Załącznik nr 1
do Zarządzenia Nr 378/17
Prezydenta Miasta Łomża
z dnia 22 listopada 2017 r.

Zakres zadań Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Łomży

1. Administrator Bezpieczeństwa Informacji wykonuje zadania i obowiązki dotyczące przetwarzania i ochrony danych osobowych określone w ustawie o ochronie danych osobowych i wydanych do niej rozporządzeniach wykonawczych oraz w innych powszechnie obowiązujących aktach prawnych, w tym przepisach sektorowych regulujących działalność w określonych dziedzinach.
2. Administrator Bezpieczeństwa Informacji podlega bezpośrednio Prezydentowi Miasta.
3. Zadaniem Administratora Bezpieczeństwa Informacji jest całościowe sprawdzanie wykonywania w Urzędzie Miejskim w Łomży ochrony danych osobowych i podejmowanie niezbędnych działań w celu zapobieżenia nieprawidłowościom, a w razie, gdy wystąpią - usunięcie ich skutków i eliminowanie przyczyn.
4. Do podstawowych obowiązków Administratora Bezpieczeństwa Informacji należy:
1) Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2) Opracowanie planu i dokonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych dla Administratora Danych.
3) Dokonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych na zlecenie GIODO.
4) Stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem.
5) Identyfikacja i analiza zagrożeń ryzyka, na które może być narażone przetwarzanie danych osobowych.
6) Określenie potrzeb w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych w których przetwarzane są dane, adekwatnych do zagrożeń, ryzyka i możliwości finansowych Urzędu oraz monitorowanie działania wdrożonych zabezpieczeń.
7) Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia bezpieczeństwa danych osobowych i systemów informatycznych.
8) Tworzenie projektów polityki bezpieczeństwa, zarządzeń, instrukcji i wytycznych dotyczących przetwarzania danych osobowych w Urzędzie oraz stałe ich aktualizowanie i kontrola przestrzegania zasad w nich określonych.
9) Współpraca z Administratorem Systemów Informatycznych.
10) Dokonywanie zgłoszeń zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz dokonywanie aktualizacji tych zgłoszeń.
11) Nadawanie pracownikom Urzędu Miejskiego w Łomży upoważnień do przetwarzania danych osobowych w zakresie niezbędnym do wykonywanych przez nich czynności służbowych oraz prowadzenie ewidencji tych pracowników i prowadzenie ewidencji upoważnień.
12) Prowadzenie stałych działań edukacyjnych w celu podnoszenia świadomości pracowników Urzędu w zakresie prawa do prywatności i ochrony danych osobowych oraz zapoznanie upoważnionych do przetwarzania danych osobowych pracowników z przepisami o ochronie danych osobowych, regulacjami wewnętrznymi i zasadami bezpiecznych zachowań użytkowników w środowisku IT.
13) Prowadzenie rejestru zbiorów danych osobowych przetwarzanych w Urzędzie, zgodnie z obowiązującymi przepisami prawa.
14) Sprawowanie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
15) Nadzór nad zabezpieczeniem pomieszczeń w których przetwarzane są dane osobowe.

16) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisywane są dane osobowe.
17) Nadzór nad prawidłowością archiwizacji, usuwania danych osobowych i wykonywaniem kopii awaryjnych.

5. Administrator Bezpieczeństwa Informacji wykonując swoje czynności realizuje zadania w imieniu Administratora Danych Osobowych i posiada uprawnienia oraz upoważnienia do:

a) kontrolowania realizacji umów dotyczących udostępniania lub powierzania danych do przetwarzania osobom lub podmiotom zewnętrznym w zakresie stosowania zapisów bezpieczeństwa przetwarzania i ochrony danych osobowych,
b) decydowania o pozbawieniu lub ograniczeniu zakresu przetwarzania danych osobowych i uprawnień nadanych w systemach informatycznych dla użytkowników, którzy powodują zagrożenie bezpieczeństwa i ochrony danych osobowych,
c) udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie prowadzonych sprawdzeń (kontroli lub audytów) i dostosowania ochrony danych do stanu zgodnego z przepisami,
d) zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących okoliczności powstania zagrożeń dla bezpieczeństwa i ochrony danych osobowych,
e) kontrolowania pracowników Urzędu w zakresie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych poprzez prowadzone sprawdzenia (kontrole lub audyty).