

## **PROJEKT USTAWY**

**z dnia .....**

**o ochronie informacji niejawnych<sup>1</sup>**

### **Rozdział 1**

#### **Przepisy ogólne**

##### **Art. 1**

1. Ustawa określa zasady ochrony informacji, które wymagają ochrony przed nieuprawnionym ujawnieniem, jako stanowiące „informacje niejawne”, niezależnie od formy i sposobu ich wyrażania, także w trakcie ich opracowania, a w szczególności:
  - 1) organizowania ochrony informacji niejawnych;
  - 2) klasyfikowania informacji niejawnych;
  - 3) przetwarzania informacji niejawnych;
  - 4) postępowania sprawdzającego, w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej „postępowaniem sprawdzającym”;
  - 5) postępowania bezpieczeństwa przemysłowego, w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych;
  - 6) szkolenia w zakresie ochrony informacji niejawnych;
  - 7) ewidencjonowania, przechowywania, przetwarzania i udostępniania danych uzyskiwanych w związku z prowadzonymi postępowaniami o ustalenie rękojmi zachowania tajemnicy, w zakresie określonym w ankiecie bezpieczeństwa osobowego oraz w kwestionariuszu bezpieczeństwa przemysłowego;
  - 8) organizacji kontroli przestrzegania zasad ochrony informacji niejawnych;
  - 9) ochrony informacji niejawnych w systemach teleinformatycznych;
  - 10) stosowania środków ochrony fizycznej informacji niejawnych.
2. Przepisy ustawy mają zastosowanie do:
  - 1) organów władzy publicznej, w szczególności:
    - a) Sejmu i Senatu Rzeczypospolitej Polskiej;
    - b) Prezydenta Rzeczypospolitej Polskiej;
    - c) organów administracji rządowej;

- d) organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych;
  - e) sądów i trybunałów;
  - f) organów kontroli państwowej i ochrony prawa;
  - 2) Sił Zbrojnych Rzeczypospolitej Polskiej i ich jednostek organizacyjnych, a także innych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
  - 3) Narodowego Banku Polskiego;
  - 4) państwowych osób prawnych i innych niż wymienione w pkt 1-3 państwowych jednostek organizacyjnych, z wyjątkiem jednostek, o których mowa w pkt 5;
  - 5) przedsiębiorców zamierzających ubiegać się, ubiegających się o zawarcie lub wykonujących umowy związane z dostępem do informacji niejawnych albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.
3. Przepisów ustawy nie stosuje się do ochrony tajemnic zawodowych lub innych tajemnic prawnie chronionych określonych w odrębnych przepisach.

## **Art. 2**

W rozumieniu ustawy:

- 1) jednostką organizacyjną – jest podmiot wymieniony w art. 1 ust. 2;
- 2) rękojmią zachowania tajemnicy – jest spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem;
- 3) dokumentem – jest każda utrwalona informacja niejawna, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, na taśmach elektromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy, kalki, taśmy atramentowej, jak również informacja niejawna utrwalona na informatycznych nośnikach danych;
- 4) materiałem – jest dokument, jak też chroniony jako informacja niejawna przedmiot lub dowolna jego część, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowana albo będąca w trakcie produkcji, a także składnik użyty do ich wytworzenia;
- 5) przetwarzaniem informacji niejawnych – są jakiegokolwiek operacje wykonywane z informacjami niejawnymi, w szczególności wytwarzanie, modyfikowanie, przechowywanie, przekazywanie lub udostępnianie informacji;

- 6) systemem teleinformatycznym – jest zespół współpracujących ze sobą, zgodnie z określonymi procedurami i metodami postępowania stosowanymi przez wyspecjalizowany personel, urządzeń i oprogramowania, zapewniający przetwarzanie informacji niejawnych, w tym także wysyłanie i odbieranie tych informacji poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.<sup>2</sup>);
- 7) akredytacją bezpieczeństwa teleinformatycznego – jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych, na zasadach określonych w ustawie;
- 8) dokumentacją bezpieczeństwa systemu teleinformatycznego – jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;
- 9) przedsiębiorcą – jest przedsiębiorca w rozumieniu ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2007 r. Nr 155, poz. 1095 z późn. zm.<sup>3</sup>) lub każda inna jednostka organizacyjna, niezależnie od formy własności, które w ramach prowadzonej działalności gospodarczej będą realizować lub realizują umowy albo zadania wynikające z przepisów prawa;
- 10) kierownikiem przedsiębiorcy jest członek jednoosobowego zarządu lub innego jednoosobowego organu zarządzającego, a jeżeli organ jest wieloosobowy – cały organ albo członek lub członkowie tego organu wyznaczeni co najmniej uchwałą zarządu do pełnienia funkcji kierownika przedsiębiorcy, z wyłączeniem pełnomocników ustanowionych przez ten organ lub jednostkę. W przypadku spółki jawnej i spółki cywilnej kierownikiem są wspólnicy prowadzący sprawy spółki, w przypadku spółki partnerskiej - wspólnicy prowadzący sprawy spółki albo zarząd, a w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej – komplementariusze prowadzący sprawy spółki. W przypadku osoby fizycznej prowadzącej działalność gospodarczą kierownikiem jest ta osoba. Za kierownika uważa się również likwidatora, a także syndyka lub zarządcę ustanowionego w postępowaniu upadłościowym.

### **Art. 3**

Do postępowań sprawdzających w zakresie bezpieczeństwa osobowego oraz postępowań bezpieczeństwa przemysłowego w zakresie nieuregulowanym w ustawie mają zastosowanie przepisy art. 6-8, art. 12, art. 14-16, art. 24 § 1 pkt 1-6 i § 2-4, art. 26 § 1, art. 28, art. 29,

art. 30 § 1-3, art. 35 § 1, art. 39, art. 41- 47, art. 50, art. 55 § 1-2, art. 57-60, art. 61 § 3 i 4, art. 63 § 4, art. 64, art. 65 § 1-2, art. 97 § 1 pkt 4 i § 2, art. 98, art. 101, art. 103, art. 104, art. 105, art. 107, art. 112, art. 113, art. 156-158 oraz art. 217 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071, z późn. zm.<sup>4</sup>).

#### **Art. 4.**

1. Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo innej zleconej pracy.
2. Zasady zwalniania od obowiązku zachowania w tajemnicy informacji niejawnych oraz sposób postępowania z aktami spraw zawierających informacje niejawne w postępowaniu przed sądami i innymi organami, określają przepisy odrębnych ustaw.
3. Jeżeli przepisy odrębnych ustaw uprawniają organy, służby lub instytucje państwowe albo ich upoważnionych pracowników do dokonywania kontroli, a w szczególności swobodnego dostępu do pomieszczeń i materiałów, a jej zakres dotyczy informacji niejawnych, uprawnienia te są realizowane z zachowaniem przepisów niniejszej ustawy.

## **Rozdział 2**

### **Klasyfikowanie informacji niejawnych**

#### **Art. 5**

1. Informację niejawną oznacza się klauzulą „ściśle tajne”, jeżeli jej nieuprawnione ujawnienie spowodowałoby wyjątkowo duże szkody dla Rzeczypospolitej Polskiej przez to, że:
  - 1) stwarzałyby zagrożenie dla niepodległości, suwerenności, integralności terytorialnej lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
  - 2) w istotny sposób zagrażałyby soюзom lub międzynarodowej pozycji Rzeczypospolitej Polskiej;
  - 3) wyrządzałyby nieodwracalne szkody obronności Rzeczypospolitej Polskiej;
  - 4) powodowałyby ujawnienie danych funkcjonariuszy lub żołnierzy służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu wykonujących czynności operacyjno-rozpoznawcze oraz osób udzielających im pomocy w tym zakresie.

2. Informację niejawną oznacza się klauzulą „tajne”, jeżeli jej nieuprawnione ujawnienie spowodowałoby duże szkody dla Rzeczypospolitej Polskiej przez to, że:
  - 1) w znacznym stopniu narażałoby na uszczerbek stosunki Rzeczypospolitej Polskiej z innymi państwami;
  - 2) zagrażałoby przygotowaniom obronnym Rzeczypospolitej Polskiej lub funkcjonowaniu jej Sił Zbrojnych;
  - 3) uniemożliwiłoby realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
  - 4) spowodowałoby duży uszczerbek dla interesów gospodarczych Rzeczypospolitej Polskiej;
  - 5) istotnie utrudniłoby wykonywanie czynności operacyjno-rozpoznawczych przez organy, służby lub instytucje do tego uprawnione;
  - 6) powodowałoby ujawnienie danych funkcjonariuszy lub żołnierzy wykonujących czynności operacyjno-rozpoznawcze oraz osób udzielających im pomocy w tym zakresie.
3. Informację niejawną oznacza się klauzulą „poufne”, jeżeli jej nieuprawnione ujawnienie mogłoby zaszkodzić Rzeczypospolitej Polskiej przez to, że:
  - 1) przyniosłoby szkody dla bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
  - 2) przyniosłoby szkody dla obronności lub Sił Zbrojnych Rzeczypospolitej Polskiej;
  - 3) zagrażałoby porządkowi publicznemu lub bezpieczeństwu obywateli;
  - 4) utrudniłoby wykonywanie ustawowych zadań przez organy, służby lub instytucje odpowiedzialne za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
  - 5) osłabiłoby system finansowy Rzeczypospolitej Polskiej;
  - 6) naraziłoby na szkodę interesy ekonomiczne Rzeczypospolitej Polskiej lub funkcjonowanie gospodarki narodowej.
4. Informację niejawną oznacza się klauzulą „zastrzeżone”, jeżeli nie oznaczono jej wyższą klauzulą tajności, a jej nieuprawnione ujawnienie byłoby niekorzystne z punktu widzenia interesów Rzeczypospolitej Polskiej, w szczególności jej polityki zagranicznej, obrony narodowej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

5. Informacje niejawne przekazane przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych oznaczają się polskim odpowiednikiem posiadanej klauzuli tajności.

#### **Art. 6**

1. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.
2. Informacje niejawne podlegają ochronie w sposób określony w ustawie do czasu zniesienia lub zmiany klauzuli tajności na zasadach określonych w ust. 3, z zastrzeżeniem ust. 6. Osoba, o której mowa w ust. 1 może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.
3. Zniesienie lub zmiana klauzuli tajności możliwa jest wyłącznie w przypadku podjęcia decyzji przez osobę, o której mowa w ust. 1 albo jej przełożonego w sytuacji ustania lub zmiany ustawowych przesłanek ochrony.
4. Do wykonania czynności, o której mowa w ust. 3, w przypadku informacji o klauzuli „ściśle tajne” lub „tajne”, niezbędna jest również wyrażona na piśmie zgoda kierownika jednostki organizacyjnej, w której materiałowi została nadana klauzula tajności.
5. Po zniesieniu lub zmianie klauzuli tajności podejmuje się niezbędne czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich ewentualnych odbiorców. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom, są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzuli tajności.
6. Uprawnienia w zakresie zniesienia lub zmiany klauzuli tajności materiału przechodzą, w przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji jednostki organizacyjnej, na jej następcę prawnego. W razie braku następcy prawnego, uprawnienia w tym zakresie przechodzą na Agencję Bezpieczeństwa Wewnętrznego, zwaną dalej „ABW” lub Służbę Kontrwywiadu Wojskowego, zwaną dalej „SKW”.
7. Materiał zawierający informacje niejawne może być oznaczony w sposób umożliwiający nadanie poszczególnym jego częściom różnych klauzul tajności.
8. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób oznaczania materiałów, umieszczania na nich klauzul tajności, a także sposób zmiany lub znoszenia nadanej klauzuli.
9. W rozporządzeniu, o którym mowa w ust. 8, Prezes Rady Ministrów uwzględni potrzebę oznaczania materiałów w sposób zapewniający ich odróżnienie od materiałów jawnych,

mając na uwadze rodzaje klauzul tajności i materiałów oraz sposób odrębnego oznaczania części materiału niejawnego, o którym mowa w ust. 7.

#### **Art. 7**

Chronione bez względu na upływ czasu pozostają:

- 1) dane identyfikujące funkcjonariuszy i żołnierzy ABW, Agencji Wywiadu, zwanej dalej AW, SKW, Służby Wywiadu Wojskowego, zwanej dalej SWW, Centralnego Biura Antykorupcyjnego, zwanego dalej CBA oraz byłego Urzędu Ochrony Państwa, zwanego dalej były UOP i byłych Wojskowych Służb Informacyjnych, zwanych dalej były WSI, wykonujących czynności operacyjno-rozpoznawcze;
- 2) dane identyfikujące osoby, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych organom, służbom i instytucjom państwowym uprawnionym do ich wykonywania na podstawie ustawy;
- 3) informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

#### **Art. 8**

Informacje niejawne, którym przyznano określoną klauzulę tajności:

- 1) mogą być udostępnione wyłącznie osobie uprawnionej zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności;
- 2) muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami ustawy określającymi wymagania dotyczące kancelarii tajnych, obiegu materiałów i środków ochrony fizycznej, odpowiednich dla przyznanej im klauzuli tajności;
- 3) muszą być chronione, odpowiednio dla przyznanej klauzuli tajności, przy zastosowaniu określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie środków bezpieczeństwa.

#### **Art. 9**

1. Odbiorca materiału, w przypadku stwierdzenia wyraźnego zawyżenia lub zaniżenia klauzuli tajności, zwraca się do osoby, która ją nadała albo przełożonego tej osoby z wnioskiem o dokonanie stosownej zmiany.

2. W przypadku odmowy dokonania zmiany lub nieudzielenia odpowiedzi w ciągu 30 dni od daty doręczenia wniosku, o którym mowa w ust. 1, odbiorca może zwrócić się do ABW lub SKW o rozstrzygnięcie sporu. Rozstrzygnięcie to jest ostateczne i nie podlega odwołaniu.
3. Spór, o którym mowa w ust. 2, jeśli jego stroną jest ABW lub SKW rozstrzyga Prezes Rady Ministrów.
4. Prezes Rady Ministrów może upoważnić Szefa Kancelarii Prezesa Rady Ministrów, sekretarza stanu albo podsekretarza stanu w Kancelarii Prezesa Rady Ministrów do wykonywania czynności, o których mowa w ust. 3.

### **Rozdział 3**

#### **Organizacja ochrony informacji niejawnych**

##### **Art. 10**

1. ABW i SKW nadzorując funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości:
  - 1) prowadzą kontrole ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;
  - 2) realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;
  - 3) prowadzą postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego według zasad określonych w ustawie;
  - 4) zapewniają ochronę informacji niejawnych wymienianych przez Rzeczpospolitą Polską z innymi państwami i organizacjami międzynarodowymi;
  - 5) prowadzą doradztwo i szkolenia określone w przepisach ustawy, w zakresie ochrony informacji niejawnych;
  - 6) wykonują inne zadania, w zakresie ochrony informacji niejawnych, określone odrębnymi przepisami.
2. SKW realizuje zadania, o których mowa w ust. 1, w odniesieniu do:
  - 1) Sił Zbrojnych Rzeczypospolitej Polskiej i ich jednostek organizacyjnych;
  - 2) Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
  - 3) wojskowych organów ochrony prawa;

- 4) ataszatów obrony w przedstawicielstwach dyplomatycznych Rzeczypospolitej Polskiej;
  - 5) żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione w pkt 1-4.
3. ABW realizuje zadania, o których mowa w ust. 1, w odniesieniu do jednostek organizacyjnych i osób będących podmiotami ustawy, z zastrzeżeniem ust. 2.

### **Art. 11**

1. Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.
2. Krajowa władza bezpieczeństwa jest właściwa do wykonywania zadań w zakresie ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi, a w szczególności do:
  - 1) sprawowania bieżącego nadzoru stanu ochrony informacji niejawnych;
  - 2) prowadzenia inspekcji w podmiotach, w których są lub będą przetwarzane informacje niejawne;
  - 3) akredytacji kancelarii tajnych i innych pomieszczeń, w których przetwarzane są informacje niejawne;
  - 4) wydawania poświadczeń bezpieczeństwa i świadectw bezpieczeństwa przemysłowego oraz innych dokumentów potwierdzających zdolność do ochrony informacji niejawnych;
  - 5) wydawania świadectw akredytacji bezpieczeństwa teleinformatycznego;
  - 6) przeprowadzania postępowań wyjaśniających w przypadkach naruszenia zasad bezpieczeństwa informacji niejawnych;
  - 7) szkolenia i doradztwa z zakresu przepisów bezpieczeństwa;
  - 8) reprezentowania Polski przed odpowiednimi organami organizacji międzynarodowych oraz krajowymi władzami bezpieczeństwa innych państw, w tym koordynowania współpracy zagranicznej w zakresie ochrony informacji niejawnych;
  - 9) wykonywania innych zadań zastrzeżonych do jej kompetencji przez odpowiednie regulacje międzynarodowe.
3. W zakresie niezbędnym do wykonywania zadań, o których mowa w ust. 2, Szef ABW lub upoważnieni przez niego funkcjonariusze ABW mają prawo do:
  - 1) wglądu w dokumenty związane z ochroną informacji niejawnych;
  - 2) wstępu do obiektów i pomieszczeń przeznaczonych do przetwarzania informacji niejawnych;

- 3) dostępu do systemów teleinformatycznych przeznaczonych do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych;
  - 4) uzyskiwania wyjaśnień i informacji.
4. Zadania i uprawnienia krajowej władzy bezpieczeństwa w odniesieniu do podmiotów, o których mowa w art. 10 ust. 2, są realizowane za pośrednictwem Szefa SKW lub upoważnionych przez niego żołnierzy i funkcjonariuszy SKW.
5. W zakresie niezbędnym do wykonywania zadań, o których mowa w ust. 2, Szef ABW zwraca się do Szefa SKW o:
- 1) udostępnienie koniecznych informacji w celu koordynacji działań w zakresie właściwego reprezentowania Rzeczypospolitej Polskiej przed organami organizacji międzynarodowych i krajowych władz bezpieczeństwa innych państw;
  - 2) udzielenie niezbędnych wyjaśnień w celu wypełniania zadań ewidencyjnych, analitycznych i innych właściwych krajowej władzy bezpieczeństwa;
  - 3) podjęcie odpowiednich działań w celu zapewnienia jednolitości i zgodności systemu ochrony informacji niejawnych z odpowiednimi przepisami bezpieczeństwa.
6. Szef ABW, w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa, współpracuje z Szefem SKW; współpraca ta polega w szczególności na:
- 1) wymianie doświadczeń i informacji;
  - 2) organizacji wspólnych odpraw, szkoleń, konferencji itp.;
  - 3) wzajemnym umożliwieniu obecności upoważnionych żołnierzy lub funkcjonariuszy przy podejmowaniu niektórych czynności;
  - 4) uzgadnianiu działań, stanowisk i opinii;
  - 5) wspólnym opracowywaniu materiałów szkoleniowych;
  - 6) współdziałaniu w zakresie dystrybucji materiałów kryptograficznych.
7. Prezes Rady Ministrów może określić w drodze rozporządzenia tryb i sposób realizowania zadań krajowej władzy bezpieczeństwa oraz tryb i sposób współpracy Szefa ABW i Szefa SKW w tym zakresie.
8. W rozporządzeniu, o którym mowa w ust. 7, Prezes Rady Ministrów uwzględni potrzebę standaryzacji, w szczególności w zakresie:
- 1) procedur akredytacji kancelarii tajnych i innych pomieszczeń, w których przetwarzane są informacje niejawne;
  - 2) inspekcji w podmiotach, w których przetwarzane są informacje niejawne;
  - 3) obiegu informacji niejawnych;
  - 4) prowadzenia szkoleń;

- 5) postępowań wyjaśniających w przypadkach naruszenia zasad bezpieczeństwa informacji niejawnych.

## **Art. 12**

1. W zakresie niezbędnym do kontroli stanu zabezpieczenia informacji niejawnych upoważnieni pisemnie funkcjonariusze albo żołnierze ABW lub SKW mają prawo do:
  - 1) swobodnego wstępu do obiektów i pomieszczeń jednostki kontrolowanej, gdzie informacje takie są przetwarzane;
  - 2) wglądu do dokumentów związanych z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej;
  - 3) żądania udostępnienia do kontroli systemów teleinformatycznych służących do przetwarzania tych informacji;
  - 4) przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji;
  - 5) żądania od kierowników i pracowników kontrolowanych jednostek organizacyjnych udzielania ustnych i pisemnych wyjaśnień;
  - 6) zasięgania, w związku z przeprowadzaną kontrolą, informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek;
  - 7) korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych;
  - 8) uczestniczenia w posiedzeniach kierownictwa, organów zarządzających lub nadzorczych, a także organów opiniodawczo-doradczych w sprawach dotyczących problematyki ochrony tych informacji w kontrolowanej jednostce organizacyjnej.
2. Jeżeli w czasie wykonywania kontroli, o której mowa w ust. 1 zostaną ustalone okoliczności wskazujące na możliwość przetwarzania informacji niejawnych w systemach teleinformatycznych nie posiadających akredytacji bezpieczeństwa teleinformatycznego, funkcjonariusze lub żołnierze ABW albo SKW mogą żądać udostępnienia do kontroli systemów teleinformatycznych służących do przetwarzania innych, niż wymienione w ust. 1 informacji.

3. Postępowania, o których mowa w art. 3 podlegają kontroli w zakresie prawidłowości ich realizacji. Kontrole te prowadzą w odniesieniu do:
  - 1) postępowań zrealizowanych przez ABW i SKW, w tym przez pełnomocników ochrony w tych służbach – Prezes Rady Ministrów;
  - 2) postępowań zrealizowanych przez pozostałych pełnomocników ochrony, z wyłączeniem postępowań realizowanych przez AW oraz SWW - ABW lub SKW.
4. Do czynności, o których mowa w ust. 1 i 3, dokonywanych przez ABW lub SKW albo przez Prezesa Rady Ministrów, mają odpowiednie zastosowanie przepisy art. 30-41, art. 49-64 ust. 1 i art. 98 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.<sup>5</sup>), z tym że przewidziane w tej ustawie uprawnienia i obowiązki:
  - 1) Najwyższej Izby Kontroli - przysługują ABW i SKW albo Kancelarii Prezesa Rady Ministrów;
  - 2) Prezesa, Wiceprezesa i pracownika Najwyższej Izby Kontroli - przysługują odpowiednio Szefowi, Zastępcy Szefa i upoważnionemu funkcjonariuszowi ABW oraz Szefowi, Zastępcy Szefa i upoważnionemu żołnierzowi albo funkcjonariuszowi SKW albo Prezesowi Rady Ministrów lub upoważnionemu pracownikowi Kancelarii Prezesa Rady Ministrów.
5. Czynności, o których mowa w ust. 1 pkt 1-5 i 8, dokonywane przez ABW w stosunku do Sejmu Rzeczypospolitej Polskiej oraz Senatu Rzeczypospolitej Polskiej, wykonywane są w uzgodnieniu odpowiednio z Marszałkiem Sejmu Rzeczypospolitej Polskiej i Marszałkiem Senatu Rzeczypospolitej Polskiej. Uzgodnienia dokonuje Prezes Rady Ministrów, a w przypadku braku uzgodnienia czynność nie może być wykonana.
6. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób przygotowania i tryb przeprowadzania kontroli w zakresie ochrony informacji niejawnych, w tym uzgadniania kontroli w stosunku do Sejmu Rzeczypospolitej Polskiej i Senatu Rzeczypospolitej Polskiej.
7. W rozporządzeniu, o którym mowa w ust. 6, Prezes Rady Ministrów uwzględni zadania funkcjonariuszy ABW oraz żołnierzy i funkcjonariuszy SKW nadzorujących i wykonujących czynności kontrolne, dokumentowanie czynności kontrolnych oraz sporządzanie: protokołu kontroli, wystąpienia pokontrolnego i informacji o wynikach kontroli.

### **Art. 13**

1. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne odpowiada za ich ochronę.
2. Kierownicy jednostek organizacyjnych współdziałają ze służbami i organami uprawnionymi do prowadzenia poszerzonych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, a w szczególności udostępniają funkcjonariuszom, pracownikom albo żołnierzom tych organów, po przedstawieniu przez nich pisemnego upoważnienia, pozostające w ich dyspozycji informacje i dokumenty niezbędne do realizacji czynności określonych w ustawie.
3. Służby i organy uprawnione do prowadzenia poszerzonych postępowań sprawdzających, w zakresie koniecznym do wykonywania swoich zadań, w celu ochrony informacji niejawnych mogą zwracać się do innych instytucji, służb i organów o udzielenie niezbędnej pomocy przy wykonywaniu czynności w ramach prowadzonych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego.
4. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób przekazywania informacji, o których mowa w ust. 2 oraz sposób udzielania pomocy, o której mowa w ust. 3.
5. W rozporządzeniu, o którym mowa w ust. 4, określa się w szczególności:
  - 1) szczegółowy zakres i warunki przekazywania przez kierowników jednostek organizacyjnych służb i organów uprawnionych do prowadzenia poszerzonych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego informacji oraz udostępniania im dokumentów niezbędnych dla celów tych postępowań;
  - 2) szczegółowy zakres i warunki udzielania przez Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy inspekcji celnej i kontroli skarbowej niezbędnej pomocy służbom i organom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego informacji przy wykonywaniu czynności w ramach tych postępowań.

### **Art. 14**

1. Kierownikowi jednostki organizacyjnej podlega bezpośrednio pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony”, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

2. Pełnomocnikiem ochrony może być osoba, która posiada:
  - 1) obywatelstwo polskie;
  - 2) co najmniej średnie wykształcenie;
  - 3) odpowiednie poświadczenie bezpieczeństwa wydane przez ABW lub SKW, a także przez były UOP oraz były WSI;
  - 4) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych przeprowadzonym przez ABW lub SKW.
3. Kierownik jednostki organizacyjnej może powołać zastępcę lub zastępców pełnomocnika ochrony, z zastrzeżeniem spełnienia przez te osoby warunków, o których mowa w ust. 2.
4. Szczegółowy zakres czynności zastępcy pełnomocnika ochrony określa kierownik jednostki organizacyjnej.

### **Art. 15**

1. Pełnomocnik ochrony kieruje wyodrębnioną, wyspecjalizowaną komórką organizacyjną do spraw ochrony informacji niejawnych, zwaną dalej „pionem ochrony”, do której zadań należy:
  - 1) zapewnienie ochrony informacji niejawnych, w tym ich ochrony fizycznej;
  - 2) zapewnienie ochrony systemów teleinformatycznych, w których przetwarzane są informacje niejawne;
  - 3) szacowanie ryzyka dla bezpieczeństwa przetwarzanych informacji niejawnych oraz zarządzanie tym ryzykiem;
  - 4) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz w roku) kontrola ewidencji, materiałów i obiegu dokumentów;
  - 5) opracowywanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej (także w razie wprowadzenia stanu nadzwyczajnego) i nadzorowanie jego realizacji;
  - 6) szkolenie pracowników w zakresie ochrony informacji niejawnych;
  - 7) prowadzenie postępowań sprawdzających;
  - 8) prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących prace zlecane, które posiadają uprawnienia do dostępu do informacji niejawnych oraz osób, którym odmówiono wydania lub cofnięto poświadczenie bezpieczeństwa;

- 9) przekazywanie ABW lub SKW danych, o których mowa w art. 69 ust. 2 osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, na podstawie wykazu, o którym mowa w pkt 8, do ewidencji, o których mowa w art. 71 ust. 1;
  - 10) obowiązek, o którym mowa w pkt 9 nie dotyczy pionów ochrony w służbach i organach uprawnionych do realizacji poszerzonych postępowań sprawdzających.
2. Kierownik jednostki organizacyjnej może powierzyć pełnomocnikowi ochrony wykonywanie innych zadań, o ile ich realizacja nie naruszy prawidłowego wykonywania zadań, o których mowa w ust. 1.

#### **Art. 16**

Pracownikiem pionu ochrony w jednostce organizacyjnej może być osoba, która posiada:

- 1) obywatelstwo polskie z zastrzeżeniem art. 21 ust. 3 pkt 3;
- 2) odpowiednie poświadczenie bezpieczeństwa z zastrzeżeniem art. 21 ust. 4 oraz art. 50 ust. 3;
- 3) zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.

#### **Art. 17**

1. W przypadku naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych, pełnomocnik ochrony zawiadamia o tym kierownika jednostki organizacyjnej i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia.
2. W przypadku naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą „poufne” lub wyższą, pełnomocnik ochrony informuje niezwłocznie również ABW lub SKW.

#### **Art. 18**

1. W jednostkach organizacyjnych, o których mowa w art. 1 ust. 2 pkt 2, pełnomocnik ochrony zapewnia ochronę fizyczną tych jednostek.

2. Minister Obrony Narodowej określi, w drodze rozporządzenia, szczegółowe zadania pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych jemu podległych i przez niego nadzorowanych.
3. Wydając rozporządzenie, o którym mowa w ust. 2, Minister Obrony Narodowej uwzględni w szczególności zadania dotyczące:
  - 1) koordynowania oraz nadzorowania działalności pionów ochrony przez pełnomocników ochrony bezpośrednio nadrzędnych jednostek organizacyjnych;
  - 2) sposób współdziałania, w zakresie ochrony informacji niejawnych z właściwymi jednostkami organizacyjnymi Służby Kontrwywiadu Wojskowego;
  - 3) organizowania szkoleń z zakresu ochrony obiektów pod względem ochrony informacji niejawnych;
  - 4) szczególne wymagania w zakresie ochrony fizycznej i technicznej jednostek organizacyjnych;
  - 5) sposób opracowywania oraz podstawowe wymagania, jakim powinny odpowiadać plany ochrony jednostek organizacyjnych, niezbędne elementy planów ochrony, sposób nadzorowania ich realizacji oraz podział stref ochronnych na rodzaje i warunki dostępu do tych stref;
  - 6) sposób opracowania i wdrożenia planu postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne” w razie wprowadzenia stanu nadzwyczajnego.

## **Rozdział 4**

### **Szkolenia w zakresie ochrony informacji niejawnych**

#### **Art. 19**

1. Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania z:
  - 1) przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych;

- 2) zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby;
  - 3) sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.
2. Szkolenie, o którym mowa w ust. 1 przeprowadzają:
    - 1) ABW lub SKW - wobec pełnomocników ochrony i ich zastępców;
    - 2) ABW lub SKW - wspólnie z pełnomocnikiem ochrony wobec kierownika jednostki organizacyjnej, w której przetwarzane są informacje niejawne o klauzuli „ściśle tajne” i „tajne”;
    - 3) pełnomocnik ochrony - w stosunku do pozostałych osób zatrudnionych, pełniących służbę lub wykonujących prace zlecone w jednostce organizacyjnej.
  3. Szkolenie przeprowadza się nie rzadziej niż raz na 5 lat. Można odstąpić od przeprowadzenia szkolenia, jeśli osoba podejmująca pracę lub rozpoczynająca wykonywanie prac zleconych przedstawi pełnomocnikowi ochrony aktualne zaświadczenie o odbyciu szkolenia.
  4. Koszty szkolenia przeprowadzanego przez podmioty, o których mowa w ust. 2 pkt 1 i 2 pokrywa jednostka organizacyjna, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje prace zlecone.
  5. Wzajemne prawa i obowiązki organizatora i uczestnika szkolenia, o którym mowa w ust. 2 pkt 1 i 2 określa umowa zawarta między organizatorem a jednostką organizacyjną, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje prace zlecone.

## **Art. 20**

1. Szkolenie, o którym mowa w art. 19 ust. 1 kończy się wydaniem zaświadczenia. Potwierdzenie odbioru tego zaświadczenia stanowi jednocześnie potwierdzenie faktu zapoznania się z przepisami dotyczącymi ochrony informacji niejawnych.
2. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych, z uwzględnieniem odrębności wynikających z wydawania zaświadczeń przez ABW i SKW oraz pełnomocników ochrony, a także wysokość opłat za szkolenie.

## **Rozdział 5**

### **Bezpieczeństwo osobowe**

#### **Art. 21**

1. Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac, związanych z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej, może nastąpić, z zastrzeżeniem art. 22, po:
  - 1) przeprowadzeniu postępowania sprawdzającego;
  - 2) przeszkoleniu w zakresie ochrony informacji niejawnych.
2. Nie mogą być dopuszczone do pracy lub pełnienia służby na stanowisku albo do wykonywania prac zleconych, z którymi łączy się dostęp do informacji niejawnych o klauzuli „tajne” i „ściśle tajne”, osoby nieposiadające obywatelstwa polskiego, z zastrzeżeniem ust. 3.
3. Wymogu określonego w ust. 2, nie stosuje się do osób:
  - 1) zajmujących stanowiska związane z kierowaniem, wykonaniem lub z bezpośrednią realizacją przez przedsiębiorcę umowy związanej z dostępem do informacji niejawnych, zwaną dalej umową, albo wykonujących zadania na rzecz obronności i bezpieczeństwa państwa, związane z dostępem do informacji niejawnych u przedsiębiorcy,
  - 2) które w imieniu podmiotu, o którym mowa w pkt. 1, uczestniczą w czynnościach zmierzających do zawarcia umowy, jeżeli czynności te związane są z dostępem do informacji niejawnych,
  - 3) zatrudnionych w pionie ochrony podmiotu, o którym mowa w pkt 1  
- z wyjątkiem osoby zajmującej stanowisko pełnomocnika ochrony oraz zastępcy pełnomocnika ochrony.
4. Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac, związanych z dostępem do informacji niejawnych o klauzuli „zastrzeżone”, wymaga przeszkolenia oraz pisemnego upoważnienia przez kierownika jednostki organizacyjnej.

#### **Art. 22**

1. Nie przeprowadza się postępowania sprawdzającego, jeżeli osoba, której ma dotyczyć to postępowanie, zwana dalej „osobą sprawdzaną”, przedstawi odpowiednie do

wymaganej klauzuli tajności poświadczenie bezpieczeństwa, z wyjątkiem poświadczenia bezpieczeństwa wydanego przez organy, o których mowa w art. 24 ust. 4 pkt 1 i 6.

2. O zatrudnieniu na stanowisku, z którym może łączyć się dostęp do informacji niejawnych osoby, o której mowa w ust. 1, przedstawiającej odpowiednie poświadczenie bezpieczeństwa, kierownik jednostki organizacyjnej informuje w terminie 7 dni organ, który wydał poświadczenie bezpieczeństwa oraz ABW lub SKW.
3. Jeżeli z ratyfikowanych przez Rzeczpospolitą Polską umów międzynarodowych wynika obowiązek dopuszczenia do informacji niejawnych obywateli obcych państw mających wykonywać w Rzeczypospolitej Polskiej pracę w interesie innego państwa lub organizacji międzynarodowej, postępowania sprawdzającego nie przeprowadza się.
4. Szef Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu lub Prezesa Rady Ministrów albo minister właściwy dla określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego lub kierownik urzędu centralnego, a w przypadku ich braku ABW lub SKW, może wyrazić pisemną zgodę na udostępnienie informacji niejawnych o klauzuli „poufne” lub wyższej osobie, wobec której wszczęto postępowanie sprawdzające.
5. W szczególnie uzasadnionych przypadkach, z zastrzeżeniem art. 4. ust. 2, podmioty, o których mowa w ust. 4, mogą wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa.
6. W stanach nadzwyczajnych Prezydent Rzeczypospolitej Polskiej lub Prezes Rady Ministrów, każdy w swoim zakresie, może wyrazić zgodę na odstąpienie od przeprowadzenia postępowania sprawdzającego.
7. W przypadkach, o których mowa w ust. 4 - 6 informacje o udostępnieniu informacji niejawnych lub wyrażeniu zgody na odstąpienie od przeprowadzenia postępowania sprawdzającego przekazuje się ABW lub SKW.
8. Zgodę na udostępnienie informacji niejawnych oznaczonych klauzulą „poufne” osobie, wobec której wszczęto postępowanie sprawdzające, może wyrazić – w formie pisemnej – kierownik jednostki organizacyjnej, w której ta osoba jest zatrudniona, pełni służbę lub wykonuje prace zlecane.
9. Postępowania sprawdzającego nie przeprowadza się, z zastrzeżeniem ust. 10, wobec:
  - 1) Prezydenta Rzeczypospolitej Polskiej oraz osoby wybranej na urząd prezydenta;
  - 2) Marszałka Sejmu Rzeczypospolitej Polskiej;
  - 3) Marszałka Senatu Rzeczypospolitej Polskiej;

- 4) Prezesa Rady Ministrów;
  - 5) członka Rady Ministrów;
  - 6) Prezesa Narodowego Banku Polskiego;
  - 7) Prezesa Najwyższej Izby Kontroli;
  - 8) Rzecznika Praw Obywatelskich;
  - 9) Generalnego Inspektora Ochrony Danych Osobowych;
  - 10) członka Rady Polityki Pieniężnej;
  - 11) członka Krajowej Rady Radiofonii i Telewizji;
  - 12) Prezesa Instytutu Pamięci Narodowej – Komisji Badania Zbrodni przeciwko Narodowi Polskiemu;
  - 13) Szefa Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu i Prezesa Rady Ministrów;
  - 14) posła i senatora, z zastrzeżeniem ust. 11;
  - 15) sędziego oraz prokuratora i asesora prokuratury pełniącym czynności prokuratorskie, w stosunku do których zasady udostępniania informacji niejawnych regulują przepisy o ustroju sądów powszechnych, o ustroju sądów wojskowych oraz o prokuraturze.
10. W stosunku do osób zajmujących lub kandydujących na stanowiska, o których mowa w ust. 9 pkt 6-15, ubiegających się o dostęp do informacji niejawnych organizacji międzynarodowych lub jeżeli dostęp taki ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską, wyłączenia, o którym mowa w ust. 9, nie stosuje się.
11. W stosunku do kandydatów na stanowiska, o których mowa w ust. 9 pkt 6-14, a także w stosunku do posłów lub senatorów, ubiegających się o dostęp do informacji niejawnych organizacji międzynarodowych lub jeżeli dostęp taki ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską, na wniosek organu uprawnionego do powołania na to stanowisko, ABW lub SKW przeprowadzają poszerzone postępowanie sprawdzające. Jeżeli do powołania jest uprawniony Sejm albo Senat, z wnioskiem tym występuje odpowiednio Marszałek Sejmu albo Marszałek Senatu. Postępowanie to powinno być zakończone przed upływem 14 dni od dnia złożenia wniosku o przeprowadzenie tego postępowania wraz z wypełnioną ankietą
12. Marszałek Sejmu lub Marszałek Senatu zwracają się do ABW o przeprowadzenie poszerzonego postępowania sprawdzającego wobec posła lub senatora, którego obowiązki

poselskie bądź senatorskie wymagają dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne”.

13. W przypadku odmowy wydania poświadczenia bezpieczeństwa osobie, o której mowa w ust. 11-12, Prezes Rady Ministrów przedstawia informację o powodach tej odmowy Marszałkowi Sejmu, jeżeli odmowa dotyczy posła albo Marszałkowi Senatu, jeżeli odmowa dotyczy senatora.
14. Prezydent Rzeczypospolitej Polskiej, Prezes Rady Ministrów oraz Marszałek Sejmu i Marszałek Senatu zapoznają się z przepisami o ochronie informacji niejawnych i składają oświadczenie o znajomości tych przepisów.

### **Art. 23**

1. W zależności od stanowiska lub zleconej pracy, o które ubiega się dana osoba przeprowadza się:
  - 1) zwykłe postępowanie sprawdzające – w przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „poufne”, z zastrzeżeniem pkt 2 lit. b-d;
  - 2) poszerzone postępowanie sprawdzające:
    - a) przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „tajne” lub „ściśle tajne”;
    - b) wobec pełnomocników ochrony, zastępców pełnomocników ochrony oraz kandydatów na te stanowiska;
    - c) wobec kierowników przedsiębiorców;
    - d) wobec osób ubiegających się o dostęp do informacji niejawnych organizacji międzynarodowych lub jeżeli dostęp taki ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską.
2. W odniesieniu do osób wskazanych w ust. 1 pkt 2 lit. b - d wydaje się poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o takiej klauzuli, jaka została wskazana we wniosku lub poleceniu.

### **Art. 24**

1. Zwykłe postępowanie sprawdzające przeprowadza pełnomocnik ochrony na pisemne polecenie kierownika jednostki organizacyjnej.
2. Na wniosek podmiotu określonego art. 21 ust. 3 pkt 1, zwykłe postępowanie sprawdzające wobec osób określonych w art. 21 ust. 3, może przeprowadzić pełnomocnik

ochrony jednostki organizacyjnej, która zawiera umowę lub zleca zadanie, z wykonaniem których łączy się dostęp do informacji niejawnych o klauzuli „poufne”. Wniosek ten przedsiębiorca składa do kierownika jednostki organizacyjnej, która zawiera z nim umowę lub zleca zadanie.

3. Na pisemny wniosek osoby uprawnionej na podstawie odrębnych przepisów do obsady stanowiska lub zlecenia prac, w tym także kierownika jednostki organizacyjnej, poszerzone postępowania sprawdzające, z zastrzeżeniem postępowań, o których mowa w ust. 4, przeprowadzają ABW lub SKW.
4. Samodzielne postępowania sprawdzające wobec własnych pracowników, funkcjonariuszy, żołnierzy oraz osób ubiegających się o przyjęcie do służby lub pracy, przeprowadzają:
  - 1) Agencja Wywiadu;
  - 2) Biuro Ochrony Rządu;
  - 3) Centralne Biuro Antykorupcyjne;
  - 4) Policja;
  - 5) Służba Więzienna;
  - 6) Służba Wywiadu Wojskowego;
  - 7) Straż Graniczna;
  - 8) Żandarmeria Wojskowa.

#### **Art. 25**

1. Postępowanie sprawdzające ma na celu ustalenie czy osoba sprawdzana daje rękojmię zachowania tajemnicy.
2. W toku postępowania sprawdzającego ustala się czy istnieją wątpliwości dotyczące:
  - 1) uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko Rzeczypospolitej Polskiej;
  - 2) zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu;
  - 3) przestrzegania porządku konstytucyjnego Rzeczypospolitej Polskiej, a przede wszystkim czy osoba sprawdzana uczestniczyła lub uczestniczy, współpracowała lub współpracuje z partiami politycznymi albo innymi organizacjami, o których mowa w art. 13 Konstytucji Rzeczypospolitej Polskiej;

- 4) ukrywania lub niezgodnego z prawdą podawania w ankiecie bezpieczeństwa osobowego lub postępowaniu sprawdzającym przez osobę sprawdzaną informacji mających znaczenie dla ochrony informacji niejawnych;
  - 5) występowania związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji;
  - 6) niewłaściwego postępowania z informacjami niejawnymi, jeżeli:
    - a) doprowadziło bezpośrednio do ujawnienia tych informacji osobom nieuprawnionym,
    - b) było wynikiem celowego działania,
    - c) stwarzało realne zagrożenie ich nieuprawnionego ujawnienia i nie miało charakteru incydentalnego,
    - d) dopuściła się go osoba szczególnie zobowiązana na podstawie ustawy do ochrony informacji niejawnych;
  - 7) informacji o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do zajmowania stanowiska albo wykonywania prac związanych z dostępem do informacji niejawnych;
  - 8) uzależnienia od alkoholu lub narkotyków.
3. W toku poszerzonego postępowania sprawdzającego ustala się ponadto, czy istnieją wątpliwości związane z wyraźną różnicą między poziomem życia osoby sprawdzanej, a uzyskiwanymi przez nią dochodami.
  4. W razie nie dających się usunąć wątpliwości, o których mowa w ust. 2 lub 3, interes ochrony informacji niejawnych ma pierwszeństwo przed innymi prawnie chronionymi interesami.
  5. Organ prowadzący postępowanie sprawdzające, kierując się zasadami bezstronności i obiektywizmu, jest obowiązany do wykazania najwyższej staranności w toku prowadzonego postępowania sprawdzającego, co do jego zgodności z przepisami ustawy.
  6. Wszystkie czynności przeprowadzone w toku postępowań sprawdzających muszą być rzetelnie udokumentowane i powinny być zakończone przed upływem 3 miesięcy – od daty pisemnego polecenia przeprowadzenia zwykłego postępowania sprawdzającego lub złożenia wniosku o przeprowadzenie postępowania sprawdzającego wraz z wypełnioną ankietą bezpieczeństwa osobowego, zwaną dalej „ankietą”.
  7. Przeprowadzenie postępowania sprawdzającego wymaga pisemnej zgody osoby, której ma dotyczyć.

8. Ustawa zezwala w zakresie niezbędnym dla ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, na zbieranie i przetwarzanie informacji o osobach trzecich, określonych w ankiecie bezpieczeństwa osobowego, bez wiedzy i zgody tych osób.
9. Wzór ankiety wraz z instrukcją jej wypełnienia stanowi załącznik do ustawy.

## **Art. 26**

1. Zwykłe postępowanie sprawdzające obejmuje:
  - 1) sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, a w szczególności Krajowym Rejestrze Karnym, danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie, a także sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy;
  - 2) sprawdzenie w ewidencjach i kartotekach niedostępnych powszechnie, danych zawartych w ankiecie oraz innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.
2. Sprawdzenie, o którym mowa w ust. 1 pkt 2, jest prowadzone na pisemny wniosek pełnomocnika ochrony przez ABW lub SKW.
3. W toku sprawdzenia, o którym mowa w ust. 1 pkt 2, ABW lub SKW ma prawo przeprowadzić rozmowę z osobą sprawdzaną w celu usunięcia nieścisłości lub sprzeczności zawartych w uzyskanych informacjach.
4. ABW lub SKW przekazuje pełnomocnikowi ochrony pisemną informację o wynikach czynności, o których mowa w ust. 1 pkt 2 oraz w ust. 3.
5. Jeżeli jest to konieczne na podstawie uzyskanych informacji, zwykłe postępowanie sprawdzające obejmuje ponadto rozmowę z osobą sprawdzaną.
6. Jeżeli w toku zwykłego postępowania sprawdzającego wystąpią wątpliwości nie pozwalające na ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, organ prowadzący postępowanie sprawdzające zapewnia osobie sprawdzanej, w trakcie wysłuchania, możliwość osobistego ustosunkowania się do informacji wywołujących te wątpliwości. Osoba ta może stawić się na wysłuchanie ze swoim pełnomocnikiem.
7. Organ prowadzący zwykłe postępowanie sprawdzające odstępuje od przeprowadzenia czynności, o której mowa w ust. 6, jeżeli:

- 1) jej przeprowadzenie wiązałoby się z ujawnieniem informacji niejawnych;
  - 2) postępowanie sprawdzające doprowadziło do nie budzącego wątpliwości ustalenia, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy .
8. W celu dokonania ustaleń, o których mowa w art. 25 ust. 2 pkt 7-8, organ prowadzący zwykłe postępowanie sprawdzające może zobowiązać osobę sprawdzaną do poddania się specjalistycznym badaniom oraz udostępnienia wyników tych badań. Lekarzowi przeprowadzającemu to badanie udostępnia się dokumentację medyczną osoby sprawdzanej, w zakresie dotyczącym zdiagnozowania wątpliwości, o których mowa w art. 25 ust. 2 pkt 7-8.

### **Art. 27**

1. Poszerzone postępowanie sprawdzające obejmuje czynności, o których mowa w art. 26 ust. 1 pkt 1-2, a ponadto, jeżeli jest to konieczne na podstawie uzyskanych informacji, postępowanie to obejmuje:
  - 1) rozmowę z przełożonymi osoby sprawdzanej oraz z innymi osobami;
  - 2) przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej;
  - 3) sprawdzenie stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, a w szczególności wobec Skarbu Państwa.
2. Do czynności, o której mowa w ust. 1 pkt 2, przepisy Kodeksu postępowania karnego i wydane na jego podstawie przepisy dotyczące wywiadu środowiskowego stosuje się odpowiednio.
3. Czynności, o których mowa w ust. 1 pkt 3, są realizowane w trybie art. 104 ust. 2 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.<sup>6</sup>). Przepisy art. 82 § 1 i 2 oraz art. 182 ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2005 r. Nr 8, poz. 60 z późn. zm.<sup>7</sup>) oraz art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65 z późn. zm.<sup>8</sup>), stosuje się odpowiednio.
4. Do poszerzonego postępowania sprawdzającego przepisy art. 26 ust. 5 - 8, stosuje się odpowiednio.
5. W przypadku osób ubiegających się o uzyskanie dostępu do informacji o klauzuli „ściśle tajne”, poszerzone postępowanie sprawdzające obejmuje także, jeżeli jest to konieczne na podstawie uzyskanych wcześniej informacji, rozmowę z trzema osobami wskazanymi przez osobę sprawdzaną w celu potwierdzenia tożsamości tej osoby oraz innych informacji mogących mieć znaczenie dla oceny dawania rękojmi zachowania tajemnicy.

## **Art. 28**

1. Postępowanie sprawdzające może zostać zawieszono w przypadku:
  - 1) długotrwałej choroby osoby sprawdzanej, uniemożliwiającej skuteczne przeprowadzenie postępowania sprawdzającego;
  - 2) wyjazdu za granicę osoby sprawdzanej na okres przekraczający 30 dni;
  - 3) gdy ocena dawania rękojmi zachowania tajemnicy zależy od uprzedniego rozstrzygnięcia zagadnienia przez inny organ, w szczególności w przypadku wszczęcia przeciwko osobie sprawdzanej postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego;
  - 4) gdy przeprowadzenie skutecznego postępowania sprawdzającego nie jest możliwe z innych przyczyn niezależnych od organu je prowadzącego.
2. O zawieszeniu postępowania sprawdzającego organ je prowadzący zawiadamia wnioskodawcę, pełnomocnika ochrony i osobę sprawdzaną.
3. Postępowanie sprawdzające zostaje podjęte, jeżeli:
  - 1) ustąpiły przyczyny uzasadniające zawieszenie postępowania;
  - 2) ujawniono okoliczności mogące stanowić podstawę do odmowy wydania poświadczenia bezpieczeństwa lub umorzenia postępowania sprawdzającego.
4. O podjęciu postępowania zawiadamia się osobę sprawdzaną, pełnomocnika ochrony oraz osobę uprawnioną do obsady stanowiska.

## **Art. 29**

Postępowanie sprawdzające kończy się:

- 1) wydaniem poświadczenia bezpieczeństwa;
- 2) odmową wydania poświadczenia bezpieczeństwa;
- 3) umorzeniem.

## **Art. 30**

1. Po zakończeniu postępowania sprawdzającego z wynikiem pozytywnym organ prowadzący postępowanie wydaje poświadczenie bezpieczeństwa i przekazuje osobie sprawdzanej, zawiadamiając o tym pełnomocnika ochrony oraz osobę uprawnioną do obsady stanowiska.
2. Poświadczenie bezpieczeństwa powinno zawierać:
  - 1) podstawę prawną;

- 2) wskazanie wnioskodawcy postępowania sprawdzającego;
  - 3) określenie organu, który przeprowadził postępowanie sprawdzające;
  - 4) datę i miejsce wystawienia;
  - 5) imię, nazwisko i datę urodzenia osoby sprawdzanej;
  - 6) rodzaj przeprowadzonego postępowania sprawdzającego ze wskazaniem klauzuli tajności informacji niejawnych, do których osoba sprawdzana może mieć dostęp;
  - 7) stwierdzenie wydania poświadczenia bezpieczeństwa;
  - 8) termin ważności;
  - 9) imienną pieczęć i czytelny podpis upoważnionego funkcjonariusza lub żołnierza ABW lub SKW albo pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające.
3. Poświadczenie bezpieczeństwa wydaje się na okres:
    - 1) 10 lat – w przypadku dostępu do informacji niejawnych, oznaczonych klauzulą „poufne”;
    - 2) 7 lat – w przypadku dostępu do informacji niejawnych, oznaczonych klauzulą „tajne”;
    - 3) 5 lat – w przypadku dostępu do informacji niejawnych, oznaczonych klauzulą „ściśle tajne”.
  4. Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych wyższą klauzulą tajności uprawnia do dostępu do informacji niejawnych oznaczonych niższą klauzulą tajności, odpowiednio przez okresy, o których mowa w ust. 3, z uwzględnieniem poświadczeń bezpieczeństwa organizacji międzynarodowych.
  5. Poświadczenia bezpieczeństwa wydane przez służby lub organy, o których mowa w art. 24 ust. 4 pkt 1 i 6 zachowują ważność wyłącznie w okresie pracy lub służby w organie, który przeprowadził postępowanie sprawdzające.
  6. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory poświadczenia bezpieczeństwa, z uwzględnieniem składników, o których mowa w ust. 2.

### **Art. 31**

1. Organ prowadzący postępowanie odmawia wydania poświadczenia bezpieczeństwa, jeżeli nie zostaną usunięte wątpliwości, o których mowa w art. 25 ust. 2, a także, jeżeli w trakcie poszerzonego postępowania sprawdzającego nie zostaną ponadto usunięte wątpliwości, o których mowa w art. 25 ust. 3.

2. Organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa, jeżeli osoba sprawdzana została skazana prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, jeżeli fakt skazania wywołuje wątpliwości, o których mowa w art. 25 ust. 2 i 3.
3. Decyzja o odmowie wydania poświadczenia bezpieczeństwa powinna zawierać:
  - 1) podstawę prawną oraz uzasadnienie faktyczne i prawne;
  - 2) wskazanie wnioskodawcy postępowania sprawdzającego;
  - 3) określenie organu, który przeprowadził postępowanie sprawdzające;
  - 4) datę i miejsce wystawienia;
  - 5) imię, nazwisko i datę urodzenia osoby sprawdzanej;
  - 6) wskazanie rodzaju przeprowadzonego postępowania sprawdzającego ze wskazaniem klauzuli informacji niejawnych, do których osoba sprawdzana miała mieć dostęp;
  - 7) stwierdzenie odmowy wydania poświadczenia bezpieczeństwa;
  - 8) imienną pieczęć i czytelny podpis, w zależności od rodzaju postępowania sprawdzającego, pełnomocnika ochrony albo upoważnionego pracownika, funkcjonariusza lub żołnierza organu albo służby upoważnionej do prowadzenia postępowania sprawdzającego;
  - 9) pouczenie o dopuszczalności i terminie wniesienia odwołania, odpowiednio, do Prezesa Rady Ministrów albo Szefa ABW lub Szefa SKW.
4. Można odstąpić od uzasadnienia faktycznego decyzji lub je ograniczyć w zakresie, w jakim wiązałyby się to z udostępnieniem osobie sprawdzanej informacji niejawnych.
5. Po zakończeniu postępowania sprawdzającego z wynikiem negatywnym organ prowadzący postępowanie wydaje decyzję o odmowie wydania poświadczenia bezpieczeństwa i doręcza tę odmowę osobie sprawdzanej, zawiadamiając o tym osobę uprawnioną do obsady stanowiska oraz pełnomocnika ochrony.
6. Osoba uprawniona do obsady stanowiska jest obowiązana, niezwłocznie po otrzymaniu zawiadomienia o odmowie wydania poświadczenia bezpieczeństwa w zakresie dostępu do informacji niejawnych uniemożliwić dostęp do informacji niejawnych osobie, której odmowa dotyczy.
7. Postępowanie sprawdzające wobec osoby, której odmówiono wydania poświadczenia bezpieczeństwa, można przeprowadzić najwcześniej po roku od daty odmowy wydania poświadczenia bezpieczeństwa.

8. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory decyzji o odmowie wydania poświadczenia bezpieczeństwa, z uwzględnieniem składników decyzji, o których mowa w ust. 3.

### **Art. 32**

1. Umorzenie postępowania sprawdzającego następuje w przypadku:
  - 1) śmierci osoby sprawdzanej;
  - 2) rezygnacji osoby sprawdzanej z ubiegania się albo zajmowania stanowiska lub wykonywania pracy, łączących się z dostępem do informacji niejawnych;
  - 3) odstąpienia przez kierownika jednostki od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac związanych z dostępem do informacji niejawnych;
  - 4) gdy postępowanie z jakiegokolwiek innej przyczyny stało się bezprzedmiotowe.
2. O umorzeniu postępowania sprawdzającego organ je prowadzący zawiadamia wnioskodawcę, pełnomocnika ochrony oraz, w przypadkach, o których mowa w ust. 1 pkt 2-4, osobę sprawdzaną.

### **Art. 33**

1. Na pisemny wniosek osoby uprawnionej do obsady stanowiska złożony co najmniej na 6 miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa właściwy organ przeprowadza kolejne postępowanie sprawdzające.
2. Do kolejnego postępowania sprawdzającego stosuje się przepisy ustawy odnoszące się do właściwego postępowania sprawdzającego, z uwzględnieniem ust. 3 i 4.
3. Kolejne postępowanie sprawdzające powinno być zakończone przed upływem terminu ważności poświadczenia bezpieczeństwa. Termin, o którym mowa w art. 25 ust. 6, nie ma zastosowania.
4. Jeżeli wobec osoby posiadającej ważne poświadczenie bezpieczeństwa, wydane przez ABW lub SKW, zostanie skierowany wniosek o przeprowadzenie postępowania sprawdzającego przed wydaniem poświadczenia bezpieczeństwa organizacji międzynarodowej, wypełnienie ankiety bezpieczeństwa osobowego nie jest wymagane, a poświadczenie bezpieczeństwa organizacji międzynarodowej jest wydawane jedynie na okres ważności posiadanego przez tę osobę poświadczenia bezpieczeństwa.

#### **Art. 34**

1. W przypadku, gdy w odniesieniu do osoby, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy, przeprowadza się kontrolne postępowanie sprawdzające z pominięciem terminu, o którym mowa w art. 25 ust. 6 i bez wypełnienia nowej ankiety bezpieczeństwa osobowego przez osobę sprawdzaną.
2. Postępowanie, o którym mowa w ust. 1 przeprowadza organ właściwy do przeprowadzenia kolejnego postępowania sprawdzającego, z zastrzeżeniem ust. 3
3. W przypadkach uzasadnionych względami bezpieczeństwa państwa kontrolne postępowanie sprawdzające może zostać przeprowadzone przez ABW lub SKW.
4. W celu weryfikacji informacji, o których mowa w ust. 1, właściwy organ może przeprowadzić niezbędne czynności sprawdzające. Pełnomocnik ochrony może przeprowadzić w tym trybie czynności, o których mowa w art. 26 ust. 1 pkt 1, a organy uprawnione do prowadzenia poszerzonych postępowań sprawdzających także czynności, o których mowa w art. 26 ust. 1 pkt 2 ustawy. Czynności te muszą być rzetelnie udokumentowane i prowadzone zgodnie z zasadami bezstronności, obiektywizmu i wykazania najwyższej staranności. Dokumentację tych czynności dołącza się do akt postępowania sprawdzającego.
5. O wszczęciu kontrolnego postępowania sprawdzającego zawiadamia się:
  - 1) kierownika jednostki organizacyjnej lub osobę uprawnioną do obsady stanowiska;
  - 2) pełnomocnika ochrony w jednostce organizacyjnej;
  - 3) osobę sprawdzaną.
6. Po otrzymaniu zawiadomienia, o którym mowa w ust. 5, kierownik jednostki organizacyjnej lub osoba uprawniona do obsady stanowiska wyłącza osobie sprawdzanej dostęp do informacji niejawnych.
7. Do kontrolnego postępowania sprawdzającego stosuje się przepisy art. 25 - 28, art. 31, art. 32 ust. 1 pkt 1 i 4 oraz art. 32 ust. 2, z uwzględnieniem ust. 6-8 oraz art. 35, 36, 37 i 38.
8. Kontrolne postępowanie sprawdzające kończy się:
  - 1) decyzją o cofnięciu poświadczenia bezpieczeństwa;
  - 2) poinformowaniem osób wymienionych w ust. 3 o braku zastrzeżeń w stosunku do osoby, którą objęto kontrolnym postępowaniem sprawdzającym,

z jednoczesnym potwierdzeniem dalszej jej zdolności do zachowania tajemnicy w zakresie określonym w posiadanym przez nią poświadczeniu bezpieczeństwa.

9. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory decyzji o cofnięciu poświadczenia bezpieczeństwa, z uwzględnieniem składników decyzji, o których mowa w art. 31 ust. 3.

## **Rozdział 6**

### **Postępowanie odwoławcze i skargowe**

#### **Art. 35**

1. Od decyzji o odmowie wydania poświadczenia bezpieczeństwa albo o umorzeniu postępowania sprawdzającego, wydanej przez ABW, SKW albo przez służby i organy, o których mowa w art. 24 ust. 4, osobie sprawdzanej służby odwołanie do Prezesa Rady Ministrów; odwołanie nie wymaga uzasadnienia.
2. Odwołanie wnosi się w terminie 14 dni od dnia doręczenia osobie sprawdzanej decyzji, o której mowa w ust. 1, za pośrednictwem organu, który przeprowadził postępowanie sprawdzające.
3. ABW, SKW oraz służby i organy, o których mowa w art. 24 ust. 4, są zobowiązane przesłać odwołanie wraz z aktami postępowania sprawdzającego Prezesowi Rady Ministrów w terminie 14 dni od dnia, w którym otrzymały odwołanie.
4. Rozpatrzenie odwołania powinno nastąpić nie później niż w ciągu 3 miesięcy od dnia otrzymania odwołania.

#### **Art. 36**

1. Prezes Rady Ministrów stwierdza, w drodze postanowienia:
  - 1) niedopuszczalność odwołania;
  - 2) uchybienie terminu do wniesienia odwołania.
2. Postanowienie w tej sprawie jest ostateczne i powinno zawierać:
  - 1) datę wydania;
  - 2) oznaczenie osoby sprawdzanej;
  - 3) powołanie podstawy prawnej;
  - 4) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne;

- 5) pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego.
3. Prezes Rady Ministrów może na żądanie osoby sprawdzanej lub z urzędu zlecić właściwemu organowi lub służbie przeprowadzenie dodatkowych czynności w celu uzupełnienia dowodów i materiałów w postępowaniu sprawdzającym.
4. Prezes Rady Ministrów wydaje decyzję, w której:
  - 1) utrzymuje w mocy decyzję organu, który przeprowadził postępowanie sprawdzające;
  - 2) uchyla decyzję organu, który przeprowadził postępowanie sprawdzające;
  - 3) uchyla decyzję organu, który przeprowadził postępowanie sprawdzające i nakazuje mu wydanie poświadczenia bezpieczeństwa;
  - 4) uchyla decyzję organu, który przeprowadził postępowanie sprawdzające i przekazuje sprawę do ponownego rozpatrzenia;
  - 5) stwierdza nieważność decyzji organu, który przeprowadził postępowanie sprawdzające.
5. Decyzja powinna zawierać:
  - 1) datę wydania;
  - 2) oznaczenie osoby sprawdzanej;
  - 3) powołanie podstawy prawnej;
  - 4) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne;
  - 5) pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego.
6. Po wydaniu decyzji lub postanowienia Prezes Rady Ministrów niezwłocznie zwraca właściwemu organowi akta, o których mowa w art. 35 ust. 3.
7. Decyzje i postanowienia doręcza się na piśmie osobie sprawdzanej i właściwemu organowi, zawiadamiając o rozstrzygnięciu zawartym w decyzji lub postanowieniu osobę uprawnioną do obsady stanowiska.
8. Do postępowania odwoławczego przepisy art. 27, art. 30 ust. 5 oraz art. 31 stosuje się odpowiednio.

### **Art. 37**

1. Od wydanej przez pełnomocnika ochrony decyzji o odmowie wydania poświadczenia bezpieczeństwa albo o umorzeniu postępowania sprawdzającego w wyniku zwykłego postępowania sprawdzającego osobie sprawdzanej służy, z wyłączeniem postępowań

sprawdzających, prowadzonych w trybie art. 24 ust. 4, odwołanie odpowiednio do Szefa ABW lub Szefa SKW.

2. Do postępowania odwoławczego przed Szefem ABW lub Szefem SKW stosuje się odpowiednio przepisy ustawy dotyczące postępowania odwoławczego przed Prezesem Rady Ministrów, z zastrzeżeniem ust. 3.
3. Odwołanie do Szefa ABW lub Szefa SKW składa się za pośrednictwem pełnomocnika ochrony, który odmówił wydania poświadczenia bezpieczeństwa albo umorzył postępowanie sprawdzające.

### **Art. 38**

1. Osobie sprawdzanej przysługuje skarga do sądu administracyjnego na decyzję lub postanowienie organu odwoławczego w terminie 30 dni od dnia doręczenia.
2. Sąd administracyjny rozpatruje skargę na posiedzeniu niejawnym.
3. Wyrok wydany na posiedzeniu niejawnym uzasadnia się tylko w przypadku uwzględnienia skargi. Odpis wyroku z uzasadnieniem doręcza się tylko właściwemu organowi odwoławczemu. Skarżącemu oraz osobie uprawnionej do obsady stanowiska doręcza się odpis wyroku.
4. Po wydaniu wyroku sąd administracyjny niezwłocznie zwraca akta postępowania sprawdzającego właściwemu organowi odwoławczemu.
5. Do skargi kasacyjnej stosuje się odpowiednio ust. 2 i 3.

## **Rozdział 7**

### **Kancelarie tajne. Środki bezpieczeństwa fizycznego**

### **Art. 39**

1. Jednostka organizacyjna, w której są przetwarzane informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne” organizuje kancelarię, zwaną dalej „kancelarią tajną”.
2. W przypadku uzasadnionym względami organizacyjnymi kierownik jednostki organizacyjnej może utworzyć więcej niż jedną kancelarię tajną.
3. W uzasadnionych przypadkach, za zgodą odpowiednio ABW lub SKW, można zorganizować kancelarię tajną obsługującą dwie lub więcej jednostek organizacyjnych. Podległość, obsada i zasady finansowania takiej kancelarii mogą zostać określone w porozumieniu właściwych kierowników jednostek organizacyjnych.

4. Kancelaria tajna stanowi wyodrębnioną komórkę organizacyjną podległą bezpośrednio pełnomocnikowi ochrony, obsługiwana przez pracowników pionu ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie dokumentów niejawnych uprawnionym osobom.
5. Kierownik jednostki organizacyjnej informuje ABW lub SKW o utworzeniu i likwidacji kancelarii tajnej z określeniem, do jakiej klauzuli tajności mogą być w niej przechowywane dokumenty niejawne.

#### **Art. 40**

1. Organizacja pracy kancelarii tajnej zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się dokument niejawny o klauzuli „tajne” lub „ściśle tajne” pozostający w dyspozycji jednostki organizacyjnej oraz kto z tym dokumentem się zapoznał.
2. Przepis ust. 1 stosuje się odpowiednio do organizacji pracy komórek organizacyjnych, w których rejestrowane są dokumenty oznaczone klauzulą „poufne”.
3. Kierownik jednostki organizacyjnej zatwierdza, opracowane przez pełnomocnika ochrony, zasady obiegu informacji niejawnych oznaczonych klauzulą "poufne" w podległych komórkach organizacyjnych.
4. Dokumenty niejawne mogą być wydawane poza kancelarię tajną na czas niezbędny do pracy z dokumentem, jeżeli odbiorca zapewnia warunki ochrony takich dokumentów przed nieuprawnionym ujawnieniem. W razie braku możliwości zapewnienia warunków ochrony, dokument może być udostępniony wyłącznie w kancelarii tajnej.
5. Kancelaria tajna odmawia udostępnienia lub wydania dokumentu, o którym mowa w art. 2 pkt 3, osobie nieuprawnionej.

#### **Art. 41**

1. W jednostkach organizacyjnych, o których mowa w art. 1 ust. 2 pkt 2 dopuszcza się organizowanie innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych.
2. Do komórek organizacyjnych, o których mowa w ust. 1, przepisy art. 39 ust. 1 i art. 40 stosuje się odpowiednio.

#### **Art. 42**

1. Jednostki organizacyjne, w których są przetwarzane informacje niejawne stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń, w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, a w szczególności przed:
  - 1) działaniem obcych służb specjalnych;
  - 2) zamachem terrorystycznym lub sabotażem;
  - 3) kradzieżą lub zniszczeniem materiału;
  - 4) próbą wejścia osób nieuprawnionych;
  - 5) nieuprawnionym dostępem pracowników do materiałów oznaczonych wyższą klauzulą tajności.
2. Zakres stosowania środków bezpieczeństwa fizycznego uzależnia się od poziomu zagrożeń nieuprawnionego dostępu do informacji niejawnych lub ich utraty.
3. Za określenie poziomu zagrożeń w odniesieniu do bezpieczeństwa informacji niejawnych odpowiada kierownik jednostki organizacyjnej, który zatwierdza odpowiednią dokumentację w zakresie bezpieczeństwa fizycznego.
4. W określeniu poziomu zagrożeń, o którym mowa w ust. 2, uwzględnia się w szczególności: występujące zagrożenia, klauzule tajności i ilość informacji niejawnych. W uzasadnionych przypadkach w określeniu poziomu zagrożeń uwzględnia się, wskazania ABW lub SKW.

#### **Art. 43**

W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych, należy w szczególności:

- 1) zorganizować strefy ochronne;
- 2) wprowadzić system kontroli określający uprawnienia do wejścia, przebywania i wyjścia ze stref ochronnych;
- 3) w pomieszczeniach, w których są przechowywane materiały niejawne, stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym na podstawie odrębnych przepisów przyznano certyfikaty lub świadectwa kwalifikacyjne.

#### **Art. 44**

1. Rada Ministrów określi, w drodze rozporządzenia, sposób przeprowadzania i podstawowe kryteria określania poziomu zagrożeń oraz dobór środków bezpieczeństwa fizycznego

właściwych do wskazanego poziomu zagrożeń, a także wymagania w zakresie organizacji i funkcjonowania kancelarii tajnych.

2. W rozporządzeniu, o którym mowa w ust. 1, Rada Ministrów uwzględni:
  - 1) rodzaje zagrożeń, które należy uwzględnić w określaniu poziomu zagrożeń;
  - 2) środki ochrony fizycznej;
  - 3) kryteria tworzenia stref ochronnych;
  - 4) strukturę organizacyjną kancelarii, z uwzględnieniem możliwości tworzenia jej oddziałów;
  - 5) podstawowe zadania kierownika kancelarii;
  - 6) tryb obiegu informacji niejawnych;
  - 7) wzór karty zapoznania z dokumentem;
  - 8) wzór dziennika ewidencji.
3. Ministrowie właściwi do spraw: wewnętrznych, administracji publicznej, zagranicznych, finansów publicznych, budżetu i instytucji finansowych, Minister Sprawiedliwości, Prezes Narodowego Banku Polskiego, Prezes Najwyższej Izby Kontroli, Pierwszy Prezes Sądu Najwyższego, Szefowie Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu oraz Prezesa Rady Ministrów, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Służby Kontrwywiadu Wojskowego, Szef Służby Wywiadu Wojskowego, Szef Centralnego Biura Antykorupcyjnego, Komendant Główny Policji, Komendant Główny Straży Granicznej, Szef Biura Ochrony Rządu, a także Prezes Instytutu Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, określą, w drodze zarządzenia, każdy w zakresie swojego działania, szczególny sposób organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych.
4. Minister Obrony Narodowej określi, w drodze zarządzenia, szczególny sposób organizacji kancelarii tajnych oraz komórek organizacyjnych, o których mowa w art. 41 ust. 1, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych.
5. Prezes Rady Ministrów określi, w drodze rozporządzenia, tryb i sposób nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów w celu ich zabezpieczenia przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem, a także obowiązki nadawców i przewoźników tych materiałów.
6. W rozporządzeniu, o którym mowa w ust. 5, Prezes Rady Ministrów uwzględni:
  - 1) obowiązki nadawców przesyłek zawierających informacje niejawne oraz wymogi, jakie muszą spełniać te przesyłki;

- 2) obowiązki podmiotów, które wykonują zadania przewoźników tych materiałów oraz warunki formalne wynikające z przepisów o ochronie informacji niejawnych, jakie muszą spełniać przewoźnicy;
- 3) sposób dokumentowania przyjmowania przez przewoźników przesyłek oraz ich wydawaniem adresatom, wraz z załącznikami w postaci wzorów niezbędnych formularzy;
- 4) warunki ochrony i sposoby zabezpieczenia przesyłek przez przewoźnika oraz warunki, jakie muszą spełniać wykorzystywane przez niego środki transportu i uczestniczące w konwojach osoby;
- 5) określenie postępowania w przypadku zaistnienia nieprzewidzianych okoliczności, mogących mieć wpływ na bezpieczeństwo przesyłki;
- 6) warunki przewożenia materiałów niejawnych poza granicami Rzeczypospolitej Polskiej.

## **Rozdział 8**

### **Bezpieczeństwo teleinformatyczne**

#### **Art. 45**

1. Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego.
2. Akredytacji, o której mowa w ust. 1, dokonuje się na podstawie dokumentacji bezpieczeństwa systemu teleinformatycznego. Akredytacja może być udzielona na czas określony.
3. W przypadku, gdy system teleinformatyczny przeznaczony będzie do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone”, akredytacji bezpieczeństwa teleinformatycznego udziela kierownik jednostki organizacyjnej, w której funkcjonował będzie system teleinformatyczny lub której przedstawiciele są organizatorami systemu teleinformatycznego.
4. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego, o której mowa w ust. 3, kierownik jednostki organizacyjnej przekazuje ABW lub SKW dokumentację bezpieczeństwa systemu teleinformatycznego.
5. W ciągu 30 dni od otrzymania dokumentów, o których mowa w ust. 4, ABW lub SKW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji

bezpieczeństwa teleinformatycznego, zalecenia w zakresie konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. Kierownik jednostki organizacyjnej w terminie 30 dni informuje ABW lub SKW o realizacji zaleceń. W szczególnie uzasadnionych przypadkach ABW lub SKW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego.

6. W przypadku, gdy system teleinformatyczny przeznaczony będzie do przetwarzania informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą, akredytacji bezpieczeństwa teleinformatycznego dokonuje ABW lub SKW.
7. Potwierdzeniem udzielenia przez ABW lub SKW akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą jest świadectwo akredytacji bezpieczeństwa teleinformatycznego, w szczególności zawierające warunki jego ważności oraz zasady przeprowadzania audytów przez ABW lub SKW w ramach sprawowania nadzoru nad systemem teleinformatycznym.
8. Świadectwo, o którym mowa w ust. 7, wydaje się na podstawie:
  - 1) pozytywnej oceny bezpieczeństwa systemu teleinformatycznego na podstawie dokumentacji bezpieczeństwa systemu teleinformatycznego;
  - 2) pozytywnego wyniku audytu bezpieczeństwa systemu teleinformatycznego, polegającego na weryfikacji poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego. ABW lub SKW może odstąpić od przeprowadzenia audytu systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne”.
9. Obowiązkowi akredytacji, o którym mowa w ust. 1-8, nie podlegają systemy teleinformatyczne oraz współpracujące z nimi środki techniczne, które służą bezpośrednio i wyłącznie do pozyskiwania i przekazywania w sposób niejawną informacji w trakcie realizacji czynności operacyjno-rozpoznawczych przez uprawnione do tego podmioty oraz do utrwalania dowodów pozyskanych w trakcie realizacji tych czynności.

#### **Art. 46**

1. Środki ochrony elektromagnetycznej przeznaczone do ochrony informacji niejawnych o klauzuli „poufne” lub wyższej, podlegają badaniom i ocenie bezpieczeństwa, w ramach procesów certyfikacji prowadzonych przez ABW lub SKW.

2. Urządzenia i narzędzia kryptograficzne przeznaczone do ochrony informacji niejawnych podlegają badaniom i ocenie bezpieczeństwa, w ramach procesów certyfikacji prowadzonych przez ABW lub SKW.
3. ABW lub SKW może na wniosek przeprowadzić proces certyfikacji urządzenia lub narzędzia służącego do ochrony informacji niejawnych realizującego zabezpieczenia teleinformatyczne.
4. Pozytywne wyniki ocen bezpieczeństwa na podstawie wyników badań prowadzonych w ramach procesów certyfikacji, o których mowa w ust. 1-3, stanowią podstawę do wydania przez ABW lub SKW certyfikatu ochrony elektromagnetycznej, certyfikatu ochrony kryptograficznej lub certyfikatu bezpieczeństwa teleinformatycznego. Certyfikaty mogą zostać wydane na czas określony.
5. ABW i SKW wzajemnie informują się o wydanych, zawieszonych i unieważnionych certyfikatach ochrony kryptograficznej, o których mowa w ust. 4.
6. Procesy certyfikacji, o których mowa w ust. 1-3, prowadzone są przez ABW lub SKW z pominięciem właściwości, o której mowa w art. 10 ust. 2.
7. Badania w ramach procesów certyfikacji, o których mowa w ust. 1-3, mogą być wykonywane w laboratoriach badawczych innych niż laboratoria ABW lub SKW, jeżeli laboratoria te są akredytowane przez ABW lub SKW.
8. Szef ABW lub Szef SKW może dopuścić do stosowania w systemie teleinformatycznym przeznaczonym do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej, bez przeprowadzenia badań i oceny, urządzenie lub narzędzie kryptograficzne, jeżeli:
  - 1) otrzymało stosowny certyfikat wydany przez krajową władzę bezpieczeństwa lub inny uprawniony organ w NATO, Unii Europejskiej lub państwie będącym członkiem NATO lub Unii Europejskiej,
  - 2) w przypadku, gdy brak jest możliwości eksploatacji tego systemu teleinformatycznego z wykorzystaniem jakichkolwiek urządzeń lub narzędzi kryptograficznych posiadających certyfikat ABW lub SKW,
  - 3) a także, gdy brak jest możliwości i celowości tworzenia takich urządzeń lub narzędzi i
  - 4) brak tego systemu teleinformatycznego powodowałby zagrożenie dla porządku publicznego, obronności, bezpieczeństwa albo interesów międzynarodowych państwa.
9. Szef ABW lub Szef SKW może dopuścić do stosowania w systemie teleinformatycznym przeznaczonym do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, bez

konieczności przeprowadzania badań i oceny, urządzenia lub narzędzia kryptograficzne, jeżeli otrzymały stosowny certyfikat wydany przez krajową władzę bezpieczeństwa lub inny uprawniony organ w NATO, Unii Europejskiej lub państwie będącym członkiem NATO lub Unii Europejskiej.

#### **Art. 47**

1. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien stanowić systematyczny opis zasad zarządzania bezpieczeństwem systemu teleinformatycznego.
2. Dokument, o którym mowa w ust. 1 powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zasady zarządzania ryzykiem, a także opisywać przyjęte sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu oraz aspekty budowy, zasady działania i eksploatacji, które mają związek lub wpływają na bezpieczeństwo systemu. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym od szczególnych wymagań bezpieczeństwa dokumencie.
3. Dokument szczególnych wymagań bezpieczeństwa opracowuje się w fazie projektowania, bieżąco uzupełnia w fazie wdrażania i modyfikuje w fazie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.
4. Dokument procedur bezpiecznej eksploatacji określa sposób i tryb postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp.
5. Dokument procedur bezpiecznej eksploatacji opracowuje się i uzupełnia w fazie wdrażania oraz modyfikuje w fazie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.
6. Podstawą dokonania wszelkich zmian w systemie teleinformatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.
7. Odpowiedzialność za opracowanie oraz przekazanie ABW lub SKW, dokumentów, o których mowa w ust. 1-5, ponosi kierownik jednostki organizacyjnej, w której funkcjonował będzie system teleinformatyczny lub której przedstawiciele są organizatorami systemu teleinformatycznego.

8. Kierownik jednostki organizacyjnej akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego.
9. Dokumentacja bezpieczeństwa systemu teleinformatycznego, przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej jest w każdym przypadku indywidualnie zatwierdzana przez ABW lub SKW, w terminie 30 dni od dnia jej otrzymania. Zatwierdzenie dokumentacji uprawnia do przejścia do kolejnej fazy budowy systemu teleinformatycznego, o której mowa w ust. 3.

#### **Art. 48**

1. Prezes Rady Ministrów określi, w drodze rozporządzenia, podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne oraz sposób opracowywania dokumentacji bezpieczeństwa systemów teleinformatycznych.
2. W rozporządzeniu, o którym mowa w ust. 1, Prezes Rady Ministrów uwzględni w szczególności podstawowe wymagania bezpieczeństwa teleinformatycznego w zakresie ochrony fizycznej, elektromagnetycznej, kryptograficznej, bezpieczeństwa transmisji, kontroli dostępu w systemach teleinformatycznych oraz wymagania w zakresie szacowania ryzyka i zarządzania ryzykiem.
3. Prezes Rady Ministrów określi, w drodze rozporządzenia, tryb akredytacji i wymagania dla laboratoriów badawczych, o których mowa w art. 46 ust. 7, a także tryb sprawowania nadzoru przez ABW lub SKW nad akredytowanymi laboratoriami.

#### **Art. 49**

1. Za przeprowadzenie czynności, o których mowa w art. 45 ust. 6-8 oraz art. 46 ust. 1-4, a także za akredytację laboratoriów badawczych, o której mowa w art. 46 ust. 7, pobiera się opłaty.
2. Z opłat, o których mowa w ust. 1, są zwolnione jednostki organizacyjne będące jednostkami budżetowymi.
3. Przedsiębiorcy obowiązani na podstawie odrębnych ustaw do wykonywania zadań publicznych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego zwolnieni są z opłat za przeprowadzenie czynności, o których mowa w art. 43 ust. 6-8, w przypadku akredytacji bezpieczeństwa teleinformatycznego systemów teleinformatycznych niezbędnych do wykonania tych zadań.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, wysokość opłat, o których mowa w ust. 1, z uwzględnieniem kosztów ponoszonych na przeprowadzenie czynności, o których mowa w art. 45 ust. 6-8 oraz art. 46 ust. 1-4 oraz akredytacji, o której mowa w art. 46 ust. 7.

#### **Art. 50**

1. Kierownik jednostki organizacyjnej wyznacza:
  - 1) pracownika lub pracowników pionu ochrony pełniących funkcję inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz za kontrolę przestrzegania procedur bezpiecznej eksploatacji;
  - 2) osobę lub zespół osób, nie pełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa dla systemu teleinformatycznego, zwane dalej „administratorem systemu”.
2. ABW i SKW udzielają kierownikom jednostek organizacyjnych pomocy niezbędnej do realizacji ich zadań, w szczególności wydając zalecenia w zakresie bezpieczeństwa teleinformatycznego.
3. Stanowiska lub funkcje, o których mowa w ust. 1, mogą zajmować lub pełnić osoby spełniające wymagania, o których mowa w art. 16, posiadające poświadczenia bezpieczeństwa upoważniające do zapoznawania się z informacjami niejawnymi o klauzuli wyższej, niż klauzula informacji przetwarzanych w systemie teleinformatycznym lub o klauzuli „ściśle tajne”, po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez ABW lub SKW.
4. Koszty szkolenia, o którym mowa w ust. 3, pokrywa jednostka organizacyjna, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje prace zlecone.
5. Wzajemne prawa i obowiązki organizatora i uczestnika szkolenia, o którym mowa w ust. 3, określa umowa zawarta między stronami.

## **Rozdział 9**

### **Bezpieczeństwo przemysłowe**

#### **Art. 51**

1. Warunkiem dostępu przedsiębiorcy do informacji niejawnych w związku z wykonywaniem umów albo zadań wynikających z przepisów prawa, zwanych dalej „umowami”, jest zapewnienie ochrony informacji niejawnych.
2. Dokumentem potwierdzającym zdolność do ochrony informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą jest świadectwo bezpieczeństwa przemysłowego, zwane dalej „świadectwem”, wydane przez ABW lub SKW, po przeprowadzeniu postępowania bezpieczeństwa przemysłowego.
3. W przypadku przedsiębiorcy wykonującego działalność osobiście, zdolność do zapewnienia ochrony informacji niejawnych potwierdza poświadczenie bezpieczeństwa do klauzuli „poufne” lub wyższej, wydane przez ABW lub SKW.
4. Zdolność do zapewnienia ochrony informacji niejawnych przez przedsiębiorcę, o którym mowa w ust. 3, potwierdza wydane przez ABW lub SKW świadectwo w przypadku dostępu do informacji niejawnych oznaczonych klauzulami tajności będącymi zagranicznymi odpowiednikami klauzuli „poufne” lub wyższej, jeżeli obowiązek uzyskania świadectwa wynika z ratyfikowanych przez RP umów międzynarodowych lub prawa wewnętrznego strony zawierającej umowę.
5. Do przedsiębiorcy, o którym mowa w ust. 3 nie stosuje się przepisów Rozdziału 9 za wyjątkiem art. 57 ust. 2 oraz art. 58 ust. 1 i 2 w części dotyczącej postępowań sprawdzających wobec osób.
6. Przepisy ust. 1-5 stosuje się także do przedsiębiorców będących podwykonawcami umów.
7. Szef Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu lub Prezesa Rady Ministrów albo minister właściwy dla określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego lub kierownik urzędu centralnego, a w przypadku ich braku Szef ABW lub Szef SKW, może wyrazić pisemną zgodę na udostępnienie informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą przedsiębiorcy, wobec którego wszczęto postępowanie bezpieczeństwa przemysłowego lub postępowanie sprawdzające. Uwierzytelnioną kopię zgody przekazuje się do ABW lub SKW.
8. W szczególnie uzasadnionych przypadkach podmioty, o których mowa w ust. 7, mogą wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych przedsiębiorcy nieposiadającemu odpowiedniego świadectwa, i wobec którego nie jest

prorowadzone postępowanie bezpieczeństwa przemysłowego lub nie jest prowadzone postępowanie sprawdzające.

9. W przypadku, gdy przedsiębiorca zamierza wykonywać umowy związane z dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone”, świadectwo nie jest wymagane.
10. Przedsiębiorca, o którym mowa w ust. 9, jest obowiązany spełniać inne wymagania ustawy w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone”.

### **Art. 52**

1. W zależności od stopnia zdolności do ochrony informacji niejawnych oznaczonych klauzulami „poufne” lub wyższą wydaje się świadectwo odpowiednio:
  - 1) pierwszego stopnia – potwierdzające pełną zdolność przedsiębiorcy do ochrony tych informacji;
  - 2) drugiego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych;
  - 3) trzeciego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach.
2. Świadectwo potwierdzające zdolność do ochrony informacji niejawnych oznaczonych klauzulą:
  - 1) „ściśle tajne”, potwierdza zdolność do ochrony informacji niejawnych oznaczonych klauzulą:
    - a) „ściśle tajne” - przez okres 5 lat od daty wystawienia,
    - b) „tajne” – przez okres 7 lat od daty wystawienia,
    - c) „poufne” – przez okres 10 lat od daty wystawienia;
  - 2) „tajne”, potwierdza zdolność do ochrony informacji niejawnych oznaczonych klauzulą:
    - a) „tajne” – przez okres 7 lat od daty wystawienia,
    - b) „poufne” – przez okres 10 lat od daty wystawienia;
  - 3) „poufne”, potwierdza zdolność do ochrony informacji niejawnych oznaczonych tą klauzulą przez okres 10 lat od daty wystawienia.

3. ABW lub SKW wydaje odrębne świadectwa potwierdzające zdolność do ochrony informacji niejawnych oznaczonych zagranicznymi odpowiednikami klauzuli „tajne” lub „poufne” stosowanymi przez organizacje międzynarodowe. Przepis ust. 2 stosuje się odpowiednio.
4. Świadectwo wygasa, jeżeli:
  - 1) upłynął okres jego ważności, o którym mowa w ust. 2;
  - 2) przedsiębiorca zrzekł się uprawnień określonych w świadectwie;
  - 3) przedsiębiorca został przejęty przez inny podmiot lub zlikwidowany.

#### **Art. 53**

1. Postępowanie bezpieczeństwa przemysłowego prowadzone jest na wniosek przedsiębiorcy, który nie wymaga uzasadnienia.
2. We wniosku przedsiębiorca określa stopień świadectwa oraz klauzulę tajności informacji niejawnych, zdolność do ochrony których ma potwierdzać świadectwo.
3. Do wniosku przedsiębiorca dołącza kwestionariusz bezpieczeństwa przemysłowego, zwany dalej „kwestionariuszem”, oraz ankiety bezpieczeństwa osobowego lub kopie poświadczeń bezpieczeństwa osób określonych w art. 54 ust. 3.
4. ABW lub SKW może wezwać przedsiębiorcę do uzupełnienia braków formalnych wniosku i jego załączników w terminie 30 dni, pod rygorem pozostawienia wniosku bez rozpatrzenia.

#### **Art. 54**

1. Postępowanie bezpieczeństwa przemysłowego obejmuje sprawdzenia przedsiębiorcy i postępowania sprawdzające wobec osób.
2. Sprawdzenia przedsiębiorcy, w tym na podstawie danych zawartych w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie, obejmują:
  - 1) strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuację finansową;
  - 2) strukturę organizacyjną;
  - 3) system ochrony osób, materiałów i obiektów ze szczególnym uwzględnieniem elementów systemu ochrony fizycznej informacji niejawnych;
  - 4) wszystkie osoby wchodzące w skład organów zarządzających, kontrolnych oraz osoby działające z ich upoważnienia;

- 5) w szczególnie uzasadnionych przypadkach osoby posiadające poświadczenia bezpieczeństwa.
3. W toku postępowania bezpieczeństwa przemysłowego przeprowadza się postępowania sprawdzające wobec nieposiadających odpowiednich poświadczeń bezpieczeństwa lub kolejne postępowania sprawdzające wobec:
  - 1) kierownika przedsiębiorcy;
  - 2) pełnomocnika ochrony i jego zastępcy;
  - 3) osób zatrudnionych w pionie ochrony;
  - 4) administratora systemu teleinformatycznego;
  - 5) pozostałych osób wskazanych w kwestionariuszu, które powinny mieć dostęp do informacji niejawnych.
4. W stosunku do osób, o których mowa w ust. 3 pkt 1-4, odpowiednie poświadczenie bezpieczeństwa oznacza poświadczenie upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą nie niższą niż wskazana we wniosku przedsiębiorcy o wydanie świadectwa.
5. Postępowania sprawdzające wobec osób, o których mowa w ust. 3, mogą być prowadzone przez służbę, która wydała świadectwo, także w okresie ważności świadectwa.

#### **Art. 55**

1. Sprawdzenie przedsiębiorcy i osób prowadzi się na podstawie danych zawartych w kwestionariuszu oraz innych informacji uzyskanych w trakcie postępowania bezpieczeństwa przemysłowego.
2. Kwestionariusz zawiera w szczególności:
  - 1) dane identyfikujące podmiot podlegający sprawdzeniu, w tym jego status prawny;
  - 2) dane o strukturze kapitału i powiązaniach kapitałowych przedsiębiorcy;
  - 3) dane o sytuacji finansowej przedsiębiorcy;
  - 4) dane o strukturze organizacyjnej przedsiębiorcy;
  - 5) dane dotyczące osób, o których mowa w art. 54 ust. 2 pkt 4;
  - 6) dane o systemie ochrony przedsiębiorcy;
  - 7) wykaz pracowników posiadających poświadczenia bezpieczeństwa uprawniające do dostępu do informacji niejawnych;

- 8) wykaz pracowników, którzy powinni być poddani zwykłemu lub poszerzonemu postępowaniu sprawdzającemu;
- 9) wykaz osób, które ze strony przedsiębiorcy wykonują lub będą wykonywać funkcje związane z ochroną informacji niejawnych;
- 10) podpis osoby upoważnionej do składania oświadczeń woli w imieniu przedsiębiorcy.

#### **Art. 56**

Postępowanie bezpieczeństwa przemysłowego powinno być zakończone w terminie nie dłuższym niż 6 miesięcy od dnia przedłożenia wszystkich dokumentów niezbędnych do jego przeprowadzenia.

#### **Art. 57**

1. W przypadku postępowania bezpieczeństwa przemysłowego prowadzonego w celu wydania świadectwa, o którym mowa w art. 52 ust. 1 pkt 3, utworzenie pionu ochrony nie jest wymagane, za wyjątkiem ubiegania się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych oznaczonych klauzulą będącą zagranicznym odpowiednikiem klauzuli „tajne” lub „poufne”, stosowaną przez organizacje międzynarodowe.
2. W przypadku nieutworzenia pionu ochrony przez przedsiębiorcę, szkolenie w zakresie ochrony informacji niejawnych w stosunku do osób, wobec których przeprowadzono postępowanie sprawdzające, o ile nie posiadają zaświadczeń o odbyciu szkolenia w tym zakresie, przeprowadza pełnomocnik ochrony jednostki organizacyjnej zawierającej umowę.

#### **Art. 58**

1. Za przeprowadzenie postępowania bezpieczeństwa przemysłowego oraz postępowań sprawdzających, za wyjątkiem postępowań sprawdzających określonych w art. 33 ust. 4 i art. 34 ust. 1 wobec osób wymienionych w art. 54 ust. 3, także w okresie ważności świadectwa, ABW lub SKW pobierają zryczałtowane opłaty.
2. Prezes Rady Ministrów określi w drodze rozporządzenia z zastrzeżeniem ust. 3, wysokość oraz tryb pobierania opłat, o których mowa w ust. 1

3. Postępowania wszczyna się po wniesieniu opłaty.

#### **Art. 59**

ABW lub SKW umarzają postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 54 ust. 3, w przypadku:

- 1) wycofania przez przedsiębiorcę wniosku o wydanie świadectwa;
- 2) wydania orzeczenia o zakazie prowadzenia przez przedsiębiorcę działalności gospodarczej;
- 3) przejęcia lub likwidacji przedsiębiorcy.

#### **Art. 60**

1. ABW lub SKW zawieszają i podejmują postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 54 ust. 3, na wniosek przedsiębiorcy.
2. Organ, o którym mowa w ust. 1, może zawiesić postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 54 ust. 3, w przypadku:
  - 1) wydania przez inny organ decyzji nakazującej przedsiębiorcy wstrzymanie prowadzenia działalności gospodarczej;
  - 2) wszczęcia postępowania upadłościowego wobec przedsiębiorcy;
  - 3) nieuregulowania w terminie zobowiązań publicznoprawnych;
  - 4) uzależnienia wyniku oceny zdolności przedsiębiorcy do ochrony informacji niejawnych od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd.
3. Organ, o którym mowa w ust. 1, podejmuje z urzędu postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 54 ust. 3, zawieszane na podstawie ust. 2 po ustaniu przyczyn.

#### **Art. 61**

1. Postępowanie bezpieczeństwa przemysłowego kończy się wydaniem przez ABW lub SKW świadectwa zgodnie z wnioskiem przedsiębiorcy albo decyzją o odmowie wydania świadectwa.

2. Organ, o którym mowa w ust. 1, odmawia wydania świadectwa, stwierdzając brak zdolności do ochrony informacji niejawnych, z powodu:
  - 1) odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa osobie lub osobom, które zajmują stanowisko kierownika przedsiębiorcy;
  - 2) braku możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy;
  - 3) niezorganizowania w terminie 6 miesięcy od daty wszczęcia postępowania kompleksowego systemu ochrony informacji niejawnych w przypadku ubiegania się o świadectwo pierwszego lub drugiego stopnia;
  - 4) podania nieprawdziwych danych lub ich zatajenia w kwestionariuszu;
  - 5) w ramach przekazywanych służbie ochrony państwa informacji o zmianach danych zawartych w kwestionariuszu.
  
3. Organ, o którym mowa w ust. 1, może odmówić wydania świadectwa, stwierdzając brak zdolności do ochrony informacji niejawnych, z powodu:
  - 1) ujawnienia w wyniku sprawdzeń osób wymienionych w art. 54 ust. 2 pkt 4 w toku postępowania bezpieczeństwa przemysłowego istotnych informacji mogących mieć wpływ na ochronę informacji niejawnych;
  - 2) niepowiadomienia w terminie 30 dni o zmianie danych zawartych w kwestionariuszu w trakcie postępowania bezpieczeństwa przemysłowego.

## **Art. 62**

1. W okresie ważności świadectwa, ABW lub SKW, może przeprowadzić z urzędu wybrane sprawdzenia przedsiębiorcy, o których mowa w art. 54 ust. 2, w celu ustalenia, czy nie utracił on zdolności do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem.
  
2. W przypadku, gdy świadectwo zostało wydane przez ABW, a przedsiębiorca realizuje umowę na rzecz Ministerstwa Obrony Narodowej, wojskowych organów ochrony prawa, wojskowych organów porządkowych, Sił Zbrojnych RP, jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, SKW – gdy w toku realizacji umowy ujawniła fakty wskazujące na możliwość utraty przez przedsiębiorcę zdolności do ochrony informacji niejawnych - może wystąpić do ABW

o przeprowadzenie kontroli, o której mowa w art. 10 ust. 1 pkt 1 lub sprawdzeń, o których mowa w art. 54 ust. 2.

3. W kontroli, o której mowa w art. 10 ust. 1 pkt 1 lub sprawdzeniu, o którym mowa w art. 54 ust. 2 pkt 3, mogą uczestniczyć żołnierze lub funkcjonariusze SKW. Przed kontrolą lub sprawdzeniem, o którym mowa w art. 54 ust. 2 pkt 3, upoważnieni żołnierze lub funkcjonariusze SKW mogą zapoznać się z aktami postępowania bezpieczeństwa przemysłowego w zakresie dotyczącym kontroli lub sprawdzenia.
4. W przypadku wydania świadectwa przez SKW i realizacji przez przedsiębiorcę umów na rzecz innych jednostek organizacyjnych niż wymienione w ust. 2, przepisy ust. 2 i 3 stosuje się odpowiednio w stosunku do ABW i jej funkcjonariuszy.

### **Art. 63**

1. Wyniki sprawdzenia przedsiębiorcy z urzędu lub ustalenia kontroli ochrony informacji niejawnych mogą stanowić podstawę wydania decyzji o cofnięciu świadectwa.
2. ABW lub SKW cofa świadectwo, stwierdzając utratę zdolności do ochrony informacji niejawnych, z powodu:
  - 1) odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa osobie lub osobom, które zajmują stanowisko kierownika przedsiębiorcy;
  - 2) braku możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy;
  - 3) utraty funkcjonalności kompleksowego systemu fizycznej ochrony informacji niejawnych;
  - 4) podania nieprawdziwych danych lub ich zatajenia w ramach przekazywanych ABW lub SKW informacji o zmianach danych zawartych w kwestionariuszu.
3. Organ, o którym mowa w ust. 2 może cofnąć świadectwo, stwierdzając utratę zdolności do ochrony informacji niejawnych, z powodu:
  - 1) ujawnienia w wyniku sprawdzeń osób wymienionych w art. 54 ust. 2 pkt 4 w toku postępowania bezpieczeństwa przemysłowego istotnych informacji mogących mieć wpływ na ochronę informacji niejawnych;
  - 2) niewykonania przez przedsiębiorcę obowiązku, o którym mowa w art. 68 ust. 1.
4. O cofnięciu świadectwa organ, o którym mowa w ust. 2, zawiadamia niezwłocznie jednostki organizacyjne, które zawarły umowy z przedsiębiorcą.

#### **Art. 64**

Przedsiębiorca może ponownie ubiegać się o wydanie świadectwa w terminie nie krótszym niż rok od dnia doręczenia decyzji o jego odmowie lub cofnięciu.

#### **Art. 65**

1. Świadectwo, decyzja o odmowie wydania świadectwa oraz decyzja o cofnięciu świadectwa powinny zawierać:
  - 1) oznaczenie organu, który wydał, odmówił wydania bądź cofnął świadectwo bezpieczeństwa przemysłowego;
  - 2) miejsce i datę wystawienia;
  - 3) nazwę podmiotu, numer KRS, numer REGON i adres jego siedziby;
  - 4) podstawę prawną;
  - 5) stwierdzenie wydania świadectwa bezpieczeństwa przemysłowego, odmowy wydania lub jego cofnięcia;
  - 6) w przypadku wydania świadectwa bezpieczeństwa przemysłowego - jego stopień, klauzulę tajności oraz termin ważności;
  - 7) imienną pieczęć i czytelny podpis upoważnionego funkcjonariusza ABW lub SKW albo żołnierza SKW.
2. Decyzja o odmowie wydania oraz decyzja o cofnięciu świadectwa powinny zawierać uzasadnienie faktyczne i prawne oraz pouczenie o dopuszczalności i terminie wniesienia:
  - 1) odwołania do Prezesa Rady Ministrów;
  - 2) skargi do sądu administracyjnego.
3. Można odstąpić od uzasadnienia faktycznego decyzji lub je ograniczyć w zakresie, w jakim wiązałyby się to z udostępnieniem informacji niejawnych.

#### **Art. 66**

Rada Ministrów określi, w drodze rozporządzenia, wzory:

- 1) kwestionariusza bezpieczeństwa przemysłowego;
- 2) świadectw bezpieczeństwa przemysłowego;
- 3) decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego;
- 4) decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego.

### **Art. 67**

1. Od decyzji o odmowie wydania oraz od decyzji o cofnięciu świadectwa przedsiębiorcy przysługuje odwołanie do Prezesa Rady Ministrów, na którego decyzję lub postanowienie przysługuje skarga do sądu administracyjnego.
2. Do odwołania i skargi, o których mowa w ust. 1, stosuje się odpowiednio przepisy art. 35, 36, 37 i 38.
3. W przypadku wydania orzeczenia o zakazie prowadzenia przez przedsiębiorcę działalności gospodarczej, przejęcia lub likwidacji przedsiębiorcy, Prezes Rady Ministrów umarza postępowanie odwoławcze.

### **Art. 68**

1. Przedsiębiorca, w czasie trwania postępowania bezpieczeństwa przemysłowego, a także w okresie ważności świadectwa, ma obowiązek informowania w terminie 30 dni ABW lub SKW o:
  - 1) zmianach danych zawartych w kwestionariuszu bezpieczeństwa przemysłowego;
  - 2) ogłoszeniu upadłości, likwidacji lub rozwiązaniu jednostki organizacyjnej albo innej formy zakończenia przez nią działalności;
  - 3) potrzebie zawarcia lub zawarciu umowy z podwykonawcą, związanej z dostępem do informacji niejawnych;
  - 4) wypowiedzeniu umowy;
  - 5) zakończeniu wykonania umowy;
  - 6) zawarciu nowej umowy związanej z dostępem do informacji niejawnych, ze szczególnym uwzględnieniem:
    - a) nazwy i adresu jednostki organizacyjnej zawierającej umowę,
    - b) przedmiotu umowy,
    - c) najwyższej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonaniem umowy.
2. Przedsiębiorca, w czasie realizacji umowy, ma obowiązek niezwłocznego informowania osoby, o której mowa w art. 69 ust. 3, o:
  - 1) zmianach w systemie ochrony informacji niejawnych;
  - 2) zmianach osób wykonujących umowę;

- 3) potrzebie zawarcia z podwykonawcą umowy związanej z dostępem do informacji niejawnych.
3. W przypadku, gdy zawierającym umowę jest Minister Obrony Narodowej, wojskowe organy ochrony prawa, wojskowe organy porządkowe, Siły Zbrojne RP, jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, ABW po uzyskaniu od przedsiębiorcy informacji, o której mowa w ust. 1 pkt 6 przekazuje ją SKW.
4. W przypadku, gdy zawierającym umowę jest inna jednostka organizacyjna niż wymienione w ust. 3, przepis ust. 3 stosuje się odpowiednio w stosunku do ABW.

#### **Art. 69**

1. Jednostka organizacyjna zawierająca umowę związaną z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą, jest odpowiedzialna za wprowadzenie do umowy lub zlecenia zadania instrukcji bezpieczeństwa przemysłowego, określającej:
  - 1) szczegółowe wymagania dotyczące ochrony informacji niejawnych oznaczonych klauzulami „poufne” lub wyższą, które zostaną przekazane przedsiębiorcy w związku z wykonywaniem umowy, odpowiednie do ilości tych informacji, klauzuli tajności oraz liczby osób mających do nich dostęp;
  - 2) skutki oraz zakres odpowiedzialności wykonawcy umowy z tytułu niewykonania lub nienależytego wykonania obowiązków wynikających z niniejszej ustawy, a także nieprzestrzegania wymagań określonych w instrukcji bezpieczeństwa przemysłowego.
2. Instrukcja bezpieczeństwa przemysłowego powinna określać w szczególności:
  - 1) klauzule tajności poszczególnych materiałów lub rodzajów materiałów niejawnych, które zostaną wytworzone przez przedsiębiorcę w związku z wykonaniem umowy;
  - 2) sposób postępowania z materiałami niejawnymi, które zostaną przekazane przedsiębiorcy lub przez niego wytworzone w związku z wykonaniem umowy.
3. Kierownik jednostki organizacyjnej zawierającej umowę związaną z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą, wyznacza osobę

odpowiedzialną za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę obowiązku ochrony przekazanych mu informacji niejawnych.

4. Jeżeli w związku z wykonaniem umowy zostaną wytworzone informacje niejawne, odpowiednią klauzulę tajności nadaje osoba, o której mowa w art. 6 ust. 1, zgodnie ze wskazaniami zawartymi w instrukcji bezpieczeństwa przemysłowego, a w przypadku ich braku, po uzgodnieniu z osobą, o której mowa w ust. 3.
5. Jednostka organizacyjna zawierająca umowę związaną z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą, ma obowiązek:
  - 1) niezwłocznego informowania ABW lub SKW o:
    - a) nazwie i adresie przedsiębiorcy, z którym zawiera umowę,
    - b) przedmiocie umowy,
    - c) najwyższej koniecznej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonaniem umowy,
    - d) naruszeniu przepisów o ochronie informacji niejawnych u przedsiębiorcy, z którym zawarto umowę,
    - e) zakończeniu wykonania umowy.
  - 2) niezwłocznego przekazania ABW lub SKW:
    - a) kopii instrukcji bezpieczeństwa przemysłowego, o której mowa w ust. 1,
    - b) kopii świadectwa przedsiębiorcy, z którym zawarto umowę.
6. W przypadku, gdy zawierającym umowę jest Minister Obrony Narodowej, wojskowe organy ochrony prawa, wojskowe organy porządkowe, Siły Zbrojne RP, jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, a świadectwo zostało wydane przez ABW, obowiązek, o którym mowa w ust. 5 realizowany jest także wobec SKW
7. W przypadku, gdy zawierającym umowę jest inna jednostka organizacyjna niż wymienione w ust. 3, przepis ust. 3 stosuje się odpowiednio w stosunku do ABW.

## **Rozdział 10**

### **Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego**

#### **Art. 70**

1. Akta postępowań sprawdzających przeprowadzonych przez służby i organy uprawnione do realizacji poszerzonych postępowań sprawdzających i akta postępowań bezpieczeństwa przemysłowego są udostępniane do wglądu, bądź przekazywane wyłącznie na pisemne żądanie:
  - 1) sądowi lub prokuratorowi dla celów postępowania karnego;
  - 2) ABW lub SKW dla celów postępowania sprawdzającego;
  - 3) właściwemu organowi w celu przeprowadzenia kontroli prawidłowości postępowania, z wyłączeniem postępowań realizowanych przez AW oraz SWW;
  - 4) właściwemu organowi w celu rozpatrzenia odwołania lub zażalenia;
  - 5) sądowi administracyjnemu w związku z rozpatrywaniem skargi.
2. Akta zwykłych postępowań sprawdzających mogą być udostępnione do wglądu i przekazane w przypadkach określonych w ust. 1 oraz udostępnione do wglądu osobie sprawdzanej.
3. Po wykorzystaniu akta są niezwłocznie zwracane wytwórcy.
4. Po zakończeniu postępowania sprawdzającego i postępowania bezpieczeństwa przemysłowego akta tych postępowań są przechowywane, z uwzględnieniem przepisów ustawy o narodowym zasobie archiwalnym oraz aktów wykonawczych wydanych na jej podstawie:
  - 1) jako wyodrębniona część w archiwach służb i organów, które przeprowadziły te postępowania;
  - 2) przez pełnomocnika ochrony - w przypadku akt zwykłych postępowań sprawdzających przeprowadzonych przez tego pełnomocnika.
5. W przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji jednostki organizacyjnej akta, o których mowa w ust. 4, przejmuje następca prawny, a w przypadku jego braku – ABW lub SKW.

#### **Art. 71**

1. ABW i SKW prowadzą ewidencję osób uprawnionych na podstawie przepisów ustawy do dostępu do informacji niejawnych o klauzuli „poufne” i wyższych, oraz ewidencję osób,

którym odmówiono wydania poświadczenia bezpieczeństwa, a także osób, wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, z wyłączeniem osób zatrudnionych, pełniących służbę lub wykonujących prace zlecone w służbach i instytucjach, o których mowa w art. 24 ust. 4.

2. Dane z ewidencji, o których mowa w ust. 1, mogą obejmować wyłącznie:

- 1) w odniesieniu do osoby - jej imię i nazwisko, numer PESEL, imię ojca, datę i miejsce urodzenia, adres miejsca zamieszkania lub pobytu;
- 2) w odniesieniu do jednostki organizacyjnej, na której ciąży obowiązek przekazania danych do ewidencji – jej nazwę oraz nazwę komórki organizacyjnej i zajmowanego stanowiska lub wykonywanych prac zleconych;
- 3) w odniesieniu do sposobu zakończenia postępowania – określenie dokumentu kończącego procedurę, datę wydania oraz numer.

3. Dane z ewidencji, o których mowa w ust. 1, oraz ewidencji, o których mowa w art. 15 pkt 8 udostępniane są na pisemne żądanie wyłącznie w przypadkach określonych w art. 70 ust. 1 pkt 1 i 3-5 oraz służbom i organom uprawnionym do realizacji poszerzonych postępowań sprawdzających dla celów postępowania sprawdzającego.

## **Rozdział 11**

### **Zmiany w przepisach obowiązujących**

#### **Art. 72**

W ustawie z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.<sup>9)</sup> wprowadza się następujące zmiany:

1) w art. 265 § 1 otrzymuje brzmienie:

„§ 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne oznaczone klauzulą „ściśle tajne” lub „tajne” na podstawie przepisów o ochronie informacji niejawnych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.”;

2) w art. 266 § 2 otrzymuje brzmienie:

„§ 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną oznaczoną klauzulą „poufne” lub „zastrzeżone” na podstawie przepisów o ochronie informacji niejawnych lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.”.

### Art. 73

W ustawie z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.<sup>10</sup>) wprowadza się następujące zmiany:

1) w art. 156 § 4 otrzymuje brzmienie:

„§ 4. Jeżeli zachodzi niebezpieczeństwo ujawnienia informacji niejawnej oznaczonej klauzulą „ściśle tajne” lub „tajne” na podstawie przepisów o ochronie informacji niejawnych, przeglądanie akt, sporządzanie odpisów i kserokopii odbywa się z zachowaniem rygorów określonych przez prezesa sądu lub sąd. Uwierzytelnionych odpisów i kserokopii nie wydaje się, chyba że ustawa stanowi inaczej.”;

2) w art. 179 § 1 otrzymuje brzmienie:

„§ 1. Osoby obowiązane do zachowania w tajemnicy informacji niejawnej oznaczonej klauzulą „ściśle tajne” lub „tajne” na podstawie przepisów o ochronie informacji niejawnych mogą być przesłuchane co do okoliczności, na które rozciąga się ten obowiązek, tylko po zwolnieniu tych osób od obowiązku zachowania w tajemnicy tej informacji przez uprawniony organ przełożony.”;

3) w art. 180 § 1 otrzymuje brzmienie:

„§ 1. Osoby obowiązane do zachowania w tajemnicy informacji niejawnej oznaczonej klauzulą „poufne” lub „zastrzeżone” na podstawie przepisów o ochronie informacji niejawnych lub zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd lub prokurator zwolni te osoby od obowiązku zachowania w tajemnicy informacji niejawnej lub zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji.”;

4) w art. 181 § 2 otrzymuje brzmienie:

„2. Minister Sprawiedliwości określi, w drodze rozporządzenia, sposób sporządzania, przechowywania i udostępniania protokołów przesłuchań oskarżonych, świadków, biegłych i kuratorów, a także innych dokumentów lub przedmiotów, na które rozciąga się obowiązek zachowania w tajemnicy (ochrony) informacji niejawnej oznaczonej klauzulą „ściśle tajne”, „tajne” „poufne” i „zastrzeżone” na podstawie przepisów o ochronie informacji niejawnych albo związanej z wykonywaniem zawodu lub funkcji, jak również dopuszczalny sposób powoływania się na takie przesłuchania, dokumenty i przedmioty w orzeczeniach i pismach procesowych, mając na uwadze konieczność zapewnienia właściwej ochrony tajemnicy przed nieuprawnionym ujawnieniem.”;

5) w art. 225 § 1 i 2 otrzymują brzmienie:

„1. Jeżeli kierownik instytucji państwowej lub samorządowej albo też osoba, u której dokonano zatrzymania rzeczy lub u której przeprowadza się przeszukanie, oświadczy, że wydane lub znalezione przy przeszukaniu pismo lub inny dokument zawiera wiadomości stanowiące informacje niejawną oznaczoną klauzulą „ściśle tajne”, „tajne”, „poufne” lub „zastrzeżone” na podstawie przepisów o ochronie informacji niejawnych, objęte tajemnicą zawodową lub inną chronioną ustawą albo ma charakter osobisty, organ przeprowadzający czynność przekazuje niezwłocznie pismo lub inny dokument bez jego odczytania prokuratorowi lub sądowi w opieczętowanym opakowaniu.

§ 2. Tryb wskazany w § 1 nie obowiązuje w stosunku do pism lub innych dokumentów, które zawierają informację niejawną oznaczoną klauzulą „poufne” lub „zastrzeżone” na podstawie przepisów o ochronie informacji niejawnych, tajemnicy zawodowej lub innej chronionej ustawą, jeżeli ich posiadaczem jest osoba podejrzana o popełnienie przestępstwa, i do pism lub innych dokumentów o charakterze osobistym, których jest ona posiadaczem, autorem lub adresatem.”;

6) art. 226 otrzymuje brzmienie:

„art. 226. W kwestii wykorzystania dokumentów zawierających informacje niejawne oznaczone klauzulą „ściśle tajne”, „tajne”, „poufne” lub „zastrzeżone” na podstawie przepisów o ochronie informacji niejawnych lub tajemnicę zawodową, jako dowodów w postępowaniu karnym, stosuje się odpowiednio zakazy i ograniczenia określone w art. 178-181. Jednakże w postępowaniu przygotowawczym o wykorzystaniu, jako dowodów, dokumentów zawierających tajemnicę lekarską decyduje prokurator.”;

7) w art. 237 w § 3 pkt 10 otrzymuje brzmienie:

„10) szpiegostwa lub ujawnienia informacji niejawnej oznaczonej klauzulą „ściśle tajne” lub „tajne” na podstawie przepisów o ochronie informacji niejawnych,”;

8) w art. 338 § 3 otrzymuje brzmienie:

„§ 3. Jeżeli zachodzi niebezpieczeństwo ujawnienia informacji niejawnej oznaczonej klauzulą „ściśle tajne” lub „tajne” na podstawie przepisów o ochronie informacji niejawnych, oskarżonemu doręcza się odpis aktu oskarżenia bez uzasadnienia. Uzasadnienie aktu oskarżenia udostępnia się jednak z zachowaniem rygorów określonych przez prezesa sądu lub sąd.”;

9) w art. 361 § 2 otrzymuje brzmienie:

„§ 2. Przepisu § 1 nie stosuje się, jeżeli zachodzi obawa ujawnienia informacji niejawnej oznaczonej klauzulą „ściśle tajne” lub „tajne” na podstawie przepisów o ochronie informacji niejawnych”.

## **Art. 74**

W ustawie z dnia 30 czerwca 2005 r. o finansach publicznych (Dz. U. Nr 249, poz. 2104 z późn. zm.<sup>11</sup>) w art. 22:

1) w ust. 2. dodaje się pkt 18 w brzmieniu:

„18) z opłat za przeprowadzenie procesów certyfikacji, o których mowa w art. 44 ust. 1-3 ustawy z dnia ..... o ochronie informacji niejawnych (Dz. U. z ... r. Nr ..., poz. ...).”;

2) w ust. 6 pkt 1 otrzymuje brzmienie:

„1) sfinansowanie wydatków bieżących i inwestycyjnych związanych z uzyskiwaniem przez jednostkę budżetową dochodów z tytułów wymienionych w ust. 1 pkt 1, a przez państwową jednostkę budżetową również z tytułów wymienionych w ust. 2 pkt 1-3, 5-11, 14 i 18;”.

## **Rozdział 12**

### **Przepisy przejściowe i końcowe**

## **Art. 75**

1. Materiały stanowiące informacje niejawne w chwili wejścia w życie ustawy podlegają ochronie zgodnie z przepisami niniejszej ustawy.
2. Kierownicy jednostek organizacyjnych zorganizują w terminie 24 miesięcy przegląd wytworzonych w podległych im jednostkach organizacyjnych materiałów, o których mowa w ust. 1 w celu ustalenia, czy spełniają ustawowe przesłanki ochrony na podstawie ustawy.
3. Obowiązek, o którym mowa w ust. 2 nie dotyczy materiałów wchodzących w skład zamkniętych zbiorów dokumentów, w szczególności podlegających archiwizacji na podstawie odrębnych przepisów.

## **Art. 76**

Poświadczenia bezpieczeństwa wydane na podstawie przepisów dotychczasowych zachowują ważność przez okres wskazany w tych przepisach.

#### **Art. 77**

1. Akredytacje systemów teleinformatycznych, udzielone przez służby ochrony państwa na podstawie dotychczasowych przepisów, zachowują ważność do czasu dokonania w systemie teleinformatycznym zmian, które mogą mieć istotny wpływ na bezpieczeństwo teleinformatyczne, nie dłużej jednak niż 5 lat od wejścia ustawy.
2. Ponowna akredytacja systemu teleinformatycznego przeprowadzana jest w trybie art. 45 ust. 3 lub ust. 6 ustawy. ABW lub SKW przeprowadzając ponowną akredytację może odstąpić od przeprowadzenia audytu bezpieczeństwa systemu teleinformatycznego, niezależnie od klauzuli informacji niejawnych przetwarzanych w systemie teleinformatycznym.

#### **Art. 78**

Laboratoria badawcze posiadające uznania ABW lub SKW uzyskane przed wejściem ustawy, są uprawnione do wykonywania badań w ramach procesów certyfikacji, o których mowa w art. 46 ust. 1-3, przez okres 6 miesięcy od wejścia ustawy.

#### **Art. 79**

1. Zaświadczenia o przeszkoleniu w zakresie ochrony informacji niejawnych wydane na podstawie przepisów dotychczasowych zachowują ważność przez okres wskazany w tych przepisach.
2. Zaświadczenia, o których mowa w art. 14 ust. 2 pkt 4 wydane przez byłe WSI, zachowują ważność z zastrzeżeniem art. 19 ust. 3.

#### **Art. 80**

1. Świadectwa bezpieczeństwa przemysłowego wydane na podstawie przepisów dotychczasowych, potwierdzające zdolność do ochrony informacji niejawnych:
  - 1) oznaczonych klauzulą „ściśle tajne” – potwierdzają zdolność do ochrony informacji niejawnych oznaczonych klauzulą „tajne” i „poufne” w okresie wskazanym w niniejszej ustawie;
  - 2) oznaczonych klauzulą „tajne” – potwierdzają zdolność do ochrony informacji niejawnych oznaczonych klauzulą „poufne” w okresie wskazanym w niniejszej ustawie.

2. Okresy ważności świadectw, o których mowa w ust. 1, liczone są od daty wydania świadectwa.

#### **Art. 81**

Do postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego wszczętych i niezakończonych przed dniem wejścia w życie ustawy, stosuje się przepisy dotychczasowe.

#### **Art. 82**

Dotychczasowe przepisy wykonawcze, wydane na podstawie ustawy, o której mowa w art. 83, zachowują moc do czasu wejścia w życie przepisów wykonawczych wydanych na podstawie niniejszej ustawy, nie dłużej jednak niż przez 12 miesięcy od dnia jej wejścia w życie.

#### **Art. 83**

Traci moc ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196 poz. 1631 z późn. zm.<sup>12</sup>).

#### **Art. 84**

Ustawa wchodzi w życie po upływie 3 miesięcy od dnia ogłoszenia.

---

<sup>1</sup> Niniejszą ustawą zmienia się ustawy: ustawę z dnia 6 czerwca 1997 r. – Kodeks karny, ustawę z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego oraz ustawę z dnia 30 czerwca 2005 r. o finansach publicznych.

<sup>2</sup> Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i poz. 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331, Nr 82, poz. 556, z 2008 r. Nr 17, poz. 101 i Nr 227, poz. 1505 oraz z 2009 r. Nr 11, poz. 59 i Nr 18, poz. 97.

<sup>3</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 127, poz. 880 i Nr 180, poz. 1280, z 2008 r. Nr 70, poz. 416, Nr 116, poz. 732, Nr 141, poz. 888, Nr 171, poz. 1056 i Nr 216, poz. 1367 oraz z 2009 r. Nr 18, poz. 97.

---

<sup>4</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 49, poz. 509, z 2002 r. Nr 113, poz. 984, Nr 153, poz. 1271 i Nr 169, poz. 1387, z 2003 r. Nr 130, poz. 1188 i Nr 170, poz. 1660, z 2004 r. Nr 162, poz. 1692, z 2005 r. Nr 64, poz. 565, Nr 78, poz. 682 i Nr 181, poz. 1524 oraz z 2008 r. Nr 229, poz. 1539.

<sup>5</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 209, poz. 1315, Nr 225, poz. 1502 oraz Nr 227, poz. 1505.

<sup>6</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 126, poz. 1070, Nr 141, poz. 1178, Nr 144, poz. 1208, Nr 153, poz. 1271, Nr 169, poz. 1385 i poz. 1387, Nr 241, poz. 2074, z 2003 r. Nr 50, poz. 424, Nr 60, poz. 535, Nr 65, poz. 594, Nr 228, poz. 2260 i Nr 229, poz. 2276, z 2004 r. Nr 64, poz. 594, Nr 68, poz. 623, Nr 91, poz. 870, Nr 96, poz. 959, Nr 121, poz. 1264, Nr 146, poz. 1546 i Nr 173, poz. 1808, z 2005 r. Nr 83, poz. 719, Nr 85, poz. 727, Nr 167, poz. 1398 i Nr 183, poz. 1538, z 2006 r. Nr 104, poz. 708, Nr 157, poz. 1119, Nr 190, poz. 1401 i Nr 245, poz. 1775, z 2007 r. Nr 42, poz. 272 i Nr 112, poz. 769, z 2008 r. Nr 171, poz. 1056, Nr 192, poz. 1179, Nr 209, poz. 1315 i Nr 231, poz. 1546 oraz z 2009 r. Nr 18, poz. 97, Nr 42, poz. 341 i Nr 65, poz. 545.

<sup>7</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 85, poz. 727, Nr 86, poz. 732 i Nr 143, poz. 1199, z 2006 r. Nr 66, poz. 470, Nr 104, poz. 708, Nr 217, poz. 1590 i Nr 225, poz. 1635, z 2007 r. Nr 105, poz. 721, Nr 112, poz. 769, Nr 120, poz. 818, Nr 192, poz. 1378, Nr 195, poz. 1414 i Nr 225, poz. 1671, z 2008 r. Nr 118, poz. 745, Nr 141, poz. 888, Nr 180, poz. 1109 i Nr 209, poz. 1316, poz. 1318 i poz. 1320 oraz z 2009 r. Nr 18, poz. 97, Nr 44, poz. 362 i Nr 57, poz. 466.

<sup>8</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 64, poz. 594, Nr 91, poz. 868, Nr 171, poz. 1800 i Nr 173, poz. 1808, z 2005 r. Nr 132, poz. 1110 i Nr 183, poz. 1537, z 2006 r. Nr 66, poz. 470, Nr 104, poz. 708 i poz. 711, Nr 157, poz. 1119, Nr 191, poz. 1413 i Nr 217, poz. 1590, z 2007 r. Nr 171, poz. 1207, z 2008 r. Nr 110, poz. 707, Nr 209, poz. 1318 i Nr 227, poz. 1505 oraz z 2009 r. Nr 18, poz. 97.

<sup>9</sup> Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1997 r. Nr 128, poz. 840, z 1999 r. Nr 64, poz. 729 i Nr 83, poz. 931, z 2000 r. Nr 48, poz. 584, Nr 93, poz. 1027 i Nr 116, poz. 1216, z 2001 r. Nr 98, poz. 1071, z 2003 r. Nr 111, poz. 1061, Nr 179, poz. 1750, Nr 199, poz. 1935 i Nr 228, poz. 2255, z 2004 r. Nr 25, poz. 219, Nr 69, poz. 626, Nr 93, poz. 889 i Nr 243, poz. 2426, z 2005 r. Nr 86, poz. 732, Nr 90, poz. 757, Nr 132, poz. 1109, Nr 163, poz. 1363, Nr 178, poz. 1479 i Nr 180, poz. 1493, z 2006 r. Nr 190, poz. 1409,

---

Nr 218, poz. 1592 i Nr 226, poz. 1648, z 2007 r. Nr 89, poz. 589, Nr 123, poz. 850, Nr 124, poz. 859 i Nr 192, poz. 1378 oraz z 2008 r. Nr 90, poz. 560, Nr 122, poz. 782, Nr 171, poz. 1056, Nr 173, poz. 1080 i Nr 214, poz. 1344.

<sup>10</sup> Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1999 r. Nr 83, poz. 931, z 2000 r. Nr 50, poz. 580, Nr 62, poz. 717, Nr 73, poz. 852 i Nr 93, poz. 1027, z 2001 r. Nr 98, poz. 1071 i Nr 106, poz. 1149, z 2002 r. Nr 74, poz. 676, z 2003 r. Nr 17, poz. 155, Nr 111, poz. 1061 i Nr 130, poz. 1188, z 2004 r. Nr 51, poz. 514, Nr 69, poz. 626, Nr 93, poz. 889, Nr 240, poz. 2405 i Nr 264, poz. 2641, z 2005 r. Nr 10, poz. 70, Nr 48, poz. 461, Nr 77, poz. 680, Nr 96, poz. 821, Nr 141, poz. 1181, Nr 143, poz. 1203, Nr 163, poz. 1363, Nr 169, poz. 1416 i Nr 178, poz. 1479, z 2006 r. Nr 15, poz. 118, Nr 66, poz. 467, Nr 95, poz. 659, Nr 104, poz. 708 i poz. 711, Nr 141, poz. 1009 i poz. 1013, Nr 167, poz. 1192 i Nr 226, poz. 1647 i poz. 1648, z 2007 r. Nr 64, poz. 432, Nr 80, poz. 539, Nr 89, poz. 589, Nr 99, poz. 664, Nr 112, poz. 766, Nr 123, poz. 849 i Nr 128, poz. 903, z 2008 r. Nr 27, poz. 162, Nr 100, poz. 648, Nr 107, poz. 686, Nr 123, poz. 802, Nr 182, poz. 1133, Nr 208, poz. 1308, Nr 214, poz. 1344, Nr 225, poz. 1485, Nr 234, poz. 1571 i Nr 237, poz. 1651 oraz z 2009 r. Nr 8, poz. 39, Nr 20, poz. 104, Nr 27, poz. 162, Nr 28, poz. 171 i Nr 68, poz. 585.

<sup>11</sup> Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 45, poz. 319, Nr 104, poz. 708, Nr 170, poz. 1217 i 1218, Nr 187, poz. 1381 i Nr 249, poz. 1832, z 2007 r. Nr 82, poz. 560, Nr 88, poz. 587, Nr 115, poz. 791 i Nr 140, poz. 984, z 2008 r. Nr 180, poz. 1112, Nr 209, poz. 1317, Nr 216, poz. 1370 i Nr 227, poz. 1505 oraz z 2009 r. Nr 19, poz. 100 i Nr 72, poz. 619.

<sup>12</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708 i 711, Nr 149, poz. 1078, Nr 218, poz. 1592 i Nr 220, poz. 1600 oraz z 2008 r. Nr 171, poz. 1056.