BURMISTRZ
MIASTA LUBAWKA
woj. dolnośląskie

Zarządzenie Nr 84/2018
Burmistrza Miasta Lubawka
z dnia 24 maja 2018 roku.

w sprawie: powołania Inspektora Ochrony Danych i Administratora Systemu Informatycznego w Urzędzie Miasta Lubawka

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2015r. poz. 1515 ze zmianami), oraz art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

z a r z ą d z a m co następuje:

§ 1

1. Wyznaczam Pana Pawła Mazura na Inspektora ochrony danych osobowych IOD w Urzędzie Miasta Lubawka. Zakres działania IOD stanowi załącznik Nr 1 do niniejszego zarządzenia.
2. Wyznaczam Pana Pawła Miechura na Administratora Systemów Informatycznych (ASI) w Urzędzie Miasta Lubawka. Zakres działania ASI stanowi załącznik Nr 2 do niniejszego zarządzenia.

§ 2

Traci moc Zarządzenie Nr 220/2015 Burmistrza Miasta Lubawka z dnia 18 listopada 2015 roku w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Miasta Lubawka.

§ 3

Zarządzenie wchodzi w życie z dniem 25 maja 2018r.

BURMISTRZ
Ewa Kocemba

Załącznik nr 1
do Zarządzenia Nr 84/2018
Burmistrza Miasta Lubawka
z dnia 24 maja 2018r.

Zakres działania Inspektora Ochrony Danych (IOD)

1) Informowanie Administratorów oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych osobowych i doradzanie im w tej sprawie.
2) Monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii i państw członkowskich o ochronie danych oraz Polityki Bezpieczeństwa i Instrukcji przetwarzania danych osobowych, w tym podział obowiązków.
3) Prowadzenie działań zwiększających świadomość, szkolenie personelu uczestniczącego w operacjach przetwarzania.
4) Prowadzenie audytów sprawdzających stan przestrzegania zasad ochrony danych osobowych przez personel przetwarzający dane osobowe.
5) Udzielanie Administratorom zaleceń, co do oceny skutków ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia.
6) Współpraca z organem nadzorczym.
7) Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia, oraz w stosownych przypadkach prowadzenia konsultacji we wszelkich innych sprawach.
8) Nadzór na przetwarzaniem danych zgodnie z rozporządzeniem i innymi przepisami prawa.
9) Prowadzenie rejestrów czynności przetwarzania danych osobowych Administratorów.
10) Udostępnianie rejestrów czynności przetwarzania danych osobowych do wglądu, każdemu zainteresowanemu, w siedzibie ADO.
11) Opracowanie Planów sprawdzeń określających przedmiot poszczególnych sprawdzeń, zakres czynności, które będą podjęte w toku sprawdzenie oraz termin przeprowadzenia sprawdzenia.
12) Przedstawienie ADO planu sprawdzeń nie później niż na miesiąc przed rozpoczęciem okresu objętego planem, który to okres nie może być krótszy niż kwartał i dłuższy niż rok. Plan sprawdzeń obejmuje, co najmniej jedno sprawdzenie.
13) Przeprowadzenie sprawdzenia pozaplanowego niezwłocznie po powzięciu przez IOD, informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia. Powiadomienia ADO o rozpoczęciu sprawdzenia pozaplanowego jeszcze przed podjęciem pierwszych czynności.
14) Przekazanie ADO sprawozdania:
    a. ze sprawdzenia planowego – w terminie określonym w planie sprawdzeń, nie później niż 30 dni od zakończenia sprawdzenia.
    b. ze sprawdzenia pozaplanowego – niezwłocznie po zakończeniu sprawdzenia.

c. ze sprawdzenia, o które zwrócił się UODO – w terminie umożliwiającym zachowanie przez ADO terminu wskazanego przez UODO.

15) Przechowywanie sprawozdania oraz dokumentów z nim związanych przez okres, co najmniej pięciu lat od dnia ich sporządzenia.
16) Zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
17) Nadzór na opracowaniem i aktualizacją dokumentacji przetwarzania danych.
18) W przypadku wykrycia podczas weryfikacji nieprawidłowości, IOD:
    a. zawiadamia ADO o nieopracowaniu lub braku dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia do wymaganego stanu, w tym przedstawienia wdrożonych dokumentów usuwających stan niezgodności.
    b. zawiadamia ADO o nieaktualności dokumentacji przetwarzania danych osobowych oraz przedstawia do wdrożenia dokumenty aktualizujące.
    c. poucza lub instruuje osoby nieprzestrzegające zasad określonych w dokumentacji przetwarzania danych osobowych o prawidłowym sposobie ich realizacji lub zawiadamia ADO, wskazując osoby odpowiedzialne za naruszenie tych zasad oraz jego zakres.
19) Przeprowadzeniu, co najmniej raz w roku, z pomocą ASI analizy ryzyka dla poszczególnych Administratorów.
20) Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.
21) Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób.
22) Nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych.
23) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe.
24) Nadzór nad zarządzaniem hasłami użytkowników i przestrzeganiem procedur określających ich zmiany.
25) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych.
26) Nadzór nad wykonywaniem kopii awaryjnych.
27) Nadzór nad systemem komunikacji w sieci komputerowej.
28) Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
29) Kontrola nad danymi osobowymi wprowadzonymi do zbiorów (przez kogo zostały wprowadzone, komu są przekazywane).
30) Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.

Inspektor Ochrony Danych uprawniony jest do:

1) wydawania poleceń wszystkim pracownikom Urzędu Miasta Lubawka w zakresie związanym z wdrożeniem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwa Informacji,

2) rozstrzygania sporów dotyczących stosowania i interpretacji wymagań zawartych w dokumentacji Systemy Zarządzania Bezpieczeństwem Informacji oraz wydawania wiążących decyzji w tym zakresie,
3) dostępu do wszystkich dokumentów występujących w Urzędzie Miasta Lubawka, których treść może być istotna z punktu widzenia funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji,
4) uzyskania wyjaśnień od pracowników w zakresie realizowanych działań w ramach Systemu Zarządzania Bezpieczeństwem Informacji,
5) Podejmowania decyzji w kwestiach bezpieczeństwa informacji, w zakresie nierodzącym zobowiązań finansowych, w szczególności w zakresie współpracy Urzędu Miasta Lubawka z zewnętrznymi jednostkami organizacyjnymi.

BURMISTRZ
Ewa Kocemba

Załącznik nr 2
do Zarządzenia Nr 84/2018
Burmistrza Miasta Lubawka
z dnia 24 maja 2018r.

Zakres działania Administratora Systemu Informatycznego (ASI)

Administrator Systemu Informatycznego, w zakresie zadań wykonywanych dla zapewnienia systemom bezpieczeństwa, zgodnego z celami i metodą wdrożonej polityki bezpieczeństwa informacji, współpracuje bezpośrednio z Administratorem Bezpieczeństwa Informacji (ABI).

Do zadań Administratora Systemu Informatycznego należy:

1) formułowanie, w uzgodnieniu z administratorem danych i/lub osobami, do których administrator delegował zarządzanie uprawnieniami oraz ABI, sposobu określania uprawnień w systemach informatycznych,
2) realizacja decyzji Administratora Danych Osobowych (/innych) odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT Urzędu, tj.:

a) tworzenie kont użytkowników w systemach informatycznych,
b) przypisywanie do kont startowych haseł uwierzytelniających użytkowników tych kont,
c) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,
d) resetowanie utraconych haseł,
e) usuwanie kont i uprawnień dla kont osób, które zakończyły pracę w Urzędzie,
f) dostarczanie ABI informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowo-programowych,
g) zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych,
h) naprawy, konserwacja oraz likwidacja urządzeń komputerowych, na których zapisywane są dane osobowe,
i) zarządzanie hasłami użytkowników i przestrzeganiem procedur określających ich zmiany,
j) sprawdzanie systemu pod kątem obecności wirusów komputerowych,
k) wykonywanie kopii awaryjnych,
l) sprawdzanie systemów komunikacji w sieci komputerowej;

3) planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Urzędzie Miasta,
4) planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych,
5) automatyzacja zadań konserwacyjnych w systemie – w tym wykonywania kopii zapasowych oprogramowania i danych,
6) monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników,
7) monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych,

8) zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych,
9) systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego,
10) zapewnienie eksploatowanym systemom opieki serwisowej producenta – zapewnienie umów regulujących formy tej opieki,
11) rozwiązywanie, samodzielnie i we współpracy z pozostałym personelem IT, problemów towarzyszących eksploatacji systemów informatycznych,
12) przygotowywanie, we współpracy a ABI instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodą wdrożonej polityki bezpieczeństwa informacji,
13) prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT

BURMISTRZ
Ewa Kocemba