

ZARZĄDZENIE NR 8/2022
Dyrektora
Zakładu Gospodarki Komunalnej

z dnia 30 grudnia 2022 r.

**w sprawie powołania Administratora Systemu Informatycznego
oraz wprowadzenia Polityki Bezpieczeństwa Danych Osobowych**

Na podstawie:

- art. 37 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady/UE/2016/679 z dn. 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/Dz. Urz. UE.L nr 119, str.1.
- Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

§ 1

Powołuje pana Juliusza Grudnickiego do pełnienia funkcji Administratora Systemu Informatycznego (ASI) w Zakładzie Gospodarki Komunalnej w Karlinie na okres od 01 stycznia 2023 do 31 grudnia 2023r.

1. Zakres czynności ASI stanowi załącznik numer 1 do zarządzenia.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Zakład Gospodarki Komunalnej
w Karlinie
Marek Lewandowski

Zakres zadań i uprawnień dla Administratora Systemu Informatycznego w Zakładzie Gospodarki Komunalnej w Karlinie:

1. Przeprowadzanie instruktaży i konsultacji w zakresie obsługi komputerów i oprogramowania zainstalowanych na stanowiskach pracy.
2. Zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do systemu informatycznego wprowadzone oraz komu z systemu są przekazywane.
3. Współpraca z IOD przy przygotowaniu i wdrażaniu dokumentacji ochrony danych osobowych.
4. Systematyczne kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
5. Zabezpieczenie zbiorów danych oraz programów służących do przetwarzania danych osobowych poprzez systematyczne wykonywanie kopii zapasowych.
6. Prowadzenie ewidencji sprzętu teleinformatycznego oraz oprogramowania.
7. Nadzór nad naprawą oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe.
8. Kontrola przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych osobowych.
9. Zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego.
10. Nadzór nad stosowaniem mechanizmów kontroli dostępu do danych osobowych.
11. Utrzymywanie, konfigurowanie i monitorowanie wydajności systemów informatycznych.
12. Kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych.
13. Informowanie na bieżąco ADO i IOD o przypadkach awarii programów wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem oraz nie właściwego wykorzystywania sprzętu komputerowego.