

Zarządzenie Nr 34/2014
Dyrektora Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu
z dnia 22 maja 2014 roku

w sprawie zmiany Administratora Bezpieczeństwa Informacji (ABI)
w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku, Nr 101, poz. 926 - tekst jednolity z późniejszymi zmianami), § 8 ust. 3 Statutu Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu oraz § 6 ust. 2 pkt. c Regulaminu Organizacyjnego Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu,

zarządzam:

§ 1

Odwołuję z funkcji Administratora Bezpieczeństwa Informacji w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu Panią Violetę Urbaś – Kierownika zespołu w Miejskim Ośrodku Gimnastyki Korekcyjnej.

§ 2

1. Powołuję na Administratora Bezpieczeństwa Informacji w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu Panią Gabrielę Kardas – Głównego specjalistę ds. organizacji imprez w Dziale Komunikacji i Imprez.
2. Zakres zadań i uprawnienia Administratora Bezpieczeństwa Informacji stanowi załącznik do niniejszego zarządzenia.

§ 3

Administrator Bezpieczeństwa Informacji podlega bezpośrednio Dyrektorowi Miejskiego Ośrodka Sportu i Rekreacji w Sosnowcu.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

D Y R E K T O R

R A F A Ł Ł Y D E K

Zakres zadań i uprawnienia Administratora Bezpieczeństwa Informacji w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu

- I. Administrator Bezpieczeństwa Informacji - zwany dalej ABI wykonuje zadania w zakresie niniejszego zarządzenia.
- II. Celem działania ABI jest nadzorowanie i kontrolowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w Miejskim Ośrodku Sportu i Rekreacji w Sosnowcu.
- III. Zadaniem ABI jest realizacja przedsięwzięć określonych art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 roku, Nr 101, poz 926 – tekst jednolity z późniejszymi zmianami), a w szczególności nadzorowanie i kontrolowanie:
 - 1) stosowania środków technicznych i przedsięwzięć organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednich do zagrożeń oraz kategorii danych,
 - 2) zabezpieczenia danych osobowych przed udostępnieniem osobom nieupoważnionym lub zabranieniem przez osobę nieuprawnioną, utratą, zmianą, uszkodzeniem lub zniszczeniem,
 - 3) przetwarzania danych osobowych zgodnie z przepisami w/w ustawy.
- IV. Do szczegółowych czynności ABI zaliczyć można:
 1. Nadzorowanie i kontrolowanie przestrzegania zasad:
 - a) przetwarzania danych osobowych przez użytkowników zgodnie z zakresem nadanego im upoważnienia,
 - b) prowadzenia dokumentacji przetwarzania danych osobowych,
 - c) stosowania przez użytkowników zasad przetwarzania danych osobowych, a w szczególności ich zbierania, utrwalania, opracowywania, zmieniania, udostępniania i ich usuwania,
 - d) ochrony obszarów przetwarzania danych w zakresie adekwatności stosowanych zabezpieczeń i możliwości wystąpienia w nich zagrożeń,
 - e) wyposażenia oraz zabezpieczenia pomieszczeń, w których przechowuje się dane sensytywne i kopie zapasowe zbiorów,
 - f) rejestracji zbiorów w Biurze Generalnego Inspektora Ochrony Danych Osobowych (GIODO) lub zmian przetwarzania danych osobowych.
 2. Realizowanie zadań w zakresie:
 - a) rozpatrywania skarg i wniosków dotyczących przetwarzania i ochrony danych,
 - b) tworzenia projektów zarządzeń, instrukcji i wytycznych Administratora Danych Osobowych,
 - c) przygotowywania informacji w zakresie rejestracji zbiorów w GIODO lub zmian w przetwarzaniu danych,
 - d) wyjaśniania i dokumentowania przypadków naruszania zasad przetwarzania i ochrony danych osobowych,
 - e) organizowania szkoleń z zakresu przetwarzania i ochrony danych osobowych,
 - f) odnotowywania i dokumentowania zmian w lokalizacjach obszarów przetwarzania danych,
 - g) wykonywania okresowych analiz zagrożeń bezpieczeństwa i ocen stanu ochrony danych osobowych przetwarzanych w obszarach.
- V. Wykonując swoje czynności ABI działa w imieniu Administratora Danych Osobowych i posiada uprawnienia do:
 - 1) wskazywania zastosowania odpowiednich zabezpieczeń technicznych i wykonywania czynności organizacyjnych mających na celu zapewnienie skutecznej ochrony danych,

- 2) parafowania umów dotyczących udostępniania lub powierzania danych do przetwarzania osobom lub podmiotom zewnętrznym w zakresie stosowania w nich zapisów bezpieczeństwa przetwarzania i ochrony danych osobowych,
- 3) wnioskowania o ograniczenie zakresu przetwarzania danych osobowych użytkownikom, którzy powodują zagrożenia bezpieczeństwa i ochrony danych osobowych,
- 4) udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie kontroli i dostosowania ochrony danych do stanu zgodnego z przepisami prawa,
- 5) zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących spowodowania zagrożenia bezpieczeństwa danych.

D Y R E K T O R

RAFAŁ ŁYDEK