ZARZĄDZENIE NR 118/2017
BURMISTRZA MIASTA i GMINY DALESZYCE
z dnia 26 września 2017r.

w sprawie wprowadzenia Oceny i analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy w Daleszycach

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U.2016.446 ze zm.), art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz.922 z późn.zm.), § 4 pkt 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) oraz §20 pkt 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (j.t.Dz.U.2016.113) wydanym na podstawie ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (j.t. Dz.U.2014.1114) Burmistrz Miasta i Gminy Daleszyce zarządza co następuje:

§ 1

Wprowadza się do stosowania dokument pn. „Ocena i analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy w Daleszycach" – załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się kierowników wszystkich komórek organizacyjnych Urzędu Miasta i Gminy w Daleszycach do zapoznania pracowników treścią i przestrzegania postanowień zawartych w dokumencie, o których stanowi § 1 niniejszego zarządzenia.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Dariusz Meresiński

Załącznik do ZARZĄDZENIA NR ...../2017
Burmistrza Miasta i Gminy Daleszyce z dnia 26.09.2017 r.

TYTUŁ DOKUMENTU	**Ocena i analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy w Daleszycach**		
WYDAŁ:	***Dariusz Meresiński*** *IMIĘ I NAZWISKO*	*PODPIS*	*26.09.2017* *DATA*
DOKUMENT OBOWIĄZUJE OD DNIA: 26.09.2017			

1. Podstawy prawne opracowanej dokumentacji.

- Art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2016 r., poz.922 z późn.zm.
- § 4 p.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.

2. Ogólne wymogi bezpieczeństwa:

Przetwarzanie danych osobowych w Urzędzie Miasta i Gminy w Daleszycach odbywa się w postaci:

- elektronicznej (np.: pliki na dysku komputera, w pamięci operacyjnej komputera)
- papierowej (wydruki)

Aby zapewnić bezpieczeństwo przetwarzania danych osobowych należy stosować:

- środki ochrony fizycznej stanowiska komputerowego oraz wydruków przed nieuprawnionym dostępem
- środki ochrony technicznej stanowiska komputerowego (np.: hasła dostępu do stacji roboczej, program antywirusowy, zasad zabezpieczeń)

3. Zagrożenia dla systemu informatycznego

Można wyróżnić trzy podstawowe zagrożenia dla systemu informatycznego, przeznaczonego do przetwarzania danych osobowych:

A. utrata poufności (pozyskanie danych przez osoby nieupoważnione)
    - nieuprawniony dostęp do pomieszczenia gdzie znajdują się dane osobowe(wydruki)
    - nieuprawniony dostęp do stacji roboczej (komputera) gdzie znajdują się dane osobowe (np. poprzez ujawnienie hasła dostępu)
    - nieuprawnione skopiowanie danych osobowych na inny nośnik
    - zgubienie nośnika zawierającego dane osobowe
    - niedostateczne zniszczenie wydruku zawierającego dane osobowe
    - klęska żywiołowa powodująca utratę poufności danych
B. utrata integralności (zmiany w systemie informatycznym przeprowadzone przez osoby nieupoważnione)
    - nielegalny dostęp do dokumentów zawierających dane osobowe (w formie papierowej i elektronicznej)
    - błędy ludzkie
    - działania wirusów (brak programów antywirusowych i firewalli)

- awarie oprogramowania komputerów

C. utrata rozliczalności (brak możliwości przypisania danemu podmiotowi konkretnych działań)
   - brak mechanizmu uniemożliwiającego usunięcie logów o pracy danej osoby na komputerze
   - brak kontroli nad kopiowaniem dokumentów z komputera na nośniki zewnętrzne

Do głównych źródeł zagrożeń dla stanowisk komputerowych, na których przetwarzane są dane osobowe zaliczyć możemy:

a. siły wyższe (siły natury) – niezależne od jednostki ludzkiej
   - pożar np.: będący skutkiem uderzenia pioruna)
   - starzenie się sprzętu i awarie
   - powódź
   - katastrofa budowlana
   - wilgoć, kurz

b. działalność człowieka
   - błędy użytkowników (w tym administratorów)
   - zgubienie nośnika informacji
   - niewłaściwe usunięcie danych z nośnika informacji
   - terroryzm
   - utrata prądu
   - szpiegostwo
   - kradzież
   - wandalizm
   - podsłuch
   - ataki socjotechniczne

W/w zagrożenia wynikające z działalności człowieka mogą zostać ograniczone poprzez rygorystyczne przestrzeganie zasad ochrony danych osobowych obowiązujących w Urzędzie Miasta i Gminy w Daleszycach oraz systematyczne szkolenia użytkowników. Skutki zagrożeń wynikających z sił natury można starać się ograniczyć poprzez odpowiednia zabezpieczenie budynku, w którym znajdują się dane osobowe.

4. Analiza zagrożeń i ryzyka

Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie go zlikwidować.

Zagrożenia i ryzyka w zakresie ochrony danych osobowych:

- Niedostateczne kwalifikacje ABI (w tym brak podnoszenia kwalifikacji)
- Brak procedur ochrony danych osobowych

- Niezgodne z wymogami prawnymi, nieaktualne, nieadekwatne do zagrożeń procedury ochrony danych osobowych
- Brak zgłoszenia zbiorów danych osobowych do rejestracji ABI lub GIODO
- Brak lub wady aktualizacji zgłoszenia zbiorów danych osobowych do rejestracji ABI lub GIODO
- Brak lub wady upoważnień do przetwarzania danych osobowych
- Udzielanie upoważnienia do przetwarzania danych osobowych osobom postępującym nieetycznie
- Brak lub wady ewidencji wydanych upoważnień
- Brak lub wady szkoleń z zakresu ochrony danych osobowych
- Wady nadzoru nad przetwarzaniem i ochroną danych osobowych
- Brak lub wady identyfikacji i analizy ryzyka w zakresie przetwarzania i ochrony danych osobowych
- Brak reakcji lub nieprawidłowa reakcja na zagrożenie bezpieczeństwa danych osobowych lub systemów i sieci teleinformatycznych

Ryzyka związane z legalnością przetwarzania danych osobowych	Ryzyka związane z poufnością danych osobowych	Ryzyka związane z integralnością danych osobowych	Ryzyka związane z rozliczalnością danych osobowych w systemie informatycznym
o Zbieranie danych osobowych dla celów niezgodnych z prawem o Niezgodne z prawem pozyskiwanie danych osobowych o Ryzyka związane z bezpieczeństwem danych osobowych o Utrata, uszkodzenie lub zniszczenie danych osobowych o Ujawnienie osobom nieuprawnionym lub stworzenie im warunków do pozyskania danych osobowych (np. poprzez opuszczenie stanowiska pracy z pozostawieniem aktywnej aplikacji umożliwiającej dostęp do zbioru danych osobowych) o Pozostawienie w miejscu niezabezpieczonym zapisanego identyfikatora i/lub hasła dostępu do zbioru danych osobowych o Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do zbioru danych osobowych przez osoby nieupoważnione o Samodzielne instalowanie lub modyfikowanie oprogramowania o Podłączanie nieuprawnionych urządzeń do sieci lokalnej o Odczytywanie danych z nośników informacji bez uprzedniego przeskanowania programem antywirusowym o Przechowywanie akt i dokumentów zawierających dane osobowe w sposób niedostatecznie zabezpieczony przed dostępem osób nieuprawnionych o Pozostawienie akt i dokumentów zawierających dane osobowe bez nadzoru (np. w niezamkniętych pomieszczeniach) o Wyrzucenie akt lub dokumentów zawierających dane osobowe w formie umożliwiającej ich	o Udostępnianie danych osobowych osobom nieupoważnionym o Zdobycie danych osobowych przez osobę nieuprawnioną o Pokonanie zabezpieczeń fizycznych lub programowych o Nieuprawnione kopiowanie danych na nośniki informacji (CD, DVD, pendrive, itp.) o Niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i komputerów przenośnych o Naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych o Podsłuch lub podgląd danych osobowych o Elektromagnetyczna emisja ujawniająca	o Uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych o Celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych o Infekcje wirusowe o Awaria sprzętu o Pożar, zalanie, ekstremalna temperatura, itp. o Zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny)	o Nieprzydzielenie użytkownikom indywidualnych identyfikatorów o Niewłaściwa administracja systemem informatycznym o Niewłaściwa konfiguracja systemu informatycznego o Zniszczenie / zafałszowanie logów systemowych o Podszywanie się pod innego użytkownika

odczytanie o Dopuszczenie do kopiowania dokumentów zawierających dane osobowe przez osoby nieuprawnione o Umożliwienie osobom nieuprawnionym (celowe lub nie) odczytania danych osobowych z ekranu monitora o Sporządzenie kopii danych na nośnikach informacji w sytuacjach nieprzewidzianych procedurami przetwarzania i ochrony danych osobowych o Wady stosowanych technicznych i informatycznych środków bezpieczeństwa			

Wnioski

Na podstawie ww. analizy największym potencjalnym zagrożeniem występującym w Urzędzie Miasta i Gminy w Daleszycach dla bezpieczeństwa danych osobowych wydaje się być:

- nieuprawniony dostęp,
- kradzież (włamanie do systemu),

Innymi zagrożeniami są:

- awaria sprzętu,
- atak wirusa,
- pożar obiektu

W celu zmniejszenia ww. zagrożeń szczególną uwagę należy zwrócić na:

- przetwarzanie danych osobowych tylko przez osoby upoważnione,
- zabezpieczenie obiektu i systemu informatycznego w zakresie ochrony antywłamaniowej oraz przestrzeganie ustalonych zasad w tym zakresie,
- przestrzeganie instrukcji obsługi sprzętu i zasad posługiwania się nim,
- stosowanie nowoczesnych zabezpieczeń antywłamaniowych.

Aby skutecznie wyeliminować ww. zagrożenia należy wprowadzić następujące dodatkowe zabezpieczenia:

- przestrzegać zasad korzystania ze sprzętu informatycznego określonych w PB i IZSI, ze zwróceniem szczególnej uwagi na dostęp osób postronnych,
- przestrzegać rygorystycznie przepisów w zakresie ochrony danych osobowych,
- przestrzegać zasad posługiwania się sprzętem komputerowym i oprogramowaniem (kopiowanie, przesyłanie, udostępnianie, ostrożność podczas obsługi poczty e-mail oraz witryn internetowych),
- stosować procedury (PB i IZSI) korzystania z systemu informatycznego w którym przetwarzane są dane osobowe.