych poszczególnych pracowników wykazały, że w rzeczywistości podejmowane są działania, a nie zostały one sformalizowane. W instrukcji zapisano, że rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji. Trudno nie odnieść wrażenia, że tego typu zapis faktycznie nie jest stosowany. Pod wątpliwość poddano, aby każdy z użytkowników danego oprogramowania faktycznie zapoznał się z taką instrukcją. O wiele lepszym rozwiązaniem jest przeprowadzanie cyklicznych wewnętrznych szkoleń z pracownikami, niż nakładanie na ich ww. obowiązków. Dalsze szczegółowe czynności wykazały, że każdy pracownik postępował przy wyłączaniu stacji roboczej w sposób określony w wewnętrznych regulacjach. Poszczególni pracownicy mają dostęp do oprogramowania merytorycznego poprzez podanie loginu i hasła. Niemniej jednak nie ma to odzwierciedlenia w prowadzonej ewidencji osób upoważnionych, w której ujęte są tylko identyfikatory, co wykazały czynności, do oprogramowania dziennika elektronicznego. W przypadku logowania się do systemu informatycznego (oprogramowanie operacyjne) pracownicy administracji mieli indywidualne identyfikatory oraz hasła. Nadmienić w tym miejscu należy, że stosowane identyfikatory przez poszczególnych pracowników administracji nie były zgodne z identyfikatorami umieszczonymi w ewidencji, o której mowa w art. 39, ust. 1 cyt. ustawy o ochronie danych osobowych. W przypadku nauczycieli stwierdzono, że stosowany był jeden identyfikator (różny w zależności od stacji roboczej), ale z tym samym hasłem. Jak

wynika ze złożonych wyjaśnień przez Dyrektora szkoły na tę okoliczność, jeden identyfikator oraz hasło do stacji roboczych w salach lekcyjnych związane jest z tym, że w jednej klasie prowadzone są zajęcia przez różnych nauczycieli, a mają oni jedynie dostęp do dziennika elektronicznego i do prowadzenia zajęć. Nie ma zainstalowanego innego oprogramowania w których następuje przetwarzanie danych osobowych. Logowanie do dziennika elektronicznego następuje po podaniu indywidualnego identyfikatora oraz hasła. Po zasięgnięciu opinii Kierownika Biura Informatyki Urzędu Miasta Kołobrzeg, wskazano kierownikowi jednostki, że istotnym staje się brak możliwości precyzyjnego, jednoznacznego ustalenia szeroko rozumianej odpowiedzialności. Dany pracownik używając ogólnego loginu oraz hasła pozostaje anonimowy. Powyższe ma również istotne znaczenie przy zabezpieczeniu danych znajdujących się w sieci szkolnej. Stosowanie jednego loginu oraz hasła przez kilka osób stwarza zagrożenia jak np. ściągnięcie nielegalnego oprogramowania, niechcianego zawirusowania stacji roboczej, celowe wykorzystanie dostępu do „sparaliżowania" działania jednostki i wiele innych. W wyniku przeprowadzonych czynności kontrolnych stwierdzono, że w jednym przypadku pracownik na tablicy korkowej miał przyczepioną karteczkę z podanym hasłem do stacji roboczej. Jeden tego typu przypadek pozwolił kontrolującemu na zalogowanie na stacjach roboczych w pozostałych klasach. Tego typu rozwiązanie (stosowanie jednego identyfikatora oraz hasła) w połączeniu z opisaną powyżej sytuacją daje możliwości do zalogowania się na każdą stację roboczą w salach lekcyjnych. Bezspornym jest, że tego typu słabości należy jak najszybciej wyeliminować. Trafnym jest stwierdzenie GIODO, który w wydanych wytycznych wskazał, że aby skutecznie zabezpieczyć system należy usunąć wszystkie słabości, podczas gdy wystarczy znaleźć jedną, aby skutecznie zaatakować. W trakcie przeprowadzanych czynności kontrolnych stwierdzono ponadto, że psycholog poprzez logowanie się do dziennika elektronicznego miał również dostęp do modułu sekretariat, w którym znajdują się inne zbiory danych niż w przypadku ograniczonego dostępu do samego dziennika elektronicznego. Wobec powyższego należałoby dokonać weryfikacji uprawnień pracowników do poszczególnych modułów oprogramowania. W 4 przypadkach stwierdzono, że pracownik używał haseł, które składały się z mniejszej ilości znaków niż wymagane 8, tym samym nie zostały spełnione obowiązki wynikające z punktu 8 części B załącznika do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W większości przypadków stwierdzono, że stacje robocze podłączone były do urządzeń typu UPS, które podtrzymują napięcie. W każdym

przypadku potwierdzono, że dana stacja robocza była zabezpieczona oprogramowaniem antywirusowym, który posiadał zaktualizowaną bazę. W 3 przypadkach stwierdzono, że stacja robocza nie była w ogóle chroniona wygaszaczem, w 6 przypadkach nie wymagane było podanie hasła w celu przywrócenia pracy w systemie operacyjnym. Nadmienić w tym zakresie należy, że tego typu wymogi nie zostały ujęte w wewnętrznych procedurach. W opinii kontrolującego tego typu zabezpieczenia powinny być jednak stosowane, jak również powinny one zostać uregulowane formalnie przez co pozwoli na ujednolicenie sposobu działania w tym zakresie. Uwagi kontrolujące budzi fakt, że stacje robocze na których pracują nauczyciele są urządzeniami typu laptop, a jak wynika z rozmowy z informatykiem nauczyciele wykorzystują komputery poza miejscem pracy. W wewnętrznych procedurach brak jest zapisów, które regulowałyby ten obszar. Niemniej jednak kontrolującemu przedstawiono dokumentację z której wynika, że Dyrektor szkoły zawierał umowy użyczenia komputerów w ramach Zintegrowanego Systemu Zarządzania Oświatą Vulcan realizowanego w ramach projektu Gmin@ na fali z nauczycielami szkoły oraz umowy użyczenia z nauczycielami na przekazanie w użyczenie tabletów nauczycielom prowadzącym zajęcia lekcyjne w cyfrowej klasie.

12. Mając na uwadze rodzaj i przedmiot zawartych umów zawieranych przez Dyrektora szkoły dokonano sprawdzenia czy same umowy zawierają postanowienia w zakresie ochrony danych osobowych oraz czy w uzasadnionych przypadkach administrator danych dokonał powierzenia innemu podmiotowi przetwarzanie danych w myśl art. 31, ust. 1 i 2 ustawy z dnia 27 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926, ze zm. – wersja obowiązująca w okresie, który poddano kontroli). Podkreślić należy, że główną intencją regulacji z art. 31 cyt. ustawy jest zapobieżenie sytuacji, w której powierzenie przez administratora innemu podmiotowi przetwarzania danych prowadziłoby do osłabienia ochrony, uszczuplałoby uprawnienia osób, których dane te dotyczą. W wyniku przeprowadzonych czynności kontrolnych, ustalono że w przypadku umowy z pielęgniarką szkolną nie ujęto tej osoby w ewidencji osób upoważnionych do przetwarzania danych osobowych o której mowa w art. 39, ust. 1 ustawy o ochronie danych osobowych, jak również dla tej osoby nie zostało wydane upoważnienie do przetwarzanie danych osobowych o którym mowa w art. 37 przedmiotowej ustawy. Ponadto nie zawarto dodatkowej umowy o której mowa w art. 31 ust. 1 przedmiotowej ustawy dotyczącej przetwarzania danych przez inny podmiot. W przypadku zawartej umowy na świadczenie usług w zakresie bezpieczeństwa i higieny pracy ustalono, że nie została zawarta umowa art. 31 ust. 1 przedmiotowej ustawy. Zwrócić należy uwagę, że jednostka wykorzystuje oprogramowanie do spraw zarówno administracyjnych – prowadzenie sekretariatu, księgowości, dziennika

elektronicznego itp. Administrator Danych powierzył w tym przypadku dane osobowe zarówno pracowników jednostki, kontrahentów, uczniów, rodziców/opiekunów prawnych podmiotowi zewnętrznemu przy czym nie zachował ciążącego na nim obowiązku zawarcia stosowanej umowy w myśl art. 31, ust. 1 przedmiotowej ustawy o ochronie danych osobowych, co należałoby dokonać.

13. Jak wykazały czynności kontrolne jednostka w ramach naboru wymaga złożenia wniosku do którego należy dołączyć kopię orzeczenia Poradni Psychologiczno-Pedagogicznej, orzeczenia o niepełnosprawności, opinię Poradni Psychologiczno-Pedagogicznej oraz we wniosku należy wskazać inne dysfunkcje, choroby, o których powinna wiedzieć szkoła. Ważnym jest, że w ramach funkcjonowania szkoły tworzone są oddziały integracyjne w celu umożliwienia uczniom niepełnosprawnym rozwoju społecznego oraz zdobycia wiedzy i umiejętności wspólnie z rówieśnikami, jak najbliżej miejsca zamieszkania. Zgodnie z zapisami art. 27 ust. 1 cyt. ustawy o ochronie danych osobowych *„Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym."* Przeprowadzona analiza wykazała, że kontrolowana jednostka przyjęła do stosowania wniosek w którym ujęto między innymi klauzulę o treści: *„Oświadczam, że wyrażam zgodę na przetwarzanie danych osobowych oraz rejestrowanie wizerunku mojego dziecka podczas zajęć, konkursów, zawodów sportowych i uroczystości organizowanych przez Gimnazjum nr 1 z Oddziałami Integracyjnymi w Kołobrzegu oraz wykorzystanie tego wizerunku poprzez umieszczanie zdjęć na stronie internetowej szkoły, w kronice szkoły oraz tablicach ściennych i folderach szkolnych w celu informacji i promocji szkoły."* Ostatecznie do powyższego nie wniesiono uwag, z uwagi, że art. 27, ust. 2, pkt 1 wskazuje, że przetwarzanie powyższych danych jest dopuszczalne, jeżeli osoba której dane dotyczą, wyrazi na to zgodę na piśmie. Jak wynika z powyższego tego typu pisemna zgoda znajduje się na wniosku o przyjęcie do szkoły, nie mniej nie zwalnia to administratora tych danych od podejmowania dodatkowych działań mających na celu zabezpieczenie tych danych.

Podsumowując przeprowadzone czynności kontrolne wskazać należy, że kontrolujący **pomimo stwierdzonych uchybień i nieprawidłowości w sposób pozytywny ocenia proces związany z przetwarzaniem danych osobowych w Gimnazjum nr 1 z Oddziałami Integracyjnymi im. Bolesława Chrobrego w Kołobrzegu.**

Dyrektor szkoły, który pełni obowiązki administratora danych osobowych podjął działania w celu zabezpieczenia danych osobowych począwszy od samego wdrożenia uregulowań wewnętrznych o których mowa w § 3, ust. 1 rozporządzenia wykonawczego, poprzez prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, stosowanie zabezpieczeń antywirusowych, po wdrożenie zasad tzw. „czystego biurka", stosowanie zamykanych szaf, sejfu itp. Niemniej jednak kontrolujący wskazuje na pewne luki, słabości systemu przetwarzania danych osobowych, które przy uwzględnieniu wytycznych GIODO należy wyeliminować. Podkreślenia wymaga fakt, że zarówno polityka bezpieczeństwa, jak i instrukcja, nie były poddawane aktualizacji od momentu ich wdrożenia, tym samym pewne ich zapisy uległy zdezaktualizowaniu, jak również we wskazanych elementach, dokumentacja ta nie spełnia w pełni wymogów określonych w rozporządzeniu wykonawczym. Niepokojącym jest także, że kierownik jednostki ograniczył się do zapisów regulujących poszczególne obszary przetwarzania danych osobowych tylko w systemach informatycznych, nie uwzględniając tradycyjnych metod ich przetwarzania.

Zasadnym jest, aby kierownik jednostki dokonał przeglądu i aktualizacji obowiązków, które zostały nałożone na administratora bezpieczeństwa informacji. Związane jest to z tym, że pewne czynności należące do obowiązków ABI zostały scedowane na poszczególnych pracowników jednostki (osoba zajmująca się sprawami kadrowymi i płacowymi oraz kierownik administracyjny), a nie zostało to sformalizowane (ani w postanowieniach polityki bezpieczeństwa i instrukcji, jak i w indywidualnych zakresach czynności). Dodatkowo powierzone obowiązki dla ABI kontrolujący ocenił, jako nie wpisujące się w pełni postanowienia przedmiotowej ustawy o ochronie danych osobowych, co szczegółowo wskazano w protokole.

Kontrolujący zwraca również uwagę, aby kierownik jednostki w uzasadnionych przypadkach zawierał umowy o powierzeniu danych osobowych w myśl art. 31, ust. 1 cyt. ustawy o ochronie danych osobowych.

Kołobrzeg, dnia 19.06.2015r.

Kontrolujący

INSPEKTOR
ds. kontroli
Krzysztof Mielnikiewicz
19.06.2015r

PEŁNOMOCNIK
d/s OCHRONY INFORMACJI NIEJAWNYCH
Marek Hilbert
1.07.15.

Sprawdzono pod kątem ustawy o ochronie danych osobowych
KIEROWNIK
Biura Kontroli
Sławomir Dąsalski
18.06.2015