Załącznik nr 1 do uchwały nr 37/2017
Zarządu Górnośląsko - Zagłębiowskiej Metropolii
z dnia 18 grudnia 2017 r.

1. *Załącznik nr 1 do Regulaminu Organizacyjnego Urzędu Metropolitalnego Górnośląsko – Zagłębiowskiej Metropolii otrzymuje brzmienie załącznika nr 1 do niniejszego załącznika.*

2. *Załącznik nr 2 do Regulaminu Organizacyjnego Urzędu Metropolitalnego Górnośląsko – Zagłębiowskiej Metropolii otrzymuje brzmienie załącznika nr 2 do niniejszego załącznika.*

3. ***§23 Regulaminu Organizacyjnego Urzędu Metropolitalnego Górnośląsko – Zagłębiowskiej Metropolii otrzymuje brzmienie:***

§ 23.
DEPARTAMENT ORGANIZACJI I ZARZĄDZANIA (OR)

Do zakresu działania **Departamentu Organizacji i Zarządzania** należy stworzenie odpowiednich warunków osobowych, organizacyjnych i informatycznych umożliwiających sprawne funkcjonowanie Urzędu, w szczególności:

1) Prowadzenie spraw kadrowych i płacowych oraz emerytalno-rentowych pracowników Urzędu.
2) Planowanie i realizacja planu finansowego Departamentu.
3) Rozliczanie miesięczne i roczne podatku dochodowego od osób fizycznych.
4) Naliczanie i odprowadzanie składek na ubezpieczenia społeczne, zdrowotne, Fundusz Pracy i PFRON.
5) Realizacja zadań związanych z naborami na wolne stanowiska urzędnicze, realizacja służby przygotowawczej dla nowoprzyjętych pracowników oraz realizacja oceny okresowej pracowników Urzędu.
6) Koordynacja działań informatycznych w Urzędzie.
7) Koordynowanie spraw związanych z wystąpieniami podmiotów prowadzących zawodową działalność lobbingową.
8) Koordynowanie spraw z zakresu załatwiania skarg, wniosków oraz petycji.
9) Prowadzenie spraw związanych z udzielaniem Upoważnień Przewodniczącego Zarządu oraz Pełnomocnictw Zarządu.
10) Prowadzenie rejestru wniosków o udzielenie informacji publicznej oraz rejestru Zarządzeń Przewodniczącego Zarządu,
11) Koordynowanie kontroli zarządczej w Urzędzie.
12) Zapewnienie właściwego obiegu korespondencji w Urzędzie.
13) Obsługa biura podawczego w Urzędzie.
14) Zarządzanie i administrowanie Biuletynem Informacji Publicznej.
15) Współpraca z organami zewnętrznymi przeprowadzającymi kontrole w Urzędzie.
16) Prowadzenie polityki szkoleniowej dla pracowników Urzędu.

Administrator Bezpieczeństwa Informacji

1) Zapewnianie przestrzegania przepisów o ochronie danych osobowych poprzez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2016 r. poz. 922) /zwanej dalej „ustawą o ochronie danych osobowych”/ oraz przestrzegania zasad w niej określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2) Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy o ochronie danych osobowych, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7 ustawy o ochronie danych osobowych.
3) Zapewnienie, aby do danych osobowych miały dostęp wyłącznie osoby upoważnione w zakresie wykonywanych zadań.
4) Nadzorowanie fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe oraz kontroli przebywających w nich osób.
5) Nadzorowanie przestrzegania zasad określonych w Polityce Bezpieczeństwa Informacji i w innych dokumentach dotyczących ochrony bezpieczeństwa danych osobowych.
6) Nadzorowanie zasad i procedur wymiany danych w sieci.
7) Nadzorowanie obiegu dokumentów zawierających dane osobowe.
8) Nadzorowanie funkcjonowania zasad i procedur związanych z uwierzytelnianiem użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych.
9) Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych.
10) Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych, jeśli takie wystąpiło. Przygotowanie oraz przedstawienie Administratorowi Danych Osobowych odpowiednich zmian do Polityki Bezpieczeństwa Informacji oraz do innych dokumentów dotyczących ochrony bezpieczeństwa danych osobowych.
11) Zlecanie modyfikacji uprawnień w systemach informatycznych w przypadku odebrania lub zmiany upoważnienia do przetwarzania danych osobowych.
12) Szkolenie osób dopuszczonych do przetwarzania danych osobowych z zakresu przepisów prawa oraz uregulowań wewnętrznych w zakresie bezpieczeństwa danych osobowych.
13) Nadzorowanie podpisania umów o zachowaniu poufności przetwarzania danych osobowych z użytkownikami upoważnionymi do przetwarzania danych osobowych, firmami, w tym firmami, którym powierzono przetwarzanie danych osobowych lub konserwacje urządzeń służących do przetwarzania danych oraz pracownikami tych firm.