PREZYDENT MIASTA

Janusz Gromek

BAK.1711.24.2014.I

ZASTĘPCA PREZYDENTA
ds. społecznych

Kołobrzeg, 26-03-2015

SPRAWOZDANIE

z planowanej kontroli

przeprowadzonej w Miejskim Ośrodku Pomocy Społecznej w Kołobrzegu

Jednostka kontrolowana:

Miejski Ośrodek Pomocy Społecznej w Kołobrzegu, ul. Okopowa 15, 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.0052.199.2014.II z dnia 02 grudnia 2014 roku wydanego przez Prezydenta Miasta Kołobrzeg.

Termin przeprowadzania czynności kontrolnych:

04 – 23 grudzień 2014 rok.

Okres objęty kontrolą:

Czynności kontrole przeprowadzono w oparciu o bieżącą działalność jednostki.

I. USTALENIA OGÓLNOORGANIZACYJNE.

1. Miejski Ośrodek Pomocy Społecznej w Kołobrzegu (dalej MOPS) jest jednostką organizacyjną Gminy Miasto Kołobrzeg działającą w formie jednostki budżetowej.
2. Uchwałą Nr XXIV/307/04 Rady Miejskiej w Kołobrzegu z dnia 16 czerwca 2004 roku nadano jednostce statut.
3. Zarządzeniem Nr 9/12 Prezydenta Miasta Kołobrzeg z dnia 10 stycznia 2012 roku zatwierdzony został Regulamin Organizacyjny MOPS w Kołobrzegu (ostatnie zmiany wprowadzono zarządzeniem nr 56/12 Prezydenta Miasta Kołobrzeg z dnia 12 czerwca 2012 roku).
4. Zarządzeniem Nr 6/2011 Dyrektora MOPS w Kołobrzegu z dnia 04 lutego 2011 roku wprowadzono w jednostce politykę bezpieczeństwa przetwarzania danych osobowych oraz instrukcję zarządzania systemami informatycznymi w MOPS.
5. Kierownikiem jednostki w okresie obejmującym czynności kontrolne była Pani Grażyna Foszcz – Mirecka, powołana na to stanowisko z dniem 01 stycznia 1993 roku, która funkcję tą pełni do chili obecnej.

II. USTALENIA SZCZEGÓŁOWE.

Zakres kontroli: Kontrolą objęto wdrożone przez Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Kołobrzegu procedury, które związane są z pojęciem bezpieczeństwa informacji, jak również sposób ich funkcjonowania w jednostce.

III. WNIOSKI. Dokonując oceny zakresu jaki został poddany kontroli należy zaznaczyć, 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 2014 roku, poz. 1182, ze zm.) 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 MOPS, który pełni jednocześnie rolę administratora danych, któremu zostały określone zadania zgodnie z zapisami art. 36, ust. 1 i 2 cyt. ustawy.

Dokonując ogólnej oceny sposobu wdrożenia, jak i samego funkcjonowania mechanizmów, które mają zapewnić szeroko rozumianą ochronę informacji w kontrolowanej jednostce, stwierdzono, że wprowadzono działania, które dają zapewnienie bezpieczeństwa danych.

Jednym z zabezpieczeń uważanych za powszechną praktykę w zakresie bezpieczeństwa informacji jest przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji co wynika wprost z zapisów § 36 ust. 3 cyt. ustawy o ochronie danych osobowych (wersja obowiązująca w okresie za który przeprowadzano czynności kontrolne). W zakresie tym ustalono, że Dyrektor MOPS'u w Kołobrzegu wyznaczył Administratora Bezpieczeństwa Informacji (dalej ABI), co zostało ujęte w § 3 Zarządzenia Nr 6/2011 Dyrektora MOPS w Kołobrzegu z dnia 04 lutego 2011 roku w sprawie wprowadzenia Polityki bezpieczeństwa przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Kołobrzegu oraz Instrukcji zarządzania systemami informatycznymi w Miejskim Ośrodku Pomocy Społecznej, a szczegółowe obowiązki ABI przedstawia załącznik nr 1 do cyt. zarządzenia. W polityce bezpieczeństwa znajdują się także zapisy odnoszące się do Administratora Systemów Informatycznych (dalej ASI), którego zadania przedstawia załącznik nr 2 do polityki bezpieczeństwa. W wyniku weryfikacja struktury zatrudnienia kontrolujący jako prawidłowe działanie uznał rozdzielenie funkcji ABI od ASI. Obowiązki ABI powierzono pracownikowi, który nie jest uzależniony od pionu służb informatycznych i co istotne

pracownik ten podlega bezpośrednio Dyrektorowi MOPS, a nie np. służbom informatycznym, co byłoby działaniem niepożądanym. Szczegółowe czynności wykazały, że jednostka dokonała zgłoszenia zbiorów danych do Generalnego Inspektora Ochrony Danych Osobowych, co zgodne jest z zapisami art. 40 cyt. ustawy o ochronie danych osobowych. Potwierdzono, że w każdym przypadku jednostka jest w posiadaniu zaświadczenia o zarejestrowaniu zbioru danych, o czym mowa w art. 42, ust. 3 i 4 cyt. ustawy.

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 jednostki i przede wszystkim dostosowana do jej wielkości i specyfiki. Przeprowadzona analiza ww. dokumentów wykazała, że w przypadku polityki bezpieczeństwa dokument ten spełnia wymogi określone w § 4 pkt. 1-5 cyt. rozporządzenia. W ocenie kontrolującego poszczególne zapisy wymagają jednak uaktualnienia i doprecyzowania co szeroko zostało omówione w protokole z kontroli.

W zakresie Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stwierdzono, że spełnia ona wymogi określone w § 5 ust. 1 – 8 rozporządzenia, nie mniej jednak, tak jak w przypadku polityki bezpieczeństwa kontrolujący mając na uwadze wytyczne GIODO, wskazuje na zbyt ogólne zapisy jak i potrzebę aktualizacji instrukcji.

Zgodnie z zapisami art. 37 cyt. ustawy Dyrektor MOPS ma obowiązek nadania upoważnień osobom, które dopuszczone zostały do przetwarzania danych osobowych. W wyniku weryfikacji przedstawionej kontrolującemu dokumentacji w tym zakresie stwierdzono, że prowadzona jest w jednostce ewidencja osób upoważnionych do przetwarzania danych, która spełnia wymogi określone w art. 39 ust. 1 cyt. ustawy o ochronie danych osobowych. Kontrolujący wniósł jedynie uwagi w odniesieniu do formy prowadzonej ewidencji. Co prawda formy prowadzenia ewidencji nie zostały wprost uregulowane i ujednolicone, ale bezspornym wydaje się, aby ewidencja ta była przede

wszystkim zabezpieczona przed jakimkolwiek uszkodzeniem czy też niepożądanym zagubieniem poszczególnych stron, co z kolei w dużej mierze przyczyni się do wiarygodności danego dokumentu.

Zgodnie z zapisami polityki bezpieczeństwa w jednostce prowadzony jest także rejestr przekazanych informacji na temat rozwiązania lub wygaśnięcia stosunku pracy lub innego zatrudnienia lub stażu, co w opinii kontrolującego jest działaniem, które minimalizuje ryzyko powstania sytuacji, w których następuje ustanie zatrudnienia, a upoważnienie wciąż obowiązuje.

Czynności kontrolne wykazały, że Dyrektor MOPS nie wydawała upoważnień dla osób sprzątających w jednostce, co uznano za działanie jak najbardziej prawidłowe. O wiele lepszym rozwiązaniem, zamiast nadawania uprawnień, w tym przypadku osobie sprzątającej, jest samo zabezpieczanie danych przed dostępem tej osoby (między innymi poprzez stosowanie zasady czystego biurka, zamykania dokumentacji w szafach na klucz, wyłączania komputerów chronionych dostępem poprzez hasła, loginy i inne). Biorąc pod uwagę same upoważnienia kontrolujący nie wniósł uwag. W każdym przypadku upoważnienia były podpisane przez Dyrektora MOPS'u, jak również dane upoważnienie ujęte zostało w ewidencji zgodnie z przyjętymi zasadami w jednostce, a ich kopie były umieszczane w aktach osobowych danego pracownika. Kontrolujący zwrócił jednak uwagę, że w przypadku nadawania identyfikatorów, były one nadawane tylko do pracy przy użyciu oprogramowania merytorycznego, natomiast nie były nadawane identyfikatory do pracy w systemie operacyjnym (identyfikator nie był co prawda wskazany w ewidencji, ale faktycznie logowanie do systemu odbywało się w każdym przypadku, po wcześniejszym wpisaniu identyfikatora oraz hasła). Jednym z istotnych elementów związanych z bezpieczeństwem informacji jest ten związany ze szkoleniem pracowników z tego zakresu. Stwierdzono, że zasady z tym związane zostały uregulowane w polityce bezpieczeństwa i co ważne potwierdzono, że szkolenia w jednostce miały miejsce. Ponadto w jednostce prowadzony jest wykaz osób (wraz z podpisami), które zapoznane zostały z zapisami polityki bezpieczeństwa przetwarzania danych osobowych.

Przeprowadzone czynności kontrolne wykazały, że jednostka posiada oprogramowanie do którego nabyła prawa. Świadczyły o tym dokumenty takie jak licencje, jak również faktury (dowody zakupu oprogramowania). W wyniku analizy poszczególnych zapisów polityki bezpieczeństwa stwierdzono jednak brak zapisów, które regulowałyby obszar związany z licencjami oraz oprogramowaniem wykorzystywanym w jednostce. Jedynie w regulaminie organizacyjnym jednostki do zadań Informatyka przypisano prowadzenie ewidencji oprogramowania i sprzętu, co jak wykazały czynności kontrolne nie było wykonywane. W zakresie stosowania legalnego oprogramowania stwierdzono, że w jednostce wprowadzono „kontrolera domeny", który jest narzędziem pozwalającym między innymi na

minimalizowanie ryzyka związanego z instalowaniem niepożądanego i nielegalnego oprogramowania na stacjach roboczych. Przeprowadzone czynności kontrolne w obecności informatyka MOPS, polegające na próbie zainstalowania oprogramowania z pamięci USB oraz próbie „ściągnięcia" i zainstalowania oprogramowania z sieci Internet wykazały, że w przypadku ujęcia danego sprzętu informatycznego w kontrolerze domeny nie było możliwości zainstalowania oprogramowania (czy to z sieci Internet czy też z dysku zewnętrznego). Za każdym razem do przeprowadzenia instalacji wymagane było podanie hasła administratora. Co prawda możliwym było ściągnięcie pliku z sieci Internet (co jest niepożądane) nie mniej co istotne nie można było dokonać instalacji pliku.

W jednostce wprowadzono odrębną ewidencję komputerów przenośnych, które są wykorzystywane przez pracowników jednostki. W wyniku porównania tej ewidencji z ewidencją księgową stwierdzono jednak, że w jednostce zachodzi nieścisłość pomiędzy zaewidencjonowanym majątkiem w księgach rachunkowych, a ewidencją komputerów dlatego też zasadnym jest, aby przeprowadzić analizę i weryfikację prowadzonej dokumentacji, jak również ważnym jest, aby Informatyk prowadził ewidencję całego sprzętu komputerowego i na bieżąco go monitorował. Powyższe niezbędne jest do starannego i rzetelnego zarządzania zasobami informatycznymi w jednostce.

W zakresie wykonywania kopii bezpieczeństwa w MOPS stwierdzono, że wszelkie czynności z tym związane są rejestrowane w sposób elektroniczny jak i ręczny. Kontrolujący zwrócił jednak uwagę na nieścisłość zapisów zawartych w cyt. instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które polegały na braku wskazania momentu od którego należy liczyć okres przechowywania kopii bezpieczeństwa. Weryfikacja kopii bezpieczeństwa w miejscu ich przechowywania wykazała, że brak było kopii rocznych. Zgodnie z udzielonymi wyjaśnieniami przez Informatyka wynika, że kopie roczne to kopie z miesiąca grudnia danego roku. Nie mniej, na podstawie przeprowadzonej weryfikacji obowiązującej instrukcji zarządzania systemami informatycznymi w MOPS w zakresie sporządzania kopii bezpieczeństwa stwierdzono, że roczna kopia powinna być sporządzona odrębnie za cały rok tj. od 01 stycznia do 31 grudnia danego roku, w sposób niezależny od kopii za miesiąc grudzień, którą podlega przechowywaniu przez okres 3 lat.

Istotnym w zakresie sporządzania kopii bezpieczeństwa, jest również fakt przechowywania ich w odrębnej instytucji, co w sposób pozytywny wpływa na ich bezpieczeństwo w przypadku wystąpienia zjawisk niepożądanych, losowych takich jak np. pożar MOPS, zalanie, inne awarie. Zwrócono jednak uwagę, że w przypadku przenoszenia kopii bezpieczeństwa do odrębnego budynku, dokonywała tego osoba nieupoważniona, tym samym naruszono zapisy § 10 cyt. instrukcji.

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.
Kontrolujący w ramach czynności kontrolnych przeprowadził oględziny w obecności Dyrektora MOPS, 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 w przeważającej liczbie przypadków pomieszczenia spełniały wymogi określone w polityce bezpieczeństwa i instrukcji zarządzania systemami informatycznymi.
W przypadku weryfikacji sposobu zabezpieczenia poszczególnych stacji roboczych, co zostało określone w postanowieniach instrukcji systemem informatycznym służącym do przetwarzania danych osobowych uwag nie wniesiono.

Podsumowując, kontrolujący pozytywnie ocenia zakres poddany szczegółowym czynnościom kontrolnym. Istotnym jest, że na pojęcie bezpieczeństwa informacji składa się szereg poszczególnych czynników, zarówno tych wewnętrznych funkcjonujących w jednostce, jak również zewnętrznych na których bezpośredniego wpływu nie ma kontrolowana jednostka. Jak wykazała analiza dokumentacji oraz czynności polegające na sprawdzeniu ich funkcjonowania w rzeczywistości w jednostce prowadzone są działania, które minimalizują ryzyko wystąpienia niepożądanego przetwarzania danych osobowych czy też ryzyko ich utracenia. Jednostka wprowadziła wymagane przepisami prawa dokumenty regulujące sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Co istotne, jak wykazały czynności kontrolne większość przyjętych w jednostce rozwiązań jest stosowana w praktyce. Jako jeden z elementów, które w znacznej mierze przyczynia się do zabezpieczenia danych osobowych wykorzystywanych przy użyciu systemów informatycznych jest wdrożony „kontroler domeny". Pozwala on na dostosowanie danej stacji roboczej do przyjętych standardów w jednostce przy jednoczesnym ograniczeniu dostępu danego pracownika do wprowadzania zmian w ustawieniach, możliwości instalowania niechcianego oprogramowania itp. Kontrolujący pomimo pozytywnej oceny sprawdzanego zakresu wskazuje jednak na potrzebę zaktualizowania i uszczegółowienia przyjętych dokumentów w szczególności polityki bezpieczeństwa przetwarzania danych osobowych. Zaznaczyć w tym miejscu należy, że wdrażana dokumentacja w tym zakresie powinna być na bieżąco monitorowana z uwagi na zmienność samego bezpieczeństwa w czasie. Nie wystarczające jest jednokrotne opracowanie i wdrożenie procedur z uwagi na chociażby nowe technologie, czy też nowopowstałe zagrożenia, co może przełożyć się na skuteczność i adekwatność przyjętych przez jednostkę rozwiązań. Kontrolujący wskazuje również na potrzebę

faktycznego wdrożenia ewidencji sprzętu, jak i oprogramowania, która również powinna podlegać bieżącemu monitorowaniu i wprowadzaniu zmian. Jest to szczególnie ważne z uwagi, że ciężko jest zarządzać zasobem na temat którego nie mamy wystarczających informacji.

Kołobrzeg, dnia 26.03.2015r.

Kontrolujący

INSPEKTOR
ds. kontroli
Krzysztof Mielnikiewicz
26.03.2015r.

Zapoznałem się
26.03.2015

Sprawdzono pod kątem ustawy o ochronie danych osobowych
01.04.2015

"Dokument nie zawiera treści, których nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie zadań przez Urząd Miasta Kołobrzeg lub jego jednostki organizacyjne".

PEŁNOMOCNIK
DS. OCHRONY INFORMACJI NIEJAWNYCH
Marek Hilbert
3. 04. 15