

# MAZOWIECKI URZĄD WOJEWÓDZKI W WARSZAWIE

---

## REGULAMIN WEWNĘTRZNY BIURA OCHRONY

**Zatwierdzam**

Dyrektor Generalny

Mazowieckiego Urzędu Wojewódzkiego

w Warszawie

Kamila Jeziorska-Chojecka

---

Warszawa, dnia 24 stycznia 2020 r.

## **REGULAMIN WEWNĘTRZNY BIURA OCHRONY**

Na podstawie § 9 ust. 1 Regulaminu Organizacyjnego Mazowieckiego Urzędu Wojewódzkiego w Warszawie stanowiącego załącznik do zarządzenia nr 5 Wojewody Mazowieckiego z dnia 18 stycznia 2019 r. w sprawie ustalenia Regulaminu Organizacyjnego Mazowieckiego Urzędu Wojewódzkiego w Warszawie oraz zarządzenia nr 60 Wojewody Mazowieckiego z dnia 12 listopada 2019 r. zmieniającego zarządzenie w sprawie ustalenia Regulaminu Organizacyjnego Mazowieckiego Urzędu Wojewódzkiego w Warszawie, ustala się Regulamin Wewnętrzny Biura Ochrony.

### **Rozdział 1**

#### **Postanowienia ogólne**

Regulamin Wewnętrzny Biura Ochrony w Mazowieckim Urzędzie Wojewódzkim w Warszawie, określa zadania i strukturę organizacyjną oraz zakres działania wewnętrznych komórek organizacyjnych Biura Ochrony.

### **Rozdział 2**

#### **Słownik terminów**

§ 1. Ilekroć w Regulaminie Wewnętrznym 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 stanowiący załącznik do zarządzenia nr 5 Wojewody Mazowieckiego z dnia 18 stycznia 2019 r. w sprawie ustalenia Regulaminu Organizacyjnego Mazowieckiego Urzędu Wojewódzkiego w Warszawie oraz zarządzenia nr 60 Wojewody Mazowieckiego z dnia 12 listopada 2019 r. zmieniającego zarządzenie w sprawie ustalenia Regulaminu Organizacyjnego Mazowieckiego Urzędu Wojewódzkiego w Warszawie;
- 8) regulaminie wewnętrznym – należy przez to rozumieć regulamin wewnętrzny biura;
- 9) Bezpieczne Stanowisko Komputerowe – system teleinformatyczny Bezpieczne Stanowisko Komputerowe w Urzędzie służący do przetwarzania informacji niejawnych.

### **Rozdział 3**

#### **Struktura biura**

§ 2. 1. W skład biura wchodzi 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.

4. Obsługę prawną biura zapewnia Biuro Kadr i Organizacji w Urzędzie.

### **Rozdział 4**

#### **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 Inspektora jego obowiązki wykonuje osoba zastępująca wyznaczona przez Wojewodę.

3. Podczas nieobecności Pełnomocnika do spraw Ochrony Informacji Niejawnych jego obowiązki, w zakresie zadań wynikających z przepisów o ochronie informacji niejawnych, wykonuje wyznaczony przez Wojewodę pracownik na podstawie stosownego upoważnienia.

4. Kancelarią Tajną kieruje zatrudniony przez Wojewodę Kierownik Kancelarii Tajnej, który w zakresie realizacji zadań określonych w § 7 regulaminu wewnętrznego 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 5**

### **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 biura;
- 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 biura.

## **Rozdział 6**

### **Zakresy działania**

**§ 6.** Do zakresu działania **Oddziału do spraw Ochrony Informacji Niejawnych** należy w szczególności:

- 1) zapewnienie stosowania odpowiednich środków bezpieczeństwa fizycznego informacji niejawnych;
- 2) nadzór nad prawidłowym wytwarzaniem, przetwarzaniem, przechowywaniem i przekazywaniem informacji niejawnych;
- 3) opracowywanie i aktualizowanie wymaganej przepisami o ochronie informacji niejawnych dokumentacji bezpieczeństwa informacji niejawnych, w szczególności:
  - a) dokumentacji dotyczącej sposobu i trybu przetwarzania informacji niejawnych,
  - b) planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego i nadzorowanie jego realizacji,
  - c) dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą;
- 4) opracowywanie i aktualizację materiałów szkoleniowych oraz prowadzenie szkoleń w zakresie ochrony informacji niejawnych i wydawanie zaświadczeń o ich odbyciu;
- 5) prowadzenie postępowań wyjaśniających okoliczności naruszenia przepisów o ochronie informacji niejawnych;
- 6) realizację zadań inspektora bezpieczeństwa teleinformatycznego oraz administratora systemu w stosunku do funkcjonującego w biurze Bezpiecznego Stanowiska Komputerowego;

- 7) nadzór nad fizycznym zabezpieczeniem pomieszczenia, w którym znajduje się Bezpieczne Stanowisko Komputerowe;
- 8) sporządzanie oraz nadzór nad przestrzeganiem procedury wydawania upoważnień osobom dopuszczonym do obsługi Bezpiecznego Stanowiska Komputerowego i urządzeń wchodzących w jego skład oraz nadzór nad przetwarzaniem dokumentów na Bezpiecznym Stanowisku Komputerowym;
- 9) prowadzenie szkoleń pracowników z zakresu bezpieczeństwa teleinformatycznego systemów i sieci teleinformatycznych Urzędu, w których są przetwarzane informacje niejawne lub dane osobowe;
- 10) okresową kontrolę zgodności funkcjonowania systemów i sieci teleinformatycznych Urzędu, w których są przetwarzane informacje ustawowo chronione, z przyjętymi zasadami i procedurami bezpieczeństwa;
- 11) opracowywanie wymaganej przepisami o ochronie informacji niejawnych dokumentacji dotyczącej systemu bezpieczeństwa teleinformatycznego, w tym szacowanie i zarządzanie ryzykiem;
- 12) kontrola ochrony informacji niejawnych oraz kontrola przestrzegania przepisów o ochronie tych informacji;
- 13) przeprowadzanie, co najmniej raz na 3 lata, okresowej kontroli ewidencji materiałów i obiegu dokumentów niejawnych w Urzędzie;
- 14) wydawanie upoważnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone”;
- 15) prowadzenie zwykłych postępowań sprawdzających i kontrolnych postępowań sprawdzających oraz przechowywanie akt zakończonych postępowań sprawdzających;
- 16) 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;
- 17) 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;
- 18) współpracę z Inspektorem w opracowywaniu i aktualizacji dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych w Urzędzie;
- 19) wydawanie upoważnień do przetwarzania danych osobowych;

- 20) realizowanie procedur związanych z nadawaniem i usuwaniem uprawnień pracowników do Systemu Rejestrów Państwowych (rejestr PESEL i Rejestr Stanu Cywilnego);
- 21) współudział w szkoleniu pracowników Urzędu w zakresie ochrony danych osobowych;
- 22) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie;
- 23) udział w prowadzonych przez Inspektora kontrolach w zakresie przestrzegania przepisów o ochronie danych osobowych;
- 24) współpracę z Biurem Informatyki w Urzędzie w zakresie realizacji zadań związanych z ochroną danych osobowych w systemach i sieciach teleinformatycznych;
- 25) przyjmowanie, ewidencjonowanie, przechowywanie i analizę dokumentacji oświadczeń o stanie majątkowym składanych Wojewodzie i Dyrektorowi Generalnemu przez zobowiązane osoby pełniące funkcje publiczne;
- 26) 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;
- 27) przyjmowanie, ewidencjonowanie i przechowywanie dokumentacji oświadczeń o stanie majątkowym składanych Wojewodzie przez zobowiązanych przedstawicieli administracji samorządowej;
- 28) dokonywanie analizy danych zawartych w oświadczeniach o stanie majątkowym, w tym opracowywanie wniosków do Centralnego Biura Antykorupcyjnego;
- 29) przygotowywanie i przesyłanie kopii oświadczeń o stanie majątkowym do urzędów skarbowych i do jednostek samorządu terytorialnego w celu ogłoszenia w Biuletynie Informacji Publicznej Urzędu;
- 30) udostępnianie oświadczeń o stanie majątkowym uprawnionym organom oraz instytucjom;
- 31) przyjmowanie oświadczeń lustracyjnych oraz ich przekazywanie do Instytutu Pamięci Narodowej - Głównej Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu;
- 32) 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;

- 33) prowadzenie i aktualizowanie ewidencji osób, które złożyły oświadczenie lustracyjne;
- 34) wzajemną wymianę z Biurem Informatyki w Urzędzie informacji o zagrożeniach cyberbezpieczeństwa i podatności na incydenty systemów informatycznych w celu zapewnienia poufności, integralności, dostępności i autentyczności danych przetwarzanych w systemach informatycznych;
- 35) współdziałanie z Biurem Informatyki w Urzędzie w kwalifikacji i ocenie incydentów;
- 36) koordynacja spraw związanych z opracowywaniem i realizacją planu działania biura oraz sporządzaniem analiz i sprawozdań;
- 37) koordynacja współpracy biura w ramach prowadzonych przez Urząd programów i projektów;
- 38) prowadzenie rejestrów skarg, wniosków i petycji związanych z działalnością biura oraz nadzór nad ich terminowym załatwianiem;
- 39) współpraca z Biurem Kadr i Organizacji w Urzędzie w zakresie spraw kadrowych, socjalnych, dyscypliny pracy i szkoleń pracowników biura;
- 40) zapewnienie obsługi sekretariatu biura oraz prawidłowego obiegu dokumentacji w biurze.

§ 7. Do zakresu działania **Kancelarii Tajnej** należy prowadzenie kancelarii tajnej oraz realizacja zadań w zakresie zapewnienia bezpieczeństwa i ochrony przetwarzanych w Urzędzie informacji niejawnych, 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) ewidencjonowanie, przechowywanie i udostępnianie osobom uprawnionym aktów prawnych Wojewody zawierających informacje niejawne o klauzuli „poufne” lub wyższej.

**§ 8.** Do zakresu działania **Inspektora**, 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 w zakresie 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.