MAZOWIECKI URZĄD WOJEWÓDZKI W WARSZAWIE

R E G U L A M I N W E W N Ę T R Z N Y

B I U R A O C H R O N Y

Zatwierdzam

Dyrektor Generalny

Mazowieckiego Urzędu Wojewódzkiego

w Warszawie

Anna Pankowska-Gałaj

Warszawa, dnia 08 lutego 2023 r.

REGULAMIN WEWNĘTRZNY BIURA OCHRONY

Na podstawie § 9 ust. 4 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, zmienionego zarządzeniem nr 60 z dnia 12 listopada 2019 r., zarządzeniem nr 53 z dnia 6 lutego 2020 r., zarządzeniem nr 477 z dnia 16 grudnia 2020 r., zarządzeniem nr 463 z dnia 23 listopada 2021 r., zarządzeniem z dnia 14 grudnia 2022 r. oraz zarządzeniem z dnia 19 stycznia 2023 r., ustala się Regulamin Wewnętrzny Biura Ochrony[1].

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 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;
6) **JAZ** – należy przez to rozumieć Jednostki Administracji Zespolonej;

[1] Traci moc Regulamin Wewnętrzny Biura Ochrony zatwierdzony przez Dyrektora Generalnego Mazowieckiego Urzędu Wojewódzkiego w Warszawie w dniu 24 stycznia 2020 r.

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, zmienionego zarządzeniem nr 60 z dnia 12 listopada 2019 r., zarządzeniem nr 53 z dnia 6 lutego 2020 r., zarządzeniem nr 477 z dnia 16 grudnia 2020 r., zarządzeniem nr 463 z dnia 23 listopada 2021 r., zarządzeniem z dnia 14 grudnia 2022 r. oraz zarządzeniem z dnia 19 stycznia 2023 r.;
8) **regulaminie wewnętrznym** – należy przez to rozumieć regulamin wewnętrzny biura;
9) **Bezpiecznym Stanowisku Komputerowym** – należy przez to rozumieć system teleinformatyczny Bezpieczne Stanowisko Komputerowe w Urzędzie, służący do przetwarzania informacji niejawnych.

Rozdział 3
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**;
3) Oddział do spraw Ochrony Danych Osobowych - **BO-III.**

2. W strukturze biura funkcjonuje, podlegający bezpośrednio Wojewodzie, Inspektor Ochrony Danych, będący jednocześnie Koordynatorem Oddziału do spraw Ochrony Danych Osobowych, 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. Do zakresu działania Pełnomocnika do spraw Ochrony Informacji Niejawnych należy w szczególności zapewnienie przestrzegania przepisów o ochronie informacji niejawnych oraz stała współpraca, w powyższym zakresie z Agencją Bezpieczeństwa Wewnętrznego i Służbą Kontrwywiadu Wojskowego.

5. W strukturze biura funkcjonuje Zastępca Pełnomocnika do spraw Ochrony Informacji Niejawnych, podległy bezpośrednio Pełnomocnikowi do spraw Ochrony Informacji Niejawnych.
6. W strukturze Oddziału do spraw Ochrony Informacji Niejawnych funkcjonuje Kancelaria Materiałów Niejawnych, zwana dalej „KMN".
7. 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 Ochrony Danych jego obowiązki wykonuje Zastępca Inspektora Ochrony Danych, jeśli został wyznaczony.
4. 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.
5. Kancelarią Tajną kieruje zatrudniony przez Wojewodę Kierownik Kancelarii Tajnej, który w zakresie realizacji zadań określonych w § 9 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.

§ 5. 1. Oddziałem do spraw Ochrony Danych Osobowych kieruje Koordynator, będący jednocześnie Inspektorem Ochrony Danych.

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

Rozdział 5

Zadania wspólne

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

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

Rozdział 6

Zakresy działania

§ 7. 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 w komórkach organizacyjnych Urzędu oraz JAZ;
3) opracowywanie i aktualizowanie dokumentacji w zakresie bezpieczeństwa informacji niejawnych, w tym:
    a) dokumentacji dotyczącej sposobu i trybu przetwarzania informacji niejawnych,
    b) planu ochrony informacji niejawnych,
    c) w razie wprowadzenia stanu nadzwyczajnego nadzorowanie realizacji procedur zawartych w powyższym planie,
    d) dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą;

4) opracowywanie i aktualizowanie 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 administratora i inspektora bezpieczeństwa teleinformatycznego w stosunku do funkcjonujących systemów do przetwarzania informacji niejawnych;
7) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których znajdują się Bezpieczne Stanowiska Komputerowe;
8) sporządzanie oraz nadzór nad przestrzeganiem zapisów 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 przetwarzane są informacje niejawne lub dane osobowe;
10) okresowa kontrola zgodności funkcjonowania systemów i sieci teleinformatycznych Urzędu, w których przetwarzane są 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 wobec pracowników Urzędu i pracowników JAZ 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) współpraca 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) realizowanie procedur związanych z nadawaniem i usuwaniem uprawnień pracowników do Systemu Rejestrów Państwowych (rejestr PESEL i Rejestr Stanu Cywilnego);
19) przyjmowanie, ewidencjonowanie, przechowywanie i analiza dokumentacji oświadczeń o stanie majątkowym składanych Wojewodzie i Dyrektorowi Generalnemu przez zobowiązane osoby pełniące funkcje publiczne;
20) 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;
21) przyjmowanie, ewidencjonowanie i przechowywanie dokumentacji oświadczeń o stanie majątkowym składanych Wojewodzie przez zobowiązanych przedstawicieli administracji samorządowej;
22) dokonywanie analizy danych zawartych w oświadczeniach o stanie majątkowym, w tym opracowywanie wniosków do Centralnego Biura Antykorupcyjnego;
23) przygotowywanie i przesyłanie kopii oświadczeń o stanie majątkowym do urzędów skarbowych i do jednostek samorządu terytorialnego w celu ich ogłoszenia w Biuletynie Informacji Publicznej;
24) udostępnianie oświadczeń o stanie majątkowym oraz ich analiz uprawnionym organom oraz instytucjom;
25) przyjmowanie oświadczeń lustracyjnych oraz ich przekazywanie do Instytutu Pamięci Narodowej - Głównej Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu;
26) 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;
27) prowadzenie i aktualizowanie ewidencji osób, które złożyły oświadczenie lustracyjne;

28) koordynacja spraw związanych z opracowywaniem i realizacją planu działania biura oraz sporządzaniem analiz i sprawozdań;
29) koordynacja współpracy biura w ramach prowadzonych przez Urząd programów i projektów;
30) prowadzenie rejestrów skarg, wniosków i petycji związanych z działalnością biura oraz nadzór nad ich terminowym załatwianiem;
31) współpraca z Biurem Kadr i Organizacji w Urzędzie w zakresie spraw kadrowych, socjalnych, dyscypliny pracy i szkoleń pracowników biura;
32) zapewnienie obsługi sekretariatu oraz prawidłowego obiegu dokumentacji w biurze;
33) przyjmowanie, rejestrowanie, przechowywanie w KMN oraz wysyłanie informacji niejawnych o klauzuli „Zastrzeżone”;
34) prowadzenie obowiązujących dzienników ewidencji dokumentów niejawnych w KMN o klauzuli „Zastrzeżone”;
35) udostępnianie oraz egzekwowanie zwrotu materiałów zawierających informacje niejawne do KMN o klauzuli „Zastrzeżone”;
36) zapewnienie przestrzegania właściwego oznaczania i rejestrowania informacji niejawnych w KMN o klauzuli „Zastrzeżone.

§ 8. Do zakresu działania **Oddziału do spraw Ochrony Danych Osobowych oraz Inspektora** należy zapewnianie przestrzegania w Urzędzie przepisów o ochronie danych osobowych, w szczególności przez:

1) informowanie Wojewody i Dyrektora Generalnego Urzędu 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 i prowadzenie 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 i Dyrektora Generalnego Urzędu 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 rejestru czynności przetwarzania, rejestru kategorii czynności przetwarzania, a także rejestru umów powierzenia przetwarzania danych osobowych;
9) opracowywanie i aktualizowanie dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych w Urzędzie;
10) przygotowywanie upoważnień do przetwarzania danych osobowych;
11) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie;
12) prowadzenie kontroli (audytu) w zakresie przestrzegania przepisów o ochronie danych osobowych w Urzędzie i w podmiotach przetwarzających;
13) współpraca z Biurem Informatyki w Urzędzie w zakresie realizacji zadań związanych z ochroną danych osobowych w systemach i sieciach teleinformatycznych;
14) prowadzenie z Biurem Informatyki wzajemnej wymiany informacji o zagrożeniach cyberbezpieczeństwa i podatności na incydenty systemów informatycznych w celu zapewnienia poufności, integralności, dostępności i autentyczności danych przetwarzanych w systemach informatycznych;
15) współdziałanie z Biurem Informatyki w kwalifikacji i ocenie incydentów i naruszeń związanych z ochroną danych osobowych w systemach i sieciach teleinformatycznych;
16) współpraca w zakresie opracowywania i realizacji planu działania biura oraz sporządzaniu analiz i sprawozdań;
17) udział w ramach biura w prowadzonych przez Urząd programach i projektach;
18) prowadzenie rejestrów skarg, wniosków i petycji związanych z działalnością oddziału oraz nadzór nad ich terminowym załatwianiem;
19) współpraca z Biurem Kadr i Organizacji w Urzędzie w zakresie spraw kadrowych, socjalnych, dyscypliny pracy i szkoleń pracowników biura.

§ 9. 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.