Zapoznałem się: 05.10.2017 r.

BURMISTRZ GOŁDAPI Tomasz Luto

SPRAWOZDANIE

Temat: **WDRAŻANIE POLITYKI BEZPIECZEŃSTWA INFORMACJI – ROLA PRACOWNIKÓW W PROCESIE OCHRONY DANYCH OSOBOWYCH**

Audytor wewnętrzny: Ewa Kraśniewska

I. INFORMACJA PODSTAWOWE:

1. Temat zadania audytowego: ***Wdrażanie Polityki Bezpieczeństwa Informacji – rola pracowników w procesie ochrony danych osobowych.***
2. Data sporządzenia wstępnych wyników z audytu: 11 września 2017r.
3. Data sporządzenia sprawozdania: 22 września 2017r.
3. Nazwa jednostki, w której przeprowadzany był audyt wewnętrzny:

Urząd Miejski w Gołdapi

4. Termin przeprowadzenia zadania audytowego: 11 września – 22 września 2017r.
5. Cel przeprowadzenia zadania audytowego:

Cel ogólny: *Ocena wdrażania Polityki Bezpieczeństwa Informacji i rola pracowników w procesie ochrony danych osobowych.*

Cele szczegółowe:

1. Zdiagnozowania poziomu świadomości pracowników z zakresu bezpieczeństwa informacji.
2. Analiza zagrożeń związanych z przetwarzaniem danych przez pracowników.

6. Zakres zadania audytowego:

Podmiotowy: Urząd Miejski w Gołdapi

Ankietowano i przeprowadzono wywiady z:

- wybranymi pracownikami jednostki.

Przedmiotowy:

Wybór celowy próby – badaniu ankietowemu poddani zostali pracownicy wszystkich wydziałów. W badaniu w dniu 14 września wzięło udział 26 osób (listy obecności). Ankiety były anonimowe.

II. ANALIZA RYZYKA

Czynności audytowe zgodnie z zakresem przedmiotowym zadania, zostały skierowane na organizację systemu w zakresie następujących ryzyk:

1. nie stosowanie się do wewnętrznych procedur i zewnętrznych uregulowań;
2. brak świadomości zagrożeń;
3. brak świadomości konsekwencji wynikających z naruszeń w zakresie ochrony danych osobowych;
4. brak umiejętności zareagowania w przypadku wystąpienia awarii, czy też podejrzenia ujawnienia danych;

III. PRZEPISY PRAWNE (KRYTERIA), USTALENIA ORAZ REGULACJE WEWNĘTRZNE DOTYCZĄCE BADANEGO OBSZARU

Przepisy prawne:

1. Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12 kwietnia 2012 r. (Dz. U. z 2012 r. poz. 526)
2. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz.U. rok 2016 poz. 922)
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny

odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004r. (Dz. U. z 2004r., nr 100, poz. 1024)

4. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. rok 2015 poz. 745)
5. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. rok 2015 poz. 719)

Regulacje wewnętrzne:
- procedury dotyczące bezpieczeństwa informacji,
- upoważnienia do przetwarzania danych osobowych.

Kryteria oceny
- zgodność działalności z przepisami prawa oraz procedurami wewnętrznymi,
- skuteczność i efektywność działania,
- ochrona zasobów,
- efektywność i skuteczność przepływu informacji,
- zarządzanie ryzykiem,
- poufność,
- dostępność

Kryteria uzgodniono **11 września 2017r.**

IV. SZCZEGÓŁOWE USTALENIA DOKONANE NA PODSTAWIE CZYNNOŚCI AUDYTOWYCH W OBSZARACH WYTYPOWANYCH DO BADANIA WRAZ ZE SKLASYFIKOWANYMI WYNIKAMI ICH OCENY WG KRYTERIÓW

Cele audytu
Zdiagnozowania poziomu świadomości pracowników z zakresu bezpieczeństwa informacji. Analiza zagrożeń związanych z przetwarzaniem danych przez pracowników.
Metodyka (sposób weryfikacji)
Pracownicy Urzędu Miejskiego w Gołdapi wypełnili ankiety przygotowane przez audytującego. Po wypełnieniu ankiet przeprowadzono wywiady z pracownikami z zakresu bezpieczeństwa informacji.
Kryteria (stan oczekiwany)
- zgodność działalności z przepisami prawa oraz procedurami wewnętrznymi, - skuteczność i efektywność działania, - ochrona zasobów, - efektywność i skuteczność przepływu informacji, - zarządzanie ryzykiem, - poufność, - dostępność,
Ustalenia stanu faktycznego
Z przeprowadzonej ankietyzacji w dniu 14 września 2017r. otrzymano następujące wyniki: 1. Czy przetwarza Pan/Pani na swoim stanowisku pracy dane osobowe?

Tak	Nie	Nie wiem	Brak odpowiedzi
17	1	1	x

2. Czy został Pan/Pani upoważniony do przetwarzania danych osobowych na zajmowanym

stanowisku?

Tak	Nie	Nie wiem	Brak odpowiedzi
17	2	7	x

3. Czy został Pan/Pani przeszkolony z zakresu ochrony informacji w **Urzędzie Miejskim w Gołdapi**?

Tak	**Nie**	Nie wiem	**Brak odpowiedzi**
13	**11**	x	**2**

4. Czy zapoznał się Pan/Pani z regulacjami obowiązującymi w jednostce tj. Polityką bezpieczeństwa i Instrukcją Zarządzania System Informatycznym?

Tak	**Nie**	**Nie wiem**	Brak odpowiedzi
13	**9**	**4**	x

5. Kiedy uczestniczył Pan/Pani w szkoleniu z zakresu bezpieczeństwa informacji?

w ostatnim roku (2017)	w ciągu ostatnich dwóch lat	w ciągu ostatnich pięciu lat	nie uczestniczyłem nigdy	**nie pamiętam**
x	3	6	6	**11**

6. Proszę ocenić w jakim stopniu w **Urzędzie Miejskim w Gołdapi** przywiązuje się wagę do znaczenia informacji i jej bezpieczeństwa?

bardzo małym	małym	**średnim**	**dużym**	bardzo dużym	nie mam zdania
1	2	**12**	**6**	3	2

7. Jakiego rodzaju straty Pani/Pana zdaniem może spowodować wyciek (utrata) informacji z **Urzędu Miejskiego w Gołdapi**?

straty finansowe	**brak zaufania klientów**	**utratę reputacji/dobrego wizerunku**	inne
13	**23**	**21**	Pociągnięcie do odpowiedzialności

8. Które z zachowań pracowników **Urzędu Miejskiego w Gołdapi** mogą powodować wyciek danych?

łamanie obowiązujących procedur	nadmierne zaufanie do osób trzecich	nadmierne gadulstwo	zmęczenie i pośpiech	kradzież danych	inne
17	18	16	17	10	x

9. Jakie zabezpieczenia fizyczne są stosowane w **Urzędzie Miejskim w Gołdapi** mające wpływ na poziom bezpieczeństwa informacji?

system alarmowy	klucze do szaf, biurek	monitoring	zasilacze awaryjne	**klucze do pomieszczeń**	inne	żadne z powyższych
13	17	9	3	**26**	hasła do komputerów	x

10. Jakie zabezpieczenia logiczne są stosowane w **Urzędzie Miejskim w Gołdapi** mające wpływ na poziom bezpieczeństwa informacji?

podpis elektroniczny	**hasła i loginy**	archiwizacja danych	programy antywirusowe	firewalle	inne	żadne z powyższych
11	**26**	13	18	2	x	x

11. Jakie zabezpieczenia organizacyjne są stosowane w **Urzędzie Miejskim w Gołdapi** mające wpływ na poziom bezpieczeństwa informacji?

polityki bezpieczeństwa informacji	kontrole przestrzegania zasad polityk bezpieczeństwa	podejmowanie działań naprawczych w przypadku incydentów utraty danych	szkolenia pracowników	inne	żadne z powyższych
16	6	5	12	x	4

12. Kto Pana/Pani zdaniem jest najbardziej prawdopodobnym źródłem incydentów związanych z bezpieczeństwem informacji?

aktualni pracownicy	byli pracownicy	dostawcy usług	klienci	hakerzy	przestępczość zorganizowana
19	13	3	15	10	1

13. Czy stosuje się Pan/Pani do zasad i reguł zawartych w dokumentach: Polityka bezpieczeństwa informacji i Instrukcja zarządzania systemem informatycznym?

Tak	Nie	**Trudno powiedzieć**	Brak odpowiedzi
12	x	**14**	x

14. Jak ocenia Pan/Pani swoją wiedzę na temat metod i technik zapewnienia bezpieczeństwa informacji w **Urzędzie Miejskim w Gołdapi?**

Bardzo dobra	Dobra	Średnia	Znikoma	Zła
1	4	19	2	x

15. Kto Pani/Pana zdaniem jest administratorem danych osobowych w **Urzędzie Miejskim w Gołdapi?**

informatyk	burmistrz	naczelnicy wydziałów	wszyscy pracownicy	sekretarz	brak takiej osoby
11	11	1	5	2	x

16. Która z poniższych odpowiedzi zawiera dane osobowe wrażliwe?

imię, nazwisko, płeć	**stan zdrowia, poglądy polityczne, kod genetyczny**	PESEL, NIP, nr telefonu	wszystkie	brak odpowiedzi
1	**12**	10	3	x

17. Czy pracowników obowiązuje nieograniczony w czasie (nie ustaje z chwilą ustania zatrudnienia lub z upływem okresu obowiązywania umowy cywilnoprawnej) obowiązek zachowania tajemnicy danych osobowych?

Tak	Nie	Nie wiem	Brak odpowiedzi
24	x	2	x

18. Co należy zrobić z wydrukowanymi w nadmiarze bądź zbędnymi dokumentami zawierającymi dane osobowe?

wyrzucić do pojemnika na śmieci	**zniszczyć w niszczarce**	gromadzić w celu archiwizacji	Brak odpowiedzi
x	**26**	x	x

19. Które z poniższych czynności są przetwarzaniem danych osobowych?

gromadzenie*	edytowanie*	**niszczenie***	kopiowanie*	**wszystkie odpowiedzi są poprawne**
8	9	**x**	11	**14**

* z pozostałych 12 odpowiedzi

20. W jaki sposób należy przesyłać dane osobowe w wiadomości e-mail, aby zagwarantować ich bezpieczeństwo?

w załączniku chronionym hasłem, które zostanie wysłane w drugim mailu	**w załączniku chronionym hasłem, które zostanie wysłane SMS-em**	w treści wiadomości, w żadnym wypadku nie w temacie	**w załączniku**	brak odpowiedzi
4	**7**	4	**9**	2

20. Jakich wyjaśnień można udzielić policjantowi podczas rozmowy telefonicznej?

wszelkich, które są dla niego niezbędne	tylko w zakresie związanymi z petentami, pod żadnym pozorem nie ujawnia się informacji o pracownikach	o nieobecności z powodu choroby innego pracownika	**tylko tych, które stanowią informację publiczną**
x	x	x	**26**

21. Co użytkownik powinien zrobić, gdy podejrzewa, że ktoś przejął jego hasło?

wyłączyć komputer i zawiadomić policję	zmienić hasło i zawiadomić policję	**wyłączyć komputer i poinformować osobę nadzorującą bezpieczeństwo informatyczne**	zmienić hasło i poinformować osobę nadzorującą bezpieczeństwo informatyczne	brak odpowiedzi
x	x	**10**	13	3

Podsumowanie ankiet:

Z 26 osób ankietowanych wszystkie przetwarzały dane osobowe, mimo że w ankiecie jedna z osób zaznaczyła, że nie przetwarza danych osobowych i 1 nie wiedziała czy takie dane przetwarza. W większości – 17 osób potwierdziło, że zostały upoważnione do przetwarzania danych osobowych. Z 26 respondentów tylko połowa potwierdziła, że była przeszkolona z zakresu ochrony informacji. Również taka sama ilość osób oświadczyła, że zapoznała się z regulacjami obowiązującymi w jednostce. Aż 11 osób nie pamiętało żeby kiedykolwiek uczestniczyło w szkoleniach z zakresu

bezpieczeństwa informacji, a 6 osób stwierdziło, że nie uczestniczyło w nich nigdy.

Większość ankietowanych przyznała, że w średnim i dużym stopniu (18) przywiązuje się wagę do znaczenia informacji i jej bezpieczeństwa w Urzędzie Miejskim w Gołdapi. Brak zaufania klientów i utrata reputacji/dobrego wizerunku zostały wskazane na pierwszym i drugim miejscu, jako straty na skutek wycieku (utraty) informacji z urzędu. Jako najbardziej ryzykowne zachowania pracowników mogące powodować wyciek danych respondenci wskazali: nadmierne zaufanie do osób trzecich (18), łamanie obowiązujących procedur (17), zmęczenie i pośpiech (17), nadmierne gadulstwo (16), kradzież danych (10).

Jako mające największy wpływ na poziom bezpieczeństwa informacji w Urzędzie Miejskim w Gołdapi wskazano wśród zabezpieczeń fizycznych: klucze do pomieszczeń (26), wśród zabezpieczeń logicznych: hasła i loginy (26), a wśród zabezpieczeń organizacyjnych: polityki bezpieczeństwa informacji (16).

Respondenci uważają za najbardziej prawdopodobne źródła incydentów: aktualnych pracowników (19), klientów (15) i byłych pracowników (13).

Pracownicy w większości nie wiedzieli, czy stosują się do zasad zawartych w wewnętrznych regulacjach (14). Swoją wiedzę ocenili na średnią (19), dobrą (4) , znikomą (2) i bardzo dobrą (1).

Odpowiedzi na pytania sprawdzające wiedzę z zakresu bezpieczeństwa informacji przedstawiały się następująco:

Kto jest administratorem danych osobowych w Urzędzie Miejskim w Gołdapi: burmistrz (11), informatyk (11), wszyscy pracownicy (5), sekretarz (2), naczelnicy (1).

Które z poniższych to dane wrażliwe: stan zdrowia, poglądy polityczne, kod genetyczny (12), PESEL, NIP, nr telefonu (10), wszystkie (3), imię, nazwisko, płeć (1).

Zdecydowana większość osób wiedziała, że pracowników obowiązuje nieograniczony w czasie obowiązek zachowania tajemnicy danych osobowych (24), wszystkie prawidłowo odpowiedziały na pytanie, co należy zrobić z wydrukowanymi w nadmiarze, bądź zbędnymi dokumentami zawierającymi dane osobowe. Na pytanie, które czynności są przetwarzaniem danych osobowych, ankietowani odpowiedzieli: gromadzenie (8), edytowanie (9), niszczenie (0), kopiowanie (11), wszystkie (14). Tylko 7 osób udzieliło poprawnej odpowiedzi na pytanie, w jaki sposób należy prawidłowo przesyłać dane osobowe w wiadomości e-mail, a jedynie 10 osób wiedziało, jak zachować się, gdy istnieje niebezpieczeństwo, że ktoś przejął hasło od komputera. Wszyscy pracownicy odpowiedzieli prawidłowo na pytanie - jakich wyjaśnień można udzielić policjantowi podczas rozmowy telefonicznej.

Podsumowanie wywiadów:

Ponadto pracownicy w rozmowie z audytorem wskazali na następujące problemy:

- brak zabezpieczeń fizycznych np. zamków w części szaf, gdzie znajdują się dokumenty z danymi osobowymi,

- brak zabezpieczeń fizycznych np. zamków w szufladach, gdzie przechowywane są pieczęcie,

- w pokojach, gdzie obsługuje się interesantów znajdują się po dwa stanowiska pracy, co może powodować wyciek danych osobowych,

- pomieszczenie, gdzie znajduje się kasa jest małe, dodatkowo kasjerka odgrodzona jest szybą tłumiącą głos, musi więc mówić głośno, aby klient ją usłyszał, w wyniku tego osoby z kolejki słyszą różne informacje, do których przetwarzania nie są upoważnione np. o zadłużeniu klienta.

Klasyfikacja wyników wg kryteriów

Ocena wystarczająca - audytor zidentyfikował luki czy słabości, jednakże nie mają one istotnego wpływu na poprawności procesu.

Wskazanie słabości kontroli zarządczej

Wyniki ankiety i wywiad wskazały słabe punkty poziomu świadomości pracowników z zakresu bezpieczeństwa informacji, jak również z zakresu fizycznego zabezpieczania danych i są one opisane w powyższym materiale.

Skutki wynikające ze wskazanych słabości kontroli zarządczej

Brak wiedzy niektórych pracowników związanych z ochroną danych osobowych może skutkować w przyszłości nieodpowiednim zabezpieczeniem danych, kradzieżą lub utratą danych, czy też nieświadomym przekazaniem danych osobom nieupoważnionym. Niezabezpieczanie danych osobowych przed utratą (zabezpieczenia fizyczne) i niedostosowanie pomieszczeń do nieuprawnionego przetwarzania danych przez osoby nieupoważnione również może być przyczyną utraty dobrego wizerunku urzędu, obniżonego zaufania klientów, ukarania przez Głównego Inspektora Ochrony Danych Osobowych itd.

Zalecenia

1. Przeprowadzenie szkoleń pracowników z zakresu ochrony danych osobowych oraz ze stosowania wewnętrznych regulacji obowiązujących w Urzędzie Miejskim w Gołdapi.
2. Przegląd zabezpieczeń fizycznych stosowanych w urzędzie. Zamontowanie zamków w szafach, gdzie przechowywane są dane osobowe i w szufladach, gdzie chowa się pieczęcie.
3. Na drzwiach pomieszczeń, gdzie przyjmuje się klientów (w tym również w kasie) umieszczenie napisów, o tym, że może tam przebywać tylko jedna osoba.

V. OPINIA W SPRAWIE ADEKWATNOŚCI, SKUTECZNOŚCI I EFEKTYWNOŚCI BADANYCH ELEMENTÓW SYSTEMU KONTROLI ZARZĄDCZEJ

Badanie audytowe wykazało słabości kontroli zarządczej w obszarach ryzyka objętych zadaniem zapewniającym:

- brak wiedzy z zakresu bezpieczeństwa informacji a tym samym świadomości zagrożeń;

- brak umiejętności w przypadku wystąpienia awarii, czy też podejrzenia ujawnienia danych.

Celem zapewnienia adekwatnej, skutecznej i efektywnej kontroli zarządczej w badanych elementach systemu jest wprowadzenie stosownych zmian w zakresie wskazanym w sformułowanych zaleceniach.

Pouczenie
Zgodnie z § 19 Rozporządzenia Ministra Finansów z dnia 4 września 2015r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (Dz.U. poz.1480) § 17. 1. Audytor wewnętrzny po przeprowadzeniu czynności audytowych uzgadnia pisemnie z audytowanym wstępne wyniki audytu wewnętrznego, w tym w szczególności ustalenia i propozycje zaleceń. 2. W celu uzgodnienia wstępnych wyników audytu wewnętrznego, o których mowa w ust. 1, audytor *wewnętrzny* może przeprowadzić naradę zamykającą. 3. W przypadku nieuzgodnienia wstępnych wyników audytu wewnętrznego, o których mowa w ust. 1, audytowany może zgłosić pisemne zastrzeżenia, w terminie określonym przez audytora wewnętrznego, nie krótszym niż 7 dni kalendarzowych od dnia poinformowania audytowanego o wstępnych wynikach. § 19. 1. Kierownik komórki audytu wewnętrznego przekazuje sprawozdanie audytowanemu i kierownikowi jednostki. 2. Audytowany, w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania, ustala sposób i termin realizacji zaleceń oraz wyznacza osoby odpowiedzialne za realizację zaleceń, powiadamiając o tym na piśmie kierownika komórki audytu wewnętrznego i kierownika jednostki. 3. W przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko kierownikowi jednostki i audytorowi wewnętrznemu. 4. W przypadku, o którym mowa w ust. 3, kierownik jednostki podejmuje decyzję dotyczącą realizacji zaleceń, informując o tym audytowanego i kierownika komórki audytu wewnętrznego. § 20. Audytor wewnętrzny monitoruje realizację zaleceń. § 21. 1. Audytor wewnętrzny po upływie terminów realizacji zaleceń przeprowadza czynności sprawdzające. 2. Wynik czynności sprawdzających audytor wewnętrzny przedstawia w notatce informacyjnej kierownikowi jednostki i audytowanemu.

Sprawozdanie otrzymują:

1) Egz. nr 1 – Burmistrz Gołdapi – wersja papierowa i elektroniczna

Audytor Wewnętrzny
CGAP S.N.3700
Ewa Krasniewska