ZARZĄDZENIE NR 9
DYREKTORA GENERALNEGO
MAZOWIECKIEGO URZĘDU WOJEWÓDZKIEGO W WARSZAWIE
z dnia 26 lutego 2019 r.

w sprawie ustalenia regulaminu organizacyjnego Biura Ochrony w Mazowieckim Urzędzie Wojewódzkim w Warszawie

Na podstawie art. 25 ust. 4 pkt 1 lit. d oraz ust. 10 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2018 r. poz. 1559) zarządza się, co następuje:

§ 1. Ustala się regulamin organizacyjny Biura Ochrony w Mazowieckim Urzędzie Wojewódzkim w Warszawie, określający zadania i strukturę wewnętrznych komórek organizacyjnych oraz ich podległość, stanowiący załącznik do zarządzenia.

§ 2. Nadzór nad wykonaniem zarządzenia powierza się Dyrektorowi Biura Ochrony w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

§ 3. Traci moc zarządzenie nr 28 Dyrektora Generalnego Mazowieckiego Urzędu Wojewódzkiego w Warszawie z dnia 11 lipca 2018 r. w sprawie ustalenia regulaminu organizacyjnego Biura Ochrony w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR GENERALNY
MAZOWIECKIEGO URZĘDU WOJEWÓDZKIEGO
W WARSZAWIE
JAROSŁAW SZAJNER

Załącznik do zarządzenia nr 9
Dyrektora Generalnego
Mazowieckiego Urzędu Wojewódzkiego
w Warszawie z dnia 26 lutego 2019 r.

REGULAMIN ORGANIZACYJNY BIURA OCHRONY W MAZOWIECKIM URZĘDZIE WOJEWÓDZKIM W WARSZAWIE

Rozdział 1
Słownik pojęć

§ 1. Ilekroć w regulaminie jest mowa o:

1) Wojewodzie - należy przez to rozumieć Wojewodę Mazowieckiego;
2) Urzędzie - należy przez to rozumieć Mazowiecki Urząd Wojewódzki w Warszawie;
3) Dyrektorze Generalnym - należy przez to rozumieć Dyrektora Generalnego Urzędu;
4) biurze - należy przez to rozumieć Biuro Ochrony w Urzędzie;
5) dyrektorze - należy przez to rozumieć Dyrektora Biura Ochrony;
6) Inspektorze – należy przez to rozumieć Inspektora Ochrony Danych;
7) regulaminie organizacyjnym – należy przez to rozumieć Regulamin Organizacyjny Mazowieckiego Urzędu Wojewódzkiego w Warszawie.

Rozdział 2
Struktura biura

§ 2. 1. W skład biura wchodzą następujące komórki organizacyjne posługujące się przy znakowaniu prowadzonych spraw i akt symbolami:

1) Oddział do spraw Ochrony Informacji Niejawnych - **BO-I**;
2) Kancelaria Tajna - **BO-II**.

2. W strukturze biura funkcjonuje, podlegający bezpośrednio Wojewodzie, Inspektor, któremu biuro zapewnia obsługę organizacyjno-administracyjną, który posługuje się przy znakowaniu spraw i akt symbolem - **IOD**
3. W strukturze biura funkcjonuje, podlegający bezpośrednio Wojewodzie, Pełnomocnik do spraw Ochrony Informacji Niejawnych, któremu biuro zapewnia obsługę organizacyjno-administracyjną.

Rozdział 3
Kierowanie biurem

§ 3. 1**.** Biurem kieruje dyrektor.

2. Podczas nieobecności dyrektora jego obowiązki wykonuje wyznaczony przez dyrektora pracownik na podstawie stosownego upoważnienia.
3. Podczas nieobecności Pełnomocnika do spraw Ochrony Informacji Niejawnych jego obowiązki, w zakresie zadań wynikających z przepisów o ochronie informacji niejawnych, wykonuje Zastępca Pełnomocnika do spraw Ochrony Informacji Niejawnych.
4. Kancelarią Tajną kieruje wyznaczony przez Wojewodę pracownik pełniący funkcję Kierownika Kancelarii Tajnej, który w zakresie realizacji zadań określonych w § 7 regulaminu podlega bezpośrednio Pełnomocnikowi do spraw Ochrony Informacji Niejawnych.

§ 4. 1. Oddziałem do spraw Ochrony Informacji Niejawnych kieruje kierownik.

2. Podczas nieobecności kierownika jego obowiązki wykonuje wskazany przez dyrektora pracownik oddziału na podstawie stosownego upoważnienia.
3. Skargi na kierownika oddziału rozpatruje dyrektor.

Rozdział 4
Zadania wspólne

§ 5. Do zadań wspólnych Oddziału do spraw Ochrony Informacji Niejawnych oraz Kancelarii Tajnej należy, w szczególności:

1) realizacja zadań, określonych w § 13 regulaminu organizacyjnego, zgodnie z zakresem działania;
2) monitorowanie zmian w przepisach prawa;
3) terminowe załatwianie skarg, wniosków i petycji związanych z zakresem działania biura;
4) zapewnienie sprawnego obiegu korespondencji przychodzącej i wychodzącej.

Rozdział 5
Zakresy działania

§ 6. 1. Do zakresu działania **Oddziału do spraw Ochrony Informacji Niejawnych** należy realizacja zadań Pełnomocnika do spraw Ochrony Informacji Niejawnych określonych w § 31 ust. 3:

1) pkt 4 regulaminu organizacyjnego;
2) pkt 1 regulaminu organizacyjnego, w szczególności przez:
   a) zapewnienie stosowania odpowiednich środków bezpieczeństwa fizycznego informacji niejawnych,
   b) nadzór nad prawidłowym wytwarzaniem, przetwarzaniem, przechowywaniem i przekazywaniem informacji niejawnych,
   c) opracowywanie i aktualizowanie wymaganej przepisami o ochronie informacji niejawnych dokumentacji bezpieczeństwa informacji niejawnych, w szczególności:
      - dokumentacji dotyczącej sposobu i trybu przetwarzania informacji niejawnych,
      - planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego i nadzorowanie jego realizacji,
      - dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą,
   d) opracowywanie i aktualizację materiałów szkoleniowych oraz prowadzenie szkoleń w zakresie ochrony informacji niejawnych i wydawanie zaświadczeń o ich odbyciu,
   e) prowadzenie postępowań wyjaśniających okoliczności naruszenia przepisów o ochronie informacji niejawnych;
3) pkt 2 i 3 regulaminu organizacyjnego, w szczególności przez:
   a) realizację zadań inspektora bezpieczeństwa teleinformatycznego oraz administratora systemu w stosunku do funkcjonującego w biurze Bezpiecznego Stanowiska Komputerowego II,
   b) nadzór nad fizycznym zabezpieczeniem pomieszczenia, w którym znajduje się Bezpieczne Stanowisko Komputerowe II,
   c) sporządzanie oraz nadzór nad przestrzeganiem procedury wydawania upoważnień osobom dopuszczonym do obsługi Bezpiecznego Stanowiska Komputerowego II i urządzeń wchodzących w jego skład oraz nadzór nad przetwarzaniem dokumentów na Bezpiecznym Stanowisku Komputerowym II,

d) prowadzenie szkoleń pracowników z zakresu bezpieczeństwa teleinformatycznego systemów i sieci teleinformatycznych Urzędu, w których przetwarzane są informacje niejawne lub dane osobowe,

e) okresową kontrolę zgodności funkcjonowania systemów i sieci teleinformatycznych Urzędu, w których przetwarzane są informacje ustawowo chronione, z przyjętymi zasadami i procedurami bezpieczeństwa;

f) opracowywanie wymaganej przepisami o ochronie informacji niejawnych dokumentacji dotyczącej systemu bezpieczeństwa teleinformatycznego w tym szacowanie i zarządzanie ryzykiem;

4) pkt 5 regulaminu organizacyjnego przeprowadzanie, co najmniej raz na 3 lata, okresowej kontroli ewidencji materiałów i obiegu dokumentów niejawnych w Urzędzie;

5) pkt 6 i 7 regulaminu organizacyjnego w szczególności przez:

a) wydawanie upoważnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone”,

b) prowadzenie zwykłych postępowań sprawdzających i kontrolnych postępowań sprawdzających oraz przechowywanie akt zakończonych postępowań sprawdzających,

c) prowadzenie aktualnego wykazu osób zatrudnionych albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto,

d) współpracę z Agencją Bezpieczeństwa Wewnętrznego i Służbą Kontrwywiadu Wojskowego w zakresie postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego oraz przekazywania i wymiany danych do prowadzonych baz danych i ewidencji;

6) pkt 9 regulaminu organizacyjnego, w szczególności przez:

a) współpracę z Inspektorem w opracowywaniu i aktualizacji dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych w Urzędzie,

b) wydawanie upoważnień do przetwarzania danych osobowych,

c) realizowanie procedur związanych z nadawaniem i usuwaniem uprawnień pracowników do Systemu Rejestrów Państwowych (rejestr PESEL i Rejestr Stanu Cywilnego),

d) współudział w szkoleniu pracowników Urzędu w zakresie ochrony danych osobowych,

e) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie,

f) udział w prowadzonych przez Inspektora kontrolach w zakresie przestrzegania przepisów o ochronie danych osobowych,

g) współpracę z Biurem Informatyki w Urzędzie w zakresie realizacji zadań związanych z ochroną danych osobowych w systemach i sieciach teleinformatycznych;

7) pkt 10 regulaminu organizacyjnego, w szczególności przez:

a) przyjmowanie, ewidencjonowanie, przechowywanie i analizę dokumentacji oświadczeń o stanie majątkowym składanych Wojewodzie i Dyrektorowi Generalnemu przez zobowiązane osoby pełniące funkcje publiczne,

b) prowadzenie i aktualizowanie ewidencji oświadczeń o stanie majątkowym oraz monitorowanie składania oświadczeń o stanie majątkowym i zmian personalnych na stanowiskach, których zajmowanie wiąże się z obowiązkiem złożenia oświadczenia o stanie majątkowym Wojewodzie lub Dyrektorowi Generalnemu,

c) przyjmowanie, ewidencjonowanie i przechowywanie dokumentacji oświadczeń o stanie majątkowym składanych Wojewodzie przez zobowiązanych przedstawicieli administracji samorządowej,

d) dokonywanie analizy danych zawartych w oświadczeniach o stanie majątkowym, w tym opracowywanie wniosków do Centralnego Biura Antykorupcyjnego w Warszawie,

e) przygotowywanie i przesyłanie kopii oświadczeń o stanie majątkowym do urzędów skarbowych i do jednostek samorządu terytorialnego w celu ogłoszenia w Biuletynie Informacji Publicznej,

f) udostępnianie oświadczeń o stanie majątkowym uprawnionym organom oraz instytucjom;

8) pkt 11 regulaminu organizacyjnego, w szczególności przez:

a) przyjmowanie oświadczeń lustracyjnych oraz ich przekazywanie do Instytutu Pamięci Narodowej - Głównej Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu,

b) monitorowanie zmian personalnych na stanowiskach, których zajmowanie wiąże się z obowiązkiem złożenia oświadczenia lustracyjnego oraz przekazywanie informacji w tym zakresie do Instytutu Pamięci Narodowej - Głównej Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu,

c) prowadzenie i aktualizowanie ewidencji osób, które złożyły oświadczenie lustracyjne;

9) pkt 12 regulaminu organizacyjnego, w szczególności przez:

a) wzajemną wymianę z Biurem Informatyki informacji o zagrożeniach cyberbezpieczeństwa i podatności na incydenty systemów informatycznych w celu

zapewnienie poufności, integralności, dostępności i autentyczności danych przetwarzanych w systemach informatycznych,

b) współdziałanie z Biurem Informatyki w kwalifikacji i ocenie incydentów;

2. Oddział do spraw **Ochrony Informacji Niejawnych** realizuje także następujące zadania:

1) koordynacja spraw związanych z opracowywaniem i realizacją planu działania biura oraz sporządzaniem analiz i sprawozdań;
2) koordynacja współpracy biura w ramach prowadzonych przez Urząd programów i projektów;
3) prowadzenie rejestrów skarg, wniosków i petycji związanych z działalnością biura oraz nadzór nad ich terminowym załatwianiem;
4) współpraca z Biurem Kadr i Obsługi Prawnej w Urzędzie w zakresie spraw kadrowych, socjalnych, dyscypliny pracy i szkoleń pracowników biura;
5) zapewnienie obsługi sekretariatu oraz prawidłowego obiegu dokumentacji w biurze.

§ 7. Do zakresu działania **Kancelarii Tajnej** należy realizacja zadania określonego w § 31 ust. 3 pkt 8 regulaminu organizacyjnego, w szczególności przez:

1) przyjmowanie, rejestrowanie, przechowywanie i wysyłanie informacji niejawnych;
2) prowadzenie obowiązujących dzienników ewidencji;
3) udostępnianie oraz egzekwowanie zwrotu materiałów zawierających informacje niejawne;
4) zapewnienie przestrzegania właściwego oznaczania i rejestrowania informacji niejawnych;
5) okresowa kontrola ewidencji i obiegu informacji niejawnych przechowywanych w Kancelarii Tajnej oraz bieżący nadzór nad postępowaniem z informacjami niejawnymi;
6) przeprowadzanie, nie rzadziej niż raz na 5 lat, przeglądu dokumentów niejawnych w celu ustalenia, czy spełniają one ustawowe przesłanki ochrony;
7) nadzór nad funkcjonowaniem systemu ochrony fizycznej Kancelarii Tajnej.

§ 8. Do zakresu działania **Inspektora,** o którym mowa w § 31 ust 2 pkt 2 regulaminu organizacyjnego, należy zapewnianie przestrzegania w Urzędzie przepisów o ochronie danych osobowych, w szczególności przez:

1) informowanie Wojewody oraz pracowników Urzędu, którzy przetwarzają dane osobowe, o obowiązkach i prawach wynikających z przepisów o ochronie danych

osobowych, a także udzielanie porad oraz rekomendowanie określonych działań w tym zakresie;

2) monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz regulacji wewnętrznych w tym zakresie, z uwzględnieniem podziału obowiązków;
3) organizowanie szkoleń dla pracowników Urzędu i podejmowanie działań zwiększających ich świadomość w zakresie ochrony danych osobowych;
4) opiniowanie spraw w zakresie ochrony danych osobowych;
5) prowadzenie planowych i doraźnych audytów pod kątem zgodności z przepisami o ochronie danych osobowych;
6) udzielanie na żądanie Wojewody zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie ich wykonania;
7) współpracę z Prezesem Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych, prowadzenie konsultacji w przypadku stwierdzenia wysokiego ryzyka przetwarzania danych oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
8) prowadzenie ewidencji rejestru czynności, rejestru kategorii czynności, a także umów powierzenia przetwarzania danych osobowych.