

**USTAWA**

z dnia \_\_\_\_\_ 2019 r.

**o ochronie informacji niejawnych**

Rozdział 1

**Przepisy ogólne**

**Art. 1.** 1. Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, zwanych dalej "informacjami niejawnymi", to jest zasady:

- 1) klasyfikowania informacji niejawnych;
- 2) organizowania ochrony informacji niejawnych;
- 3) przetwarzania informacji niejawnych;
- 4) postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej odpowiednio "postępowaniem sprawdzającym" lub "kontrolnym postępowaniem sprawdzającym";
- 5) postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, zwanego dalej "postępowaniem bezpieczeństwa przemysłowego";
- 6) organizacji kontroli stanu zabezpieczenia informacji niejawnych;
- 7) ochrony informacji niejawnych w systemach informatycznych;
- 8) stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych
- 9) ochrony informacji niejawnych w razie ogłoszenia mobilizacji i w czasie wojny.

2. Przepisy ustawy mają zastosowanie do:

- 1) organów władzy publicznej, w szczególności:
  - a) Sejmu i Senatu,
  - 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) 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;
- 5) jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy;

6) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

3. Przepisy ustawy nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych.

4. Do informacji chronionych na podstawie niniejszej ustawy nie mają zastosowania przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 4.05.2016, str. 1) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 i 1669).

**Art. 2.** W rozumieniu ustawy:

- 1) administratorem systemu – jest osoba odpowiedzialna za funkcjonowanie systemu informatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu informatycznego;
- 2) akredytacją bezpieczeństwa informatycznego – jest dopuszczenie systemu informatycznego do przetwarzania informacji niejawnych;
- 3) aktami postępowania – jest wyodrębniony zbiór dokumentów, zawierających w szczególności czynności utrwalone w ramach prowadzonego postępowania sprawdzającego, kontrolnego postępowania sprawdzającego lub postępowania bezpieczeństwa przemysłowego;
- 4) audytem bezpieczeństwa systemu informatycznego – jest weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu informatycznego;
- 5) certyfikacją – jest proces potwierdzania zdolności do ochrony informacji niejawnych urządzenia kryptograficznego lub kryptograficznego narzędzia programowego przeznaczonych do zastosowania w systemie informatycznym albo środka ochrony elektromagnetycznej albo urządzenia lub narzędzia służącego do realizacji zabezpieczenia informatycznego, przeznaczonego do ochrony informacji niejawnych;
- 6) dokumentacją bezpieczeństwa systemu informatycznego – jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu, opracowane zgodnie z zasadami określonymi w ustawie;
- 7) dokumentem – jest każda utrwalona informacja niejawna;
- 8) dokumentem procedur bezpiecznej eksploatacji systemu – jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie informatycznym oraz zakres odpowiedzialności użytkowników tego systemu i pracowników mających do niego dostęp;
- 9) dokumentem szczególnych wymagań bezpieczeństwa – jest systematyczny opis budowy, funkcjonalności oraz sposobu zarządzania bezpieczeństwem systemu informatycznego;
- 10) inspektorem bezpieczeństwa informatycznego – jest pracownik pionu ochrony, odpowiedzialny za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu informatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;
- 11) jednostką organizacyjną – jest podmiot wymieniony w art. 1 ust. 2;

- 12) kancelarią tajną - jest wyodrębniona komórka organizacyjna w zakresie ochrony informacji niejawnych o klauzulach „tajne” i „ściśle tajne”, podległa pełnomocnikowi ochrony i obsługiwana przez pracowników pionu ochrony, odpowiedzialna za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom;
- 13) kancelarią tajną międzynarodową - jest wyodrębniona komórka organizacyjna w zakresie ochrony informacji niejawnych międzynarodowych o klauzulach równorzędnych klauzulom „poufne” lub wyższym, podległa pełnomocnikowi ochrony i obsługiwana przez pracowników pionu ochrony, odpowiedzialna za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom;
- 14) kierownikiem jednostki organizacyjnej – jest osoba stojąca na czele jednostki organizacyjnej, która zarządza jednostką i zapewnia, przy pomocy lub za pośrednictwem podległych pracowników, realizację zadań tej jednostki;
- 15) kierownikiem przedsiębiorcy – jest kierownik jednostki organizacyjnej będący członkiem 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 przedsiębiorcy są wspólnicy prowadzący sprawę spółki, w przypadku spółki partnerskiej – wspólnicy prowadzący sprawę spółki albo zarząd, a w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej - komplementariusze prowadzący sprawę spółki; w przypadku osoby fizycznej prowadzącej działalność gospodarczą kierownikiem przedsiębiorcy jest ta osoba; za kierownika przedsiębiorcy uważa się również likwidatora, a także syndyka lub zarządcę ustanowionego w postępowaniu upadłościowym;
- 16) materiałem – jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;
- 17) Ministrem Koordynatorem Służb Specjalnych - jest Minister - członek Rady Ministrów, którego zakres działania, wyznaczony na podstawie art. 33 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2012 r. poz. 392, z 2015 r. poz. 1064 oraz z 2018 r. poz. 1669), obejmuje zadania związane z działalnością służb specjalnych, w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2018 r. poz. 2387, 2245, 2399 oraz z 2019 r. poz. 53), w tym koordynację działalności służb specjalnych;
- 18) poziomem zagrożeń – jest ocena znaczenia istotnych czynników mających wpływ na zagrożenia związane z nieuprawnionym dostępem do informacji niejawnych lub ich utratą, przeprowadzana w celu doboru odpowiednich środków bezpieczeństwa fizycznego;
- 19) przedsiębiorcą – jest przedsiębiorca w rozumieniu ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. poz. 646, 1479, 1629, 1633 i 2212) lub każda inna jednostka organizacyjna, niezależnie od formy własności, którzy w ramach prowadzonej działalności gospodarczej zamierzają realizować lub realizują związane z dostępem do informacji niejawnych umowy lub zadania wynikające z przepisów prawa;
- 20) przetwarzaniem informacji niejawnych – są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;

- 21) rękojmnią zachowania tajemnicy – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem;
- 22) rozwiązaniem informatycznym – jest urządzenie lub zespół urządzeń, oprogramowanie, narzędzie lub usługa informatyczna umożliwiająca przetwarzanie informacji niejawnych w postaci elektronicznej, eksploatowana lub planowana do wdrożenia w jednostkach organizacyjnych wskazanych w art. 10 ust. 2;
- 23) ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego skutków;
- 24) systemem informatycznym – jest urządzenie informatyczne lub zespół urządzeń informatycznych wraz z oprogramowaniem zapewniający co najmniej funkcjonalność sporządzania oraz przechowywania informacji niejawnych na informatycznym nośniku danych, z wyłączeniem urządzeń służących wyłącznie do rejestracji, odtwarzania lub wyświetlania informacji niejawnych oraz urządzeń z wyłączoną możliwością przesyłania oraz zapisu danych, w tym urządzeń służących wyłącznie do drukowania lub kopiowania materiałów niejawnych;
- 25) systemem ochrony informacji niejawnych – jest zbiór powiązanych ze sobą wymogów określonych w ustawie, jakie powinna spełniać jednostka organizacyjna w celu przetwarzania informacji niejawnych;
- 26) szacowaniem ryzyka – jest całościowy proces identyfikacji, analizy i oceny ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie informatycznym;
- 27) środkami ochrony elektromagnetycznej – są rozwiązania techniczne i organizacyjne, służące do obniżenia ujawniającej emisji elektromagnetycznej przeznaczone do ochrony informacji niejawnych;
- 28) zarządzaniem ryzykiem – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji w systemach informatycznych, z uwzględnieniem ryzyka;
- 29) zatrudnieniem – jest świadczenie pracy na podstawie ustawy z dnia 26 czerwca 1974 r. – Kodeks Pracy (Dz. U. z 2018 r. poz. 917 z późn. zm.<sup>1</sup>), a także mianowanie, w tym pełnienie służby, powołanie, wyznaczenie oraz powierzenie obowiązków lub wykonywanie innych świadczeń przez osobę fizyczną na podstawie umowy cywilnoprawnej, z wyłączeniem umowy o dzieło.

**Art. 3.** Do postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, w zakresie nieuregulowanym w ustawie, mają zastosowanie przepisy art. 6, art. 7, art. 8, art. 12, art. 14, art. 15, art. 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, art. 42, art. 43, art. 44, art. 45, art. 46, art. 47, art. 50, art. 55, art. 57, art. 58, art. 59, art. 60, art. 61 § 3, art. 61a, art. 63 § 4, art. 64, art. 65, art. 72, art. 75 § 1, art. 77 § 1, art. 97 § 1 pkt 4 i § 2, art. 98, art. 101, art. 102, art. 103, art. 104, art. 105 § 1-2, art. 107, art. 109 § 1, art. 112, art. 113 § 1, art. 125 § 1, art. 156, art. 157 § 2, art. 158 oraz art. 217 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz. U. z 2018 r. poz. 2096 oraz z 2019 r. poz. 60).

**Art. 4. 1.** Agencja Bezpieczeństwa Wewnętrznego, zwana dalej „ABW” albo Służba Kontrwywiadu Wojskowego, zwana dalej „SKW”, pobiera opłatę za:

---

<sup>1</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 1000, 1076, 1608, 1629, 2215, 2244, 2245, 2377 i 2432.

- 1) przeprowadzenie czynności w ramach poszerzonych postępowań sprawdzających prowadzonych wobec przedsiębiorcy wykonującego działalność jednoosobowo i osobiście oraz osób wymienionych w art. 57 ust. 3, z wyjątkiem kolejnych postępowań sprawdzających, o których mowa w art. 32 ust. 4 i 5 oraz kontrolnego postępowania sprawdzającego;
- 2) przeprowadzenie czynności sprawdzenia przedsiębiorcy, o których mowa w art. 57 ust. 2;
- 3) szkolenia w zakresie ochrony informacji niejawnych, przeprowadzane przez ABW albo SKW dla:
  - a) pełnomocnika ochrony i jego zastępcy oraz osób przewidzianych na te stanowiska,
  - b) kierownika jednostki organizacyjnej, która przetwarza informacje niejawne o klauzuli „ściśle tajne” lub „tajne”,
  - c) przedsiębiorców wykonujących działalność jednoosobowo i osobiście,
  - d) kierowników przedsiębiorców, u których nie zatrudniono pełnomocnika ochrony;
- 4) prowadzenie:
  - a) specjalistycznych szkoleń z zakresu bezpieczeństwa informatycznego,
  - b) czynności w ramach akredytacji bezpieczeństwa informatycznego, której udzielenie pozostaje we właściwości ABW albo SKW,
  - c) czynności w ramach certyfikacji środków ochrony elektromagnetycznej, urządzeń kryptograficznych i kryptograficznych narzędzi programowych oraz urządzeń lub narzędzi służących do realizacji zabezpieczenia informatycznego, przeznaczonych do ochrony informacji niejawnych.

## 2. Zwolnienie z ponoszenia opłaty, o której mowa w ust. 1:

- 1) pkt 1, za przeprowadzenie czynności w ramach poszerzonych postępowań sprawdzających - przysługuje przedsiębiorcom w przypadku złożenia wniosku o przeprowadzenie postępowania sprawdzającego wobec pełnomocnika do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 5 ustawy z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2016 r. poz. 2012) oraz kandydata na to stanowisko;
- 2) pkt 3, za szkolenia w zakresie ochrony informacji niejawnych - przysługuje Ministerstwu Obrony Narodowej, jednostkom organizacyjnym podległym Ministrowi Obrony Narodowej lub przez niego nadzorowanym z wyjątkiem przedsiębiorców, sądom wojskowym, ataszatom obrony w placówkach zagranicznych, Policji oraz posłom i senatorom;
- 3) pkt 4 – za przeprowadzenie:
  - a) specjalistycznych szkoleń z zakresu bezpieczeństwa informatycznego – przysługuje Ministerstwu Obrony Narodowej, jednostkom organizacyjnym podległym Ministrowi Obrony Narodowej lub przez niego nadzorowanym z wyjątkiem przedsiębiorców, sądom wojskowym, ataszatom obrony w placówkach zagranicznych oraz Policji;
  - b) czynności w ramach akredytacji bezpieczeństwa informatycznego, której udzielenie pozostaje we właściwości ABW albo SKW – przysługuje jednostkom organizacyjnym będącym jednostkami budżetowymi oraz przedsiębiorcom obowiązującym na podstawie odrębnych ustaw do wykonywania zadań publicznych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w przypadku akredytacji bezpieczeństwa informatycznego systemów informatycznych niezbędnych do wykonania tych zadań;
  - c) czynności w ramach certyfikacji środków ochrony elektromagnetycznej, urządzeń kryptograficznych i kryptograficznych narzędzi programowych oraz urządzeń lub

narzędzi służących do realizacji zabezpieczenia informatycznego, przeznaczonych do ochrony informacji niejawnych – przysługuje jednostkom organizacyjnym będącym jednostkami budżetowymi.

3. Prezes Rady Ministrów określi, w drodze rozporządzenia, wysokość opłat, o których mowa w ust. 1, oraz termin i tryb ich dokonywania, uwzględniając, że wysokość opłat nie może przekroczyć:

- 1) kwoty przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłaty nagród z zysku za ubiegły rok, ogłoszonego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 60 pkt 5 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. z 2018 r. poz. 123 z późn. zm.<sup>2</sup>) – za czynności, o których mowa w ust. 1 pkt 1;
- 2) 7-krotności kwoty, o której mowa w pkt 1 – za czynności, o których mowa w ust. 1 pkt 2;
- 3) 25% kwoty, o której mowa w pkt 1 – za czynności, o których mowa w ust. 1 pkt 3;
- 4) stukrotności kwoty, o której mowa w pkt 1 – za czynności, o których mowa w ust. 1 pkt 4.

## Rozdział 2

### Klasyfikowanie informacji niejawnych

**Art. 5.** 1. Informacjom niejawnym nadaje się klauzulę "ściśle tajne", jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

- 1) zagrazi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
- 2) zagrazi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
- 3) zagrazi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
- 4) osłabi gotowość obronną Rzeczypospolitej Polskiej;
- 5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrazi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
- 6) zagrazi lub może zagrazić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
- 7) zagrazi lub może zagrazić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy przewidzianych w ustawie z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka (Dz. U. z 2015 r. poz. 21), albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego, lub osób dla nich najbliższych.

2. Informacjom niejawnym nadaje się klauzulę "tajne", jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

- 1) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;

---

<sup>2</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 1000, 1515, 1544, 1629, 1669, 2429 oraz z 2019 r. poz. 60.

- 2) pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
- 3) zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
- 4) utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
- 5) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
- 6) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

3. Informacjom niejawnym nadaje się klauzulę "poufne", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

- 1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- 2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
- 3) zakłóci porządek publiczny lub zagrazi bezpieczeństwu obywateli;
- 4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
- 5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- 6) zagrazi stabilności systemu finansowego Rzeczypospolitej Polskiej;
- 7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

4. Informacjom niejawnym nadaje się klauzulę "zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

**Art. 6.** 1. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia materiału innego niż dokument.

2. Informacje niejawne podlegają ochronie w sposób określony w ustawie do czasu zniesienia lub zmiany klauzuli tajności na zasadach określonych w ust. 3. Osoba uprawniona do podpisania dokumentu lub oznaczenia materiału innego niż dokument, może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.

3. Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, która jest uprawniona do podpisania dokumentu lub oznaczenia materiału innego niż dokument, albo jej przełożonego, w przypadku ustania lub zmiany ustawowych przesłanek ochrony, o których mowa w art. 5.

4. Kierownik jednostki organizacyjnej przeprowadza nie rzadziej niż raz na 5 lat przegląd wytworzonych w podległej mu jednostce organizacyjnej materiałów zawierających informacje niejawne w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.

5. Obowiązek, o którym mowa w ust. 4, nie dotyczy zbiorów materiałów spraw zakończonych oraz kartotek ewidencyjnych, w szczególności stanowiących materiał archiwalny przekazany do właściwych archiwów na podstawie odrębnych przepisów.

6. Kierownik właściwego archiwum, w uzasadnionych przypadkach, w szczególności przed udostępnieniem, może zwrócić się do kierownika jednostki organizacyjnej, która przekazała

materiał archiwalny, o którym mowa w ust. 5, o przeprowadzenie przeglądu tego materiału w celu ustalenia, czy spełnia on ustawowe przesłanki ochrony, i dokonać w razie potrzeby zmiany lub zniesienia klauzuli tajności.

7. Pisemną zgodę na zniesienie lub zmianę klauzuli tajności, w przypadku informacji niejawnych o klauzuli "ściśle tajne" wyraża kierownik jednostki organizacyjnej, w której materiałowi została nadana klauzula tajności.

8. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom, są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzuli tajności.

9. Uprawnienia w zakresie zniesienia lub zmiany klauzuli tajności materiału przechodzą, w przypadku rozwiązania, zniesienia, likwidacji, upadłości obejmującej likwidację majątku upadłego, przekształcenia lub reorganizacji jednostki organizacyjnej, na jej następcę prawnego. W razie braku następcy prawnego uprawnienia w tym zakresie przechodzą na ABW lub SKW, zgodnie z ich właściwością określoną w art. 10 ust. 2 i 3.

10. Poszczególne części materiału mogą być oznaczone różnymi klauzulami tajności.

11. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób oznaczania materiałów, umieszczania na nich klauzul tajności, a także tryb i sposób zmiany lub znoszenia nadanej klauzuli uwzględniając 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, o którym mowa w ust. 10.

**Art. 7.** 1. Chronione bez względu na upływ czasu, z zastrzeżeniem ust. 2, są:

- 1) dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji, uprawnionych do wykonywania na podstawie ustawy czynności operacyjno-rozpoznawczych jako funkcjonariuszy, żołnierzy lub pracowników wykonujących te czynności;
- 2) dane mogące doprowadzić do identyfikacji osób, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy;
- 3) informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

2. Ochronie nie podlegają dane, o których mowa w ust. 1 pkt 1 i 2, zawarte w dokumentach, zbiorach danych, rejestrach i kartotekach, a także w aktach funkcjonariuszy i żołnierzy organów bezpieczeństwa państwa, przekazanych do Instytutu Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu na podstawie przepisów:

- 1) ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (Dz. U. z 2016 r. poz. 1575 oraz z 2018 r. poz. 5, 369, 1000 i 1277),
- 2) ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944-1990 oraz treści tych dokumentów (Dz. U. z 2017 r. poz. 2186 z późn. zm.<sup>3</sup>)

- chyba że nadano im klauzulę tajności w wyniku przeglądu, o którym mowa w art. 19 ustawy z dnia 29 kwietnia 2016 r. o zmianie ustawy o Instytucie Pamięci Narodowej - Komisji Ścigania

---

<sup>3</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 651, 730, 1000, 1349, 1669 i 1735.



Zbrodni przeciwko Narodowi Polskiemu oraz niektórych innych ustaw (Dz. U. poz. 749), lub przeglądu, o którym mowa w art. 6 ust. 4.

**Art. 8.** Informacje niejawne, którym nadano określoną klauzulę tajności:

- 1) mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do informacji niejawnych o określonej klauzuli tajności;
- 2) muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące bezpieczeństwa systemów informatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności;
- 3) muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

**Art. 9.** 1. Odbiorca materiału, w przypadku stwierdzenia zawyżenia, zaniżenia lub nieuzasadnionego nadania klauzuli tajności, może zwrócić 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 dnia doręczenia wniosku, o którym mowa w ust. 1, odbiorca materiału może zwrócić się o rozstrzygnięcie sporu do ABW albo SKW, zgodnie z ich właściwością.

3. Spór, o którym mowa w ust. 2, ABW lub SKW rozstrzyga w terminie 30 dni od dnia doręczenia wniosku o rozstrzygnięcie sporu.

4. Jeżeli stroną sporu, o którym mowa w ust. 2, jest ABW albo SKW, to spór rozstrzyga Minister Koordynator Służb Specjalnych, a w przypadku gdy minister ten nie został powołany, Prezes Rady Ministrów, w terminie 30 dni od dnia doręczenia wniosku o rozstrzygnięcie sporu.

5. W przypadku niepowołania Ministra Koordynatora Służb Specjalnych 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. 4.

### 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 kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;
- 2) realizują zadania w zakresie bezpieczeństwa systemów informatycznych, z zastrzeżeniem art. 50 ust. 6;
- 3) prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego;
- 4) zapewniają ochronę informacji niejawnych wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi;
- 5) prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych;
- 6) uzyskują informacje z jednostek organizacyjnych w zakresie realizowanych przez te jednostki zadań w obszarze ochrony informacji niejawnych;

- 7) uzyskują wyjaśnienia i informacje oraz wgląd do dokumentów dotyczących funkcjonowania systemu ochrony informacji niejawnych;
- 8) uzyskują od służb, o których mowa w art. 23 ust. 8, dane, w tym dane statystyczne, związane z funkcjonowaniem systemu ochrony informacji niejawnych, dotyczące w szczególności osób:
  - a) wobec których jest lub było prowadzone postępowanie sprawdzające lub kontrolne postępowanie sprawdzające,
  - b) którym wydano upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone”, o którym mowa w art. 21 ust. 4 pkt 1 lub ust. 5 albo zgodę, o której mowa w art. 37 ust. 1 lub 5,
  - c) wobec których przeprowadzono szkolenia, o których mowa w art. 20.

2. SKW realizuje zadania w odniesieniu do:

- 1) Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, ujętych w wykazie wydanym na podstawie art. 33 ust. 1d ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2012 r. poz. 392, z 2015 r. poz. 1064 oraz z 2018 r. poz. 1669);
- 2) jednostek organizacyjnych o szczególnym znaczeniu dla obronności państwa innych niż wymienione w pkt 1;
- 3) sądów wojskowych;
- 4) ataszatów obrony w placówkach zagranicznych;
- 5) żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione w pkt 1;
- 6) międzynarodowych dowództw wojskowych i wielonarodowych jednostek wojskowych z udziałem Sił Zbrojnych Rzeczypospolitej Polskiej oraz instytucji organizacji międzynarodowych lub innych podmiotów wielonarodowych, z siedzibą na terytorium Rzeczypospolitej Polskiej, których zakres zadań dotyczy obronności lub wojskowości.

3. ABW realizuje zadania w odniesieniu do jednostek organizacyjnych i osób podlegających ustawie, niewymienionych w ust. 2.

4. Minister Koordynator Służb Specjalnych, a w przypadku, gdy minister ten nie został powołany, Prezes Rady Ministrów, w przypadku szczególnie uzasadnionym bezpieczeństwem narodowym, może:

- 1) nakazać ABW wykonywanie czynności, o których mowa w ust. 1 pkt 1, 2 i 4-6 wobec podmiotów, pozostających we właściwości SKW;
- 2) nakazać SKW wykonywanie czynności, o których mowa w ust. 1 pkt 1, 2 i 4-6 wobec podmiotów, pozostających we właściwości ABW;
- 3) zlecić ABW wszczęcie lub kontynuowanie postępowań, o których mowa w ust. 1 pkt 3, pozostających we właściwości SKW albo we właściwości służb, o których mowa w art. 23 ust. 8;
- 4) zlecić SKW wszczęcie lub kontynuowanie postępowań, o których mowa w ust. 1 pkt 3, pozostających we właściwości ABW albo we właściwości służb, o których mowa w art. 23 ust. 8.

5. ABW lub SKW wykonują czynności i prowadzą postępowania nakazane lub zlecone w trybie, o którym mowa w ust. 4.

6. W przypadkach, o których mowa w ust. 4 pkt 3 i 4, ABW, SKW lub służba, o której mowa w art. 23 ust. 8, przekazuje ABW lub SKW akta prowadzonego postępowania wraz z dowodem wniesienia opłaty, o ile została wniesiona.

7. Szef ABW, w porozumieniu z Szefem SKW, określa właściwość ABW lub SKW w zakresie realizacji zadań w stosunku do jednostek organizacyjnych niewymienionych w ust. 2 pkt 6, które

utworzono w oparciu o zawarte przez Rzeczpospolitą Polską umowy międzynarodowe lub zawarte przez Ministra Obrony Narodowej porozumienia międzynarodowe.

8. W przypadku, gdy po wszczęciu postępowania sprawdzającego, kontrolnego postępowania sprawdzającego lub postępowania bezpieczeństwa przemysłowego nastąpi zmiana właściwości służby je realizującej, jest ono kontynuowane przez służbę, która je wszczęła.

9. W przypadku wystąpienia wątpliwości w obszarze ochrony informacji niejawnych pomiędzy ABW a SKW, rozstrzyga je Minister Koordynator Służb Specjalnych, a w przypadku gdy minister ten nie został powołany, Prezes Rady Ministrów, nie później niż 30 dni od dnia przekazania stanowiska przez obie służby.

10. Rada Ministrów określi, w drodze rozporządzenia, wykaz jednostek organizacyjnych o szczególnym znaczeniu dla obronności państwa, o których mowa w ust. 2 pkt 2, uwzględniając wymóg identyfikacji każdej z jednostek w sposób indywidualny, w przypadku spółek – w szczególności poprzez określenie numeru w Krajowym Rejestrze Sądowym każdej ze spółek lub każdej ze spółek wchodzących w skład grupy kapitałowej.

**Art. 11.** 1. Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.

2. Krajowa władza bezpieczeństwa jest właściwa do nadzorowania systemu ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi, zwanych dalej "informacjami niejawnymi międzynarodowymi".

3. Na pisemny wniosek:

- 1) kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska,
- 2) pełnomocnika do spraw ochrony informacji niejawnych,
- 3) osoby ubiegającej się o stanowisko albo zajmującej stanowisko w organizacji międzynarodowej lub wykonującej na jej rzecz prace związane z dostępem do informacji niejawnych międzynarodowych

– krajowa władza bezpieczeństwa wydaje dokumenty zaświadczające w obrocie zagranicznym posiadanie uprawnień do dostępu do informacji niejawnych międzynarodowych.

4. Krajowa władza bezpieczeństwa może, w szczególnie uzasadnionych przypadkach, wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych międzynarodowych osobie, o której mowa w art. 23 ust. 5 pkt 1, art. 23 ust. 6 pkt 1, art. 35 ust. 8, a także kierownikowi urzędu centralnego lub osobom je zastępującym, nieposiadającym odpowiedniego poświadczenia bezpieczeństwa.

5. Krajowa władza bezpieczeństwa może wyrazić pisemną zgodę na udostępnienie informacji niejawnych międzynarodowych osobie, wobec której wszczęto poszerzone postępowanie sprawdzające. Zgoda zachowuje ważność do czasu wydania odpowiedniego poświadczenia bezpieczeństwa, nie dłużej jednak niż przez okres 6 miesięcy od dnia jej wydania.

6. Zgodę, o której mowa w ust. 4 lub 5, wydaje się w przypadku spełnienia przez osobę, której zgoda ma dotyczyć, określonych przez właściwą organizację międzynarodową lub inne państwo wymogów w zakresie udostępniania informacji niejawnych osobom nieposiadającym wymaganych uprawnień.

7. Szef ABW, w porozumieniu z Szefem SKW, określi, w drodze wytycznych, szczegółowe zasady postępowania z informacjami niejawnymi międzynarodowymi, uwzględniając potrzebę zapewnienia jednolitości systemu ochrony informacji niejawnych międzynarodowych i jego zgodności z wymogami określonymi przez organizacje międzynarodowe lub państwa, z którymi Rzeczpospolita Polska zawarła umowy o wzajemnej ochronie informacji niejawnych.

8. Szef ABW pełni funkcję krajowej władzy bezpieczeństwa w odniesieniu do podmiotów, o których mowa w art. 10 ust. 2, za pośrednictwem Szefa SKW, także w przypadku czynności, o których mowa w ust. 3-6.

9. W zakresie niezbędnym do wykonywania funkcji krajowej władzy bezpieczeństwa odpowiednio, Szef ABW lub upoważnieni przez niego funkcjonariusze ABW oraz Szef SKW lub upoważnieni przez niego żołnierze lub funkcjonariusze SKW, mają prawo do przeprowadzenia inspekcji stanu zabezpieczenia informacji niejawnych międzynarodowych, stosując odpowiednio art. 12 ust. 1-3.

10. Szef ABW organizuje współdziałanie z Szefem SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa.

11. Prezes Rady Ministrów określi, w drodze rozporządzenia, zakres, tryb i sposób współdziałania Szefa ABW i Szefa SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa ABW uwzględniając rolę Szefa ABW w nadzorze nad systemem ochrony informacji niejawnych wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi oraz konieczność zapewnienia jednolitości stosowanych przez krajową władzę bezpieczeństwa procedur w sferze cywilnej i wojskowej.

**Art. 12. 1.** W zakresie niezbędnym do kontroli stanu zabezpieczenia informacji niejawnych, upoważnieni pisemnie funkcjonariusze ABW albo funkcjonariusze lub żołnierze SKW mają prawo do:

- 1) 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) badania obiegu i udostępniania materiałów niejawnych;
- 4) żądania udostępnienia do kontroli systemów informatycznych służących do przetwarzania tych informacji oraz innych systemów lub urządzeń, w szczególności systemów teleinformatycznych w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650);
- 5) przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji;
- 6) żądania od osób zatrudnionych w jednostce podlegającej kontroli lub od osób, które były zatrudnione w jednostce podlegającej kontroli, udzielania, we wskazanym terminie, ustnych i pisemnych wyjaśnień;
- 7) zabezpieczania materiału dowodowego zebranego w toku kontroli;
- 8) 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;
- 9) powoływania oraz korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych;
- 10) 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 stanu zabezpieczenia informacji niejawnych zaistnieje potrzeba weryfikacji uzyskanych informacji w jednostkach niebędących przedmiotem

kontroli, a ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, funkcjonariuszom ABW albo funkcjonariuszom lub żołnierzom SKW przysługują wobec jednostki niekontrolowanej uprawnienia określone w ust. 1 pkt 1-7, wyłącznie w zakresie weryfikacji ustaleń dokonanych w jednostce kontrolowanej.

3. Jeżeli w czasie wykonywania kontroli stanu zabezpieczenia informacji niejawnych zostanie w znacznym stopniu uprawdopodobnione podejrzenie możliwości przetwarzania informacji niejawnych w systemach informatycznych nieposiadających akredytacji bezpieczeństwa informatycznego lub innych systemach lub urządzeniach, w szczególności systemach teleinformatycznych w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, funkcjonariusze ABW albo funkcjonariusze lub żołnierze SKW mogą żądać udostępnienia do kontroli tych systemów, wyłącznie w celu i zakresie niezbędnym do ustalenia, czy przetwarzanie takie miało miejsce, oraz wyjaśnienia okoliczności z tym związanych.

4. Postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego, z wyłączeniem postępowań, prowadzonych przez służby, o których mowa w art. 23 ust. 8, podlegają kontroli co do ich zgodności z przepisami prawa. Kontrolę tę prowadzi:

- 1) Prezes Rady Ministrów albo Minister Koordynator Służb Specjalnych, jeżeli został powołany – w odniesieniu do postępowań zrealizowanych przez ABW albo SKW;
- 2) odpowiednio ABW lub SKW – w odniesieniu do postępowań zrealizowanych przez pełnomocników ochrony.

5. Do czynności, o których mowa w ust. 1 i 4, dokonywanych przez ABW, SKW, Prezesa Rady Ministrów albo Ministra Koordynatora Służb Specjalnych mają zastosowanie odpowiednio przepisy art. 30 ust. 4, art. 31-37, art. 39 ust. 2 i 2a, art. 40 ust. 2-4, art. 41, art. 49 ust. 2-6, art. 50 ust. 2-3 i art. 98 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524 oraz z 2018 r. poz. 1000), z tym że przewidziane w tej ustawie uprawnienia i obowiązki:

- 1) Najwyższej Izby Kontroli – wykonują odpowiednio ABW i SKW albo Kancelaria Prezesa Rady Ministrów lub urząd obsługujący Ministra Koordynatora Służb Specjalnych;
- 2) Prezesa, Wiceprezesa i pracownika Najwyższej Izby Kontroli – wykonują odpowiednio Szef, zastępca Szefa i upoważniony funkcjonariusz ABW oraz Szef, zastępca Szefa i upoważniony funkcjonariusz lub żołnierz SKW albo Prezes Rady Ministrów lub Minister Koordynator Służb Specjalnych lub upoważniony pracownik Kancelarii Prezesa Rady Ministrów lub urzędu obsługującego Ministra Koordynatora Służb Specjalnych.

6. Czynności, o których mowa w ust. 1 pkt 1-7 i 10, dokonywane przez ABW w stosunku do Kancelarii Sejmu, Kancelarii Senatu oraz Kancelarii Prezydenta Rzeczypospolitej Polskiej są wykonywane w uzgodnieniu odpowiednio, z Marszałkiem Sejmu, Marszałkiem Senatu oraz Szefem Kancelarii Prezydenta Rzeczypospolitej Polskiej. Uzgodnienia dokonuje Prezes Rady Ministrów, a w przypadku braku uzgodnienia czynność nie może być wykonana.

7. Prezes Rady Ministrów określi, w drodze rozporządzenia:

- 1) sposób przygotowania oraz zakres i tryb przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych;
- 2) tryb uzgadniania terminu kontroli, w tym czynności, o których mowa w ust. 1 pkt 1-6 i 10, wykonywanych w stosunku do Kancelarii Sejmu, Kancelarii Senatu oraz Kancelarii Prezydenta Rzeczypospolitej Polskiej;
- 3) zadania funkcjonariuszy ABW oraz funkcjonariuszy lub żołnierzy SKW nadzorujących i wykonujących czynności kontrolne;
- 4) sposób dokumentowania czynności kontrolnych oraz sporządzania protokołu kontroli i sprawozdania z działalności kontrolnej

– uwzględniając potrzebę zapewnienia, aby zakres i sposób prowadzenia kontroli umożliwił sprawne i obiektywne ustalenie stanu faktycznego zabezpieczenia informacji niejawnych w kontrolowanej jednostce organizacyjnej oraz jego rzetelne udokumentowanie.

**Art. 13.** 1. Kierownicy jednostek organizacyjnych oraz inne instytucje i osoby współdziałają z ABW, SKW oraz służbami, o których mowa w art. 23 ust. 8, przez nieodpłatne udostępnienie lub przekazanie funkcjonariuszom, pracownikom albo żołnierzom tych służb pozostających w ich dyspozycji informacji i dokumentów lub ich kopii niezbędnych do realizacji czynności w ramach prowadzonych przez nie:

- 1) postępowań sprawdzających, kontrolnych postępowań sprawdzających, czynności, o których mowa w art. 34 ust. 1 oraz postępowań bezpieczeństwa przemysłowego;
- 2) sprawdzeń przedsiębiorcy, o których mowa w art. 65 ust. 1;
- 3) sprawdzeń wynikających z obowiązków, o których mowa w art. 15 ust. 6 i 8 oraz w art. 21 ust. 7, realizowanych przez ABW lub SKW.

2. ABW, SKW oraz służby, o których mowa w art. 23 ust. 8:

1) udostępniają sobie wzajemnie, w związku z prowadzonymi przez te służby czynnościami, o których mowa w ust. 1, pozostające w ich dyspozycji informacje i dokumenty lub ich kopie, niezbędne do realizacji tych czynności, z wyłączeniem dokumentów i informacji określonych w art. 5 ust. 1 pkt 5-7;

2) mogą zwracać się do innych służb i instytucji o udzielenie niezbędnej pomocy przy wykonywaniu czynności, o których mowa w ust. 1 pkt 1 i 2.

3. Prezes Rady Ministrów określi, w drodze rozporządzenia, szczegółowy zakres, warunki, sposób i tryb:

- 1) przekazywania oraz udostępniania ABW, SKW oraz służbom, o których mowa w art. 23 ust. 8, informacji oraz dokumentów lub ich kopii, niezbędnych dla celów realizowanych czynności, o których mowa w ust. 1,
- 2) udzielania przez Centralne Biuro Antykorupcyjne, zwane dalej "CBA", Policję, Straż Graniczną, Żandarmerię Wojskową, zwaną dalej „ŻW” oraz Krajową Administrację Skarbową niezbędnej pomocy ABW, SKW oraz służbom, o których mowa w art. 23 ust. 8 przy wykonywaniu czynności w ramach sprawdzeń, o których mowa w ust. 1

– uwzględniając zakres danych, jaki powinny zawierać wnioski o udzielenie informacji lub pomocy, a także możliwość wykorzystywania systemów informatycznych dla zapewnienia efektywności ich przekazywania i udzielania informacji.

**Art. 14.** 1. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.

2. Kierownikiem jednostki organizacyjnej może być wyłącznie osoba legitymująca się poświadczeniem bezpieczeństwa upoważniającym do dostępu do informacji niejawnych o klauzuli odpowiadającej najwyższej klauzuli tajności informacji niejawnych, które jednostka ta przetwarza lub zamierza przetwarzać lub wobec której wszczęto poszerzone postępowanie sprawdzające.

3. Kierownikiem jednostki organizacyjnej, która przetwarza lub zamierza przetwarzać informacje niejawne o klauzuli „zastrzeżone”, może być osoba legitymująca się upoważnieniem do dostępu do informacji niejawnych o tej klauzuli, wydanym przez ABW lub SKW.

4. W przypadku odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa albo upoważnienia, o którym mowa w ust. 3, kierownikowi jednostki organizacyjnej innej niż przedsiębiorca, funkcję kierownika jednostki organizacyjnej przejmuje osoba go zastępująca,

wskazana przez osobę lub organ uprawniony do obsady stanowiska, a w przypadku ich braku – przez kierownika jednostki organizacyjnej. Przepisy ust. 2 i 3 stosuje się odpowiednio.

5. W przypadku gdy kierownikiem jednostki organizacyjnej jest osoba, która objęła swą funkcję w wyniku wyborów powszechnych, do wykonywania obowiązków kierownika jednostki organizacyjnej może wyznaczyć swojego zastępcę. W przypadku takiego wyznaczenia odpowiedzialność, o której mowa w ust. 1, ponosi osoba upoważniająca. Przepisy ust. 2 i 3 stosuje się odpowiednio.

**Art. 15.** 1. Kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej "pełnomocnikiem ochrony", który odpowiada za zapewnienie przestrzegania w jednostce organizacyjnej przepisów o ochronie informacji niejawnych.

2. Pełnomocnikiem ochrony może być osoba, która:

- 1) posiada obywatelstwo polskie;
- 2) posiada wykształcenie wyższe;
- 3) posiada poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli tajności odpowiadającej najwyższej klauzuli tajności informacji, które jednostka organizacyjna przetwarza lub zamierza przetwarzać, wydane przez ABW albo SKW;
- 4) posiada aktualne zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych przeprowadzonym przez ABW albo SKW;
- 5) uzyskała pozytywną opinię Szefa ABW lub Szefa SKW, jeżeli ma zajmować stanowisko w podmiocie kluczowym dla zapewnienia bezpieczeństwa państwa z punktu widzenia ochrony informacji niejawnych, o którym mowa w ust. 14 pkt 1, z wyłączeniem ABW, SKW oraz służb, o których mowa w art. 23 ust. 8.

3. Kierownik jednostki organizacyjnej może zatrudnić zastępcę pełnomocnika ochrony. Zastępcy pełnomocnika ochrony przysługują uprawnienia pełnomocnika ochrony, chyba że kierownik jednostki organizacyjnej określi szczegółowy zakres jego zadań.

4. Zastępcą pełnomocnika ochrony może być osoba, która spełnia wymogi określone w ust. 2.

5. W przypadku wszczęcia kontrolnego postępowania sprawdzającego, a także w nagłych, nieprzewidzianych sytuacjach, uniemożliwiających wykonywanie zadań przez dotychczasowego pełnomocnika ochrony oraz braku w jednostce organizacyjnej osoby spełniającej wymogi określone w ust. 2, obowiązki pełnomocnika ochrony przejmuje kierownik jednostki organizacyjnej, z wyłączeniem prowadzenia postępowań sprawdzających. Po zaistnieniu okoliczności, o których mowa w zdaniu pierwszym, kierownik jednostki organizacyjnej niezwłocznie podejmuje działania zmierzające do powołania pełnomocnika ochrony.

6. W celu uzyskania potwierdzenia spełniania wymogów formalnych, o których mowa w ust. 2, kierownik jednostki organizacyjnej informuje odpowiednio ABW lub SKW o zamiarze zatrudnienia pełnomocnika ochrony lub jego zastępcy.

7. W informacji o zamiarze zatrudnienia, o którym mowa w ust. 6, kierownik jednostki organizacyjnej zawiera następujące dane:

- 1) nazwę jednostki organizacyjnej, w której ma być zatrudniony pełnomocnik ochrony lub jego zastępca;
- 2) następujące dane dotyczące osoby mającej objąć funkcję pełnomocnika ochrony lub jego zastępcy:
  - a) imię i nazwisko,
  - b) numer PESEL,

- c) numer posiadanego poświadczenia bezpieczeństwa, datę jego wydania oraz nazwę organu wydającego,
- d) numer posiadanego zaświadczenia o przeszkoleniu w zakresie ochrony informacji niejawnych, datę jego wydania oraz nazwę organu wydającego.

8. W stosunku do osoby, która ubiega się o stanowisko pełnomocnika ochrony lub jego zastępcy w podmiocie kluczowym dla zapewnienia bezpieczeństwa państwa z punktu widzenia ochrony informacji niejawnych, o którym mowa w ust. 14 pkt 1, kierownik jednostki organizacyjnej kieruje odpowiednio do Szefa ABW albo Szefa SKW dodatkowo wnioskiem o wydanie pozytywnej opinii, o której mowa w ust. 2 pkt 5.

9. Wniosek, o którym mowa w ust. 8, zawiera następujące dane dotyczące osoby mającej objąć funkcję pełnomocnika ochrony lub jego zastępcy:

- 1) określenie dotychczas zajmowanego przez tę osobę stanowiska wraz z wykazem jej obowiązków służbowych oraz opisem sposobu i jakości ich realizacji;
- 2) przebieg kariery zawodowej tej osoby od ukończenia 18 roku życia, zawierający wskazanie wszystkich uprzednio zajmowanych stanowisk we wszystkich uprzednich miejscach zatrudnienia oraz w obecnym miejscu zatrudnienia;
- 3) szczegółowe uzasadnienie zamiaru obsadzenia przez tę osobę stanowiska pełnomocnika ochrony lub jego zastępcy.

10. Opinię pozytywną wydaje się w terminie 30 dni od dnia otrzymania od kierownika jednostki organizacyjnej wniosku, o którym mowa w ust. 8.

11. O zatrudnieniu lub odwołaniu pełnomocnika ochrony lub jego zastępcy kierownik jednostki organizacyjnej informuje w terminie 7 dni odpowiednio ABW lub SKW, wskazując datę odpowiednio zatrudnienia lub odwołania.

12. Szef ABW lub Szef SKW może wycofać pozytywną opinię dotyczącą osoby, jeżeli nie wykonuje ona zadań określonych w ustawie albo wykonuje je niewłaściwie, narażając interes bezpieczeństwa państwa.

13. W przypadku wycofania pozytywnej opinii, kierownik jednostki organizacyjnej niezwłocznie uniemożliwia wykonywanie obowiązków służbowych na zajmowanym stanowisku osobie, której Szef ABW lub Szef SKW wycofał tę opinię.

14. Rada Ministrów określi, w drodze rozporządzenia:

- 1) rodzaje organów władzy publicznej i urzędów administracji publicznej oraz wykaz innych podmiotów kluczowych dla zapewnienia bezpieczeństwa państwa z punktu widzenia ochrony informacji niejawnych,
- 2) wzór wniosku, o którym mowa w ust. 8  
– uwzględniając konieczność określenia rodzajów podmiotów i stanowisk adekwatnie do poziomu zapewnienia bezpieczeństwa państwa.

**Art. 16. 1.** Do zadań pełnomocnika ochrony należy:

- 1) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;
- 2) zapewnienie ochrony systemów informatycznych, w których są przetwarzane informacje niejawne;
- 3) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;
- 4) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów;



- 5) opracowywanie i aktualizowanie planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji;
- 6) opracowanie dokumentacji określającej poziom zagrożeń w przypadku przetwarzania w jednostce organizacyjnej informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą;
- 7) opracowanie dokumentacji określającej sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne” w komórkach organizacyjnych;
- 8) opracowanie instrukcji określającej sposób i tryb przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony;
- 9) udział w tworzeniu instrukcji bezpieczeństwa przemysłowego w przypadku pełnomocnika ochrony jednostki organizacyjnej zawierającej z przedsiębiorcą umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej;
- 10) informowanie ABW lub SKW o zdarzeniach i okolicznościach istotnych dla bezpieczeństwa państwa;
- 11) organizowanie szkoleń w zakresie ochrony informacji niejawnych oraz wydawanie zaświadczeń potwierdzających odbycie szkolenia;
- 12) prowadzenie zwykłych postępowań sprawdzających;
- 13) prowadzenie aktualnego wykazu osób, wobec których prowadzono postępowania sprawdzające oraz kontrolne postępowania sprawdzające, a także zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, obejmującego:
  - a) imię i nazwisko,
  - b) numer PESEL,
  - c) imię ojca,
  - d) datę i miejsce urodzenia,
  - e) adres miejsca zamieszkania lub pobytu,
  - f) określenie dokumentu kończącego postępowanie sprawdzające, numer dokumentu i datę jego wydania, datę ważności poświadczenia bezpieczeństwa w zakresie najwyższej klauzuli tajności oraz nazwę organu, który wydał ten dokument,
  - g) w przypadkach zgód, o których mowa w art. 11 ust. 4 lub 5 lub art. 37 ust. 1 i 5 oraz upoważnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone”, o których mowa w art. 21 ust. 4 pkt 1 i ust. 5 - określenie nazwy dokumentu, numer dokumentu i datę jego wydania, określenie klauzuli tajności informacji niejawnych do dostępu do których uprawnienia ten dokument, datę jego ważności, nazwę organu, który go wydał oraz podstawę prawną jego wydania,
  - h) w przypadkach, o których mowa w art. 35 ust. 5, 6 i 8 - podstawę prawną dostępu do informacji niejawnych, określenie klauzuli tajności informacji niejawnych do dostępu do których osoba jest uprawniona oraz datę objęcia stanowiska związanego z dostępem do informacji niejawnych,
  - i) numer i datę wydania zaświadczenia o przeszkoleniu w zakresie ochrony informacji niejawnych oraz nazwę organu, który wydał to zaświadczenie,
  - j) zajmowane stanowisko oraz nazwę komórki i jednostki organizacyjnej, a w przypadku wykonywania czynności zleconych – nazwę jednostki organizacyjnej wykonującej czynności związane z dostępem do informacji niejawnych;
- 14) niezwłoczne przekazywanie odpowiednio do ABW albo SKW danych wymienionych w pkt 13 do prowadzonej przez te służby ewidencji osób, o której mowa w art. 77 ust. 1.

2. Dokumentacja, o której mowa w ust. 1 pkt 5-8, jest zatwierdzana przez kierownika jednostki organizacyjnej.

3. Zadania, o których mowa w ust. 1, pełnomocnik ochrony realizuje przy pomocy wyodrębnionej i podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnych, zwanej dalej "pionem ochrony", jeżeli jest ona utworzona w jednostce organizacyjnej.

4. Zadanie, o którym mowa w ust. 1 pkt 14, nie dotyczy pełnomocników ochrony w służbach, o których mowa w art. 23 ust. 8.

5. Kierownik jednostki organizacyjnej może powierzyć pełnomocnikowi ochrony, zastępcy pełnomocnika ochrony oraz pracownikom pionu ochrony wykonywanie innych zadań, jeżeli ich realizacja nie naruszy prawidłowego wykonywania zadań, o których mowa w ust. 1.

**Art. 17.** Pracownikiem pionu ochrony w jednostce organizacyjnej może być osoba, która posiada:

- 1) obywatelstwo polskie, z wyjątkiem pracowników pionu ochrony zatrudnionych u przedsiębiorców;
- 2) odpowiednie poświadczenie bezpieczeństwa lub upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone”;
- 3) aktualne zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.

**Art. 18.** 1. W przypadku uzasadnionego podejrzenia lub stwierdzenia 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 oraz ograniczenia jego negatywnych skutków.

2. W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli "poufne" lub wyższej pełnomocnik ochrony zawiadamia niezwłocznie odpowiednio ABW lub SKW, podając dane, o których mowa w art. 16 ust. 1 pkt 13 lit. a, b oraz j, osoby, która dopuściła się, bądź mogła dopuścić się tych naruszeń.

**Art. 19.** Minister Obrony Narodowej określi, w drodze rozporządzenia:

- 1) szczegółowe zadania pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych jemu podległych lub przez niego nadzorowanych;
- 2) szczególne wymagania dotyczące stosowania środków bezpieczeństwa fizycznego przeznaczonych do ochrony informacji niejawnych;
- 3) miejsce i rolę Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz pełnomocników ochrony kierowników bezpośrednio nadrzędnych jednostek organizacyjnych w resortowym systemie ochrony informacji niejawnych;
- 4) zakres, tryb i sposób współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych z SKW;
- 5) rodzaje, szczegółowe cele oraz sposób organizacji szkoleń w zakresie ochrony informacji niejawnych;
- 6) zakres stosowania środków bezpieczeństwa fizycznego oraz kryteria tworzenia stref ochronnych;
- 7) tryb opracowywania oraz niezbędne elementy planów ochrony informacji niejawnych, w tym postępowanie z materiałami zawierającymi informacje niejawne oznaczone klauzulą "tajne" lub "ściśle tajne" w razie wprowadzenia stanu nadzwyczajnego, a także sposób nadzorowania ich realizacji

- uwzględniając nadrzędną rolę Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych w koordynowaniu i nadzorowaniu przedsięwzięć w zakresie ochrony informacji niejawnych, w celu zapewnienia jednolitego i skutecznego systemu ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.

**Art. 20.** 1. Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się po uzyskaniu poświadczenia bezpieczeństwa lub innego określonego w ustawie uprawnienia do dostępu do informacji niejawnych albo w trakcie procedury ich uzyskiwania, 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, z uwzględnieniem zasad ich przetwarzania, w tym w systemach informatycznych;
- 3) sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.

2. Szkolenie w zakresie ochrony informacji niejawnych:

- 1) przeprowadzają, odpowiednio ABW lub SKW, dla:
  - a) pełnomocnika ochrony i jego zastępcy oraz osób przewidzianych na te stanowiska,
  - b) przedsiębiorców wykonujących działalność jednoosobowo i osobiście,
  - c) kierowników przedsiębiorców, u których nie zatrudniono pełnomocnika ochrony,
  - d) kierownika jednostki organizacyjnej, która przetwarza informacje niejawne o klauzuli „ściśle tajne” lub „tajne” - wspólnie z pełnomocnikiem ochrony, jeżeli został zatrudniony;
- 2) organizuje pełnomocnik ochrony jednostki organizacyjnej zlecającej realizację umowy, z której wykonaniem łączy się dostęp do informacji niejawnych dla:
  - a) przedsiębiorców wykonujących działalność jednoosobowo i osobiście,
  - b) kierowników przedsiębiorców, u których nie zatrudniono pełnomocnika ochrony ;
- 3) organizuje pełnomocnik ochrony – dla pozostałych osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w jednostce organizacyjnej, a także wobec pracowników przedsiębiorcy, z którym zawarto umowę, z której wykonaniem łączy się dostęp do informacji niejawnych, a u którego nie zatrudniono pełnomocnika ochrony;
- 4) przeprowadza ABW – dla posłów i senatorów.

3. W szczególnie uzasadnionych przypadkach szkolenie w zakresie ochrony informacji niejawnych, o którym mowa w ust. 2 pkt 1 lit. d, może być przeprowadzone odrębnie przez ABW lub SKW oraz pełnomocnika ochrony.

4. Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się nie rzadziej niż raz na 5 lat. Można odstąpić od przeprowadzenia szkolenia, jeżeli osoba podejmująca pracę lub rozpoczynająca pełnienie służby albo wykonywanie czynności zleconych przedstawi pełnomocnikowi ochrony aktualne zaświadczenie o odbyciu szkolenia.

5. Szkolenie w zakresie ochrony informacji niejawnych kończy się wydaniem zaświadczenia. Odbierając zaświadczenie, osoba przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.

6. ABW i SKW organizują i prowadzą specjalistyczne szkolenie z zakresu bezpieczeństwa informatycznego. Szkolenie to:

- 1) kończy się wydaniem zaświadczenia;
- 2) przeprowadza się nie rzadziej niż raz na 5 lat.

7. Wzajemne prawa i obowiązki podmiotu przeprowadzającego szkolenie, uczestnika szkoleń, o których mowa w ust. 2 pkt 1 i 2 oraz ust. 6, a także jednostki organizacyjnej, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje czynności zlecone, określa umowa zawarta między tym podmiotem, uczestnikiem szkolenia oraz jednostką organizacyjną.

8. Prezes Rady Ministrów określi w drodze rozporządzenia wzory zaświadczeń stwierdzających odbycie:

- 1) szkolenia w zakresie ochrony informacji niejawnych,
  - 2) specjalistycznego szkolenia z zakresu bezpieczeństwa informatycznego
- uwzględniając odrębności wynikające z wydawania zaświadczeń przez ABW i SKW oraz pełnomocników ochrony.

## Rozdział 4

### 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. 35 ust. 5 i 6 lub art. 37 ust. 1 i 5, po:

- 1) uzyskaniu poświadczenia bezpieczeństwa;
- 2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.

2. Informacje niejawne mogą być udostępnione wyłącznie osobie spełniającej wymogi określone w ustawie i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych.

3. Osoby nieposiadające obywatelstwa polskiego nie mogą być dopuszczone do pracy lub pełnienia służby na stanowiskach albo wykonywania czynności zleconych, z którymi łączy się dostęp do informacji niejawnych o klauzuli "tajne" lub "ściśle tajne".

4. Przepisu ust. 3 nie stosuje się do osób:

- 1) zajmujących stanowiska związane z wykonywaniem przez przedsiębiorcę umowy związanej z dostępem do informacji niejawnych albo wykonujących zadania na rzecz obronności lub bezpieczeństwa państwa, związane z dostępem do informacji niejawnych u przedsiębiorcy;
- 2) które w imieniu przedsiębiorcy, o którym mowa w pkt 1, uczestniczą w czynnościach zmierzających do zawarcia umowy, jeżeli czynności te są związane z dostępem do informacji niejawnych;
- 3) zatrudnionych w pionie ochrony przedsiębiorcy, o którym mowa w pkt 1, z wyjątkiem osoby zajmującej stanowisko pełnomocnika ochrony oraz zastępcy pełnomocnika ochrony.

5. Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac, związanych z dostępem danej osoby do informacji niejawnych o klauzuli "zastrzeżone", w przypadku gdy nie posiada ona poświadczenia bezpieczeństwa, może nastąpić po:

- 1) pisemnym upoważnieniu przez kierownika jednostki organizacyjnej;
- 2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.

6. Kierownikowi jednostki organizacyjnej oraz przedsiębiorcy wykonującemu działalność jednoosobowo i osobiście, upoważnienie, o którym mowa w ust. 5 pkt 1, wydaje ABW albo SKW.

7. Odpowiednio, kierownik jednostki organizacyjnej oraz ABW albo SKW w odniesieniu do osoby, o której mowa w ust. 6:

- 1) może odmówić wydania upoważnienia, a wydane cofnąć;

2) nie wydaje upoważnienia, a wydane cofa, jeśli została ona skazana prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe – co nie wymaga uzasadnienia.

8. W celu weryfikacji występowania okoliczności, o których mowa w ust. 7 pkt 2, pełnomocnik ochrony oraz ABW albo SKW w odniesieniu do osób, o których mowa w ust. 6, dokonuje sprawdzenia w Krajowym Rejestrze Karnym danych osoby ubiegającej się o dostęp do informacji o klauzuli „zastrzeżone”. Jeśli w jednostce organizacyjnej nie powołano pełnomocnika ochrony, sprawdzenia tego dokonuje pełnomocnik ochrony jednostki organizacyjnej, w której dana osoba ma mieć dostęp do informacji niejawnych. Art. 60 ust. 2 stosuje się odpowiednio. W odniesieniu do osób, o których mowa w ust. 6, ABW albo SKW dokonują także sprawdzenia w niejawnych ewidencjach i kartotekach oraz innych niejawnych zasobach informacyjnych.

9. Pełnomocnik ochrony jednostki organizacyjnej oraz ABW i SKW przechowują przez 10 lat dokumentację czynności związanych z weryfikacją, o której mowa w ust. 8.

10. Upoważnienie wydane przez kierownika jednostki organizacyjnej zachowuje ważność wyłącznie w okresie pracy, służby lub wykonywania prac zleconych przez daną osobę w tej jednostce organizacyjnej, nie dłużej jednak niż przez 10 lat od dnia jego wydania. Przepis ten stosuje się odpowiednio w stosunku do upoważnienia wydanego kierownikowi jednostki organizacyjnej przez ABW albo SKW.

11. Przepisu ust. 10 nie stosuje się do upoważnienia wydanego przez ABW albo SKW przedsiębiorcy wykonującemu działalność jednoosobowo i osobiście. Upoważnienie takie zachowuje ważność przez okres 10 lat od dnia jego wydania.

12. Jeżeli przepisy odrębnych ustaw uprawniają organy, służby lub instytucje albo ich upoważnionych pracowników do dokonywania kontroli, w szczególności do swobodnego dostępu do pomieszczeń i materiałów, a jej zakres dotyczy informacji niejawnych, uprawnienia te są realizowane z zachowaniem przepisów niniejszej ustawy.

**Art. 22.** W zależności od stanowiska lub wykonywania czynności zleconych, o które ubiega się osoba, zwana dalej "osobą sprawdzaną", przeprowadza się:

- 1) zwykle postępowanie sprawdzające – przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli "poufne", z wyłączeniem stanowisk i prac, o których mowa w pkt 2 lit. b-c;
- 2) poszerzone postępowanie sprawdzające:
  - a) przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli "tajne" lub "ściśle tajne",
  - b) wobec pełnomocnika ochrony, zastępcy pełnomocnika ochrony oraz administratora systemu, a także kandydatów na te stanowiska, także w sytuacji, gdy pełnią lub będą pełnić swą funkcję w jednostce organizacyjnej przetwarzającej informacje niejawne wyłącznie o klauzuli „zastrzeżone”,
  - c) wobec kierowników jednostek organizacyjnych, w których są przetwarzane informacje niejawne o klauzuli "poufne" lub wyższej,
  - d) wobec osób ubiegających się o dostęp do informacji niejawnych międzynarodowych Organizacji Traktatu Północnoatlantyckiego, zwanej dalej „NATO”, Unii Europejskiej, zwanej dalej „UE” lub Europejskiej Agencji Kosmicznej, zwanej dalej „ESA” o klauzuli równorzędnej klauzuli „poufne” lub wyższej, stosowanej przez te organizacje.

**Art. 23.** 1. Pełnomocnik ochrony przeprowadza zwykłe postępowanie sprawdzające na pisemne polecenie kierownika jednostki organizacyjnej, wyłącznie wobec osób zatrudnionych w jednostce organizacyjnej, w której pełni swoją funkcję lub osób, którym jednostka ta zleciła wykonanie czynności, z zastrzeżeniem art. 60 ust. 2.

2. Pełnomocnik ochrony pełniący swą funkcję u przedsiębiorcy przeprowadza zwykłe postępowanie sprawdzające wyłącznie w okresie ważności świadectwa bezpieczeństwa przemysłowego lub po wszczęciu postępowania bezpieczeństwa przemysłowego.

3. ABW albo SKW przeprowadzają:

- 1) poszerzone postępowania sprawdzające na pisemny wniosek:
  - a) kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska lub zlecenia prac;
  - b) instytucji organizacji międzynarodowej bądź krajowej władzy bezpieczeństwa państwa członkowskiego NATO, UE lub ESA;
- 2) postępowania sprawdzające na pisemny wniosek lub polecenie odpowiednio wobec:
  - a) funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy w ABW albo SKW;
  - b) osób wykonujących czynności zlecone lub ubiegających się o wykonywanie tych czynności na rzecz ABW albo SKW.

4. Wniosek, o którym mowa w ust. 3 pkt 1 lit. a, zawiera uzasadnienie ze wskazaniem zadań, jakie wykonuje lub będzie wykonywać osoba ubiegająca się o wydanie poświadczenia bezpieczeństwa oraz rodzaju informacji niejawnych, o których mowa w art. 5 ust. 1-4 oraz informacji niejawnych międzynarodowych, do których osoba ta ma lub będzie mieć dostęp w związku z realizacją tych zadań. W szczególnie uzasadnionych przypadkach ABW albo SKW mogą zwrócić się do wnioskodawcy o przekazanie szczegółowego uzasadnienia wniosku. W przypadku postępowań, o których mowa w art. 57 ust. 3 oraz przedsiębiorcy wykonującego działalność jednoosobowo i osobiście, uzasadnienie nie jest wymagane.

5. ABW przeprowadza poszerzone postępowania sprawdzające wobec:

- 1) Szefa SKW, Szefa Agencji Wywiadu, zwanej dalej "AW", Szefa CBA, Komendanta Służby Ochrony Państwa, zwanej dalej „SOP”, Komendanta Głównego Policji, Dyrektora Generalnego Służby Więziennej, Komendanta Głównego Straży Granicznej oraz osób przewidzianych na te stanowiska lub którym powierzono wykonywanie obowiązków na tych stanowiskach;
- 2) pełnomocnika ochrony, zastępcy pełnomocnika ochrony oraz osób przewidzianych na te stanowiska lub którym powierzono wykonywanie obowiązków na tych stanowiskach w SKW, AW, CBA, SOP, Policji, Służbie Więziennej oraz Straży Granicznej.

6. SKW przeprowadza poszerzone postępowania sprawdzające wobec:

- 1) Szefa ABW, Szefa SWW, Komendanta Głównego ŻW oraz osób przewidzianych na te stanowiska lub którym powierzono wykonywanie obowiązków na tych stanowiskach;
- 2) pełnomocnika ochrony, zastępcy pełnomocnika ochrony oraz osób przewidzianych na te stanowiska lub którym powierzono wykonywanie obowiązków na tych stanowiskach w ABW, SWW oraz ŻW.

7. Osoby mianowane na stanowiska, o których mowa w ust. 5 pkt 1 i 2, muszą posiadać poświadczenie bezpieczeństwa wydane przez ABW, jeśli objęte są postępowaniem sprawdzającym prowadzonym przez ABW, a osoby mianowane na stanowiska, o których mowa w ust. 6 pkt 1 i 2, muszą posiadać poświadczenie bezpieczeństwa wydane przez SKW, jeśli objęte są postępowaniem sprawdzającym prowadzonym przez SKW.

8. AW, SWW, CBA, SOP, Policja, ŻW, Służba Więzienna i Straż Graniczna przeprowadzają na piśmie wniosek lub polecenie, postępowania sprawdzające wobec:

- 1) własnych funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy,
- 2) osób wykonujących na ich rzecz czynności zlecone lub ubiegających się o wykonywanie tych czynności

– z wyłączeniem postępowań, o których mowa w ust. 5 i 6 oraz art. 22 pkt 2 lit. b i d, a także z wyłączeniem okoliczności, o których mowa w art. 10 ust. 4 pkt 3 i 4.

9. Organami uprawnionymi do prowadzenia postępowań sprawdzających w służbach, o których mowa w ust. 8 są powoływani w nich pełnomocnicy ochrony.

10. Służbom, o których mowa w ust. 8, przysługują uprawnienia ABW oraz SKW w ramach postępowań sprawdzających oraz kontrolnych postępowań sprawdzających przeprowadzanych przez te służby.

**Art. 24.** 1. Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

2. W toku postępowania sprawdzającego ustala się, czy osoba sprawdzana została skazana prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe oraz została oskarżona lub nieprawomocnie skazana albo przedstawiono jej zarzut popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3, a także czy istnieją uzasadnione wątpliwości dotyczące:

- 1) uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko bezpieczeństwu lub porządkowi ustrojowemu Rzeczypospolitej Polskiej lub bezpieczeństwu jej sojuszników;
- 2) zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu;
- 3) uczestnictwa w działalności, współpracy lub popierania przez osobę sprawdzaną organizacji, o których mowa w art. 13 Konstytucji Rzeczypospolitej Polskiej albo zorganizowanych grup przestępczych;
- 4) świadomego ukrywania lub podawania przez osobę sprawdzaną w ankiecie bezpieczeństwa osobowego, zwanej dalej "ankietą", lub postępowaniu sprawdzającym niepełnych lub niezgodnych z prawdą informacji mających znaczenie dla ochrony informacji niejawnych;
- 5) wystąpienia związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji;
- 6) niewłaściwego postępowania osoby sprawdzanej z informacjami prawnie chronionymi w okresie ostatnich 10 lat poprzedzających wszczęcie postępowania, a w szczególności z informacjami niejawnymi, w tym naruszenia przepisów ustawy lub niewypełnienia albo rażąco nieprawidłowego wykonania wynikających z niej obowiązków, jeżeli:
  - a) doprowadziło to bezpośrednio do ujawnienia tych informacji osobom nieuprawnionym,
  - b) było to wynikiem celowego działania,
  - c) stwarzało zagrożenie ich nieuprawnionego ujawnienia mogącego skutkować szkodą dla ich ochrony i nie miało charakteru incydentalnego,
  - d) dopuścił się tego kierownik jednostki organizacyjnej, pełnomocnik ochrony lub jego zastępca, kierownik kancelarii tajnej lub jego zastępca oraz administrator systemu i

inspektor bezpieczeństwa informatycznego, nie miało to charakteru incydentalnego i mogło skutkować szkodą dla ochrony tych informacji;

- 7) informacji o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do wykonywania prac związanych z dostępem do informacji niejawnych;
- 8) uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych albo mających znaczenie dla ochrony informacji niejawnych uzależnień behawioralnych, w szczególności od hazardu.

3. W toku poszerzonego postępowania sprawdzającego ustala się ponadto, czy istnieją wątpliwości dotyczące wystąpienia związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji, wynikające z sytuacji majątkowej osoby sprawdzanej, a w szczególności:

- 1) poziomu życia nieadekwatnego do udokumentowanych dochodów legalnego pochodzenia uzyskiwanych przez osobę sprawdzaną oraz osoby prowadzące wraz z nią wspólne gospodarstwo domowe a także pozostające na jej utrzymaniu;
- 2) posiadania przez osobę sprawdzaną oraz osoby prowadzące wraz z nią wspólne gospodarstwo domowe zobowiązań finansowych, których nie są one w stanie na bieżąco regulować z udokumentowanych dochodów legalnego pochodzenia.

4. W razie niedających 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 rzetelnie udokumentować czynności przeprowadzone w toku postępowania sprawdzającego oraz wykazać najwyższą staranność w toku prowadzonego postępowania sprawdzającego co do jego zgodności z przepisami ustawy.

6. Wszystkie czynności przeprowadzone w toku postępowań sprawdzających powinny być zakończone przed upływem 6 miesięcy od daty:

- 1) złożenia do pełnomocnika ochrony wypełnionej ankiety, w przypadku zwykłego postępowania sprawdzającego;
- 2) wszczęcia poszerzonego postępowania sprawdzającego, z wyłączeniem postępowań, o których mowa w art. 57 ust. 3;
- 3) wniesienia przez przedsiębiorcę opłaty za przeprowadzenie czynności w ramach poszerzonych postępowań sprawdzających.

7. W przypadku niedotrzymania terminu, o którym mowa w ust. 6, organ prowadzący postępowanie informuje, na wniosek osoby sprawdzanej, o przewidywanym terminie zakończenia postępowania oraz - jeżeli nie naruszy to zasad ochrony informacji niejawnych - o powodach przedłużania się postępowania.

8. Przeprowadzenie postępowania sprawdzającego wymaga pisemnej zgody osoby, której ma dotyczyć.

9. Zbieranie i przetwarzanie informacji o osobach trzecich może odbywać się bez wiedzy i zgody tych osób, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy. Informacje o osobach trzecich mogą być zbierane i przetwarzane wyłącznie w zakresie określonym w ust. 2 pkt 1-5 oraz w ust. 3, przy zastosowaniu art. 26 ust. 2 pkt 3.

10. W celu weryfikacji informacji uzyskanych w toku postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego oraz wynikających z nich wniosków i hipotez, mogących mieć wpływ na ocenę dawania rękojmi zachowania tajemnicy przez osobę sprawdzaną albo w celu ścigania za popełnienie przestępstwa lub przestępstwa skarbowego, organ prowadzący



postępowanie może w treści dokonywanego sprawdzenia lub po zakończeniu postępowania przekazać właściwemu organowi informacje lub kopie dokumentów, uzyskanych w jego trakcie.

11. Ankieta po wypełnieniu stanowi tajemnicę prawnie chronioną i po jej przekazaniu do organu prowadzącego postępowanie sprawdzające włączana jest do akt postępowania. Wzór ankiety wraz z instrukcją jej wypełnienia stanowi załącznik do ustawy.

**Art. 25.** 1. Zwykle postępowanie sprawdzające, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, obejmuje czynności:

- 1) sprawdzenia w ewidencjach, rejestrach i kartotekach, w szczególności w Krajowym Rejestrze Karnym oraz innych zasobach informacyjnych, zwane dalej „sprawdzeniami w ewidencjach”,
- 2) sprawdzenia w niejawnych ewidencjach i kartotekach oraz innych niejawnych zasobach informacyjnych, w szczególności służb specjalnych i Policji, zwane dalej „sprawdzeniami w ewidencjach niejawnych”

– danych zawartych w ankiecie wypełnionej i podpisanej przez osobę sprawdzaną, a także uzyskanie informacji lub sprawdzenie innych danych uzyskanych w toku postępowania sprawdzającego.

2. Sprawdzenia w ewidencjach niejawnych są prowadzone na pisemny wniosek pełnomocnika ochrony przez ABW albo SKW. Dla celów sprawdzenia pełnomocnik ochrony przekazuje do ABW lub SKW kopię części III i IV ankiety lub informacje tam zawarte.

3. W ramach realizacji skierowanego przez pełnomocnika ochrony wniosku, o którym mowa w ust. 2, ABW albo SKW może przeprowadzić rozmowę z osobą sprawdzaną w celu usunięcia nieścisłości lub sprzeczności powstałych w wyniku sprawdzeń w ewidencjach niejawnych.

4. ABW albo SKW przekazuje pełnomocnikowi ochrony informacje uzyskane w wyniku sprawdzeń w ewidencjach niejawnych oraz rozmowy, o której mowa w ust. 3. W przypadku, gdy przekazanie tych informacji byłoby sprzeczne z zasadami ochrony informacji niejawnych, ABW albo SKW przekazuje pełnomocnikowi ochrony jedynie opinię dotyczącą dawania przez osobę sprawdzaną rękojmi zachowania tajemnicy.

5. W toku postępowania sprawdzającego można przeprowadzić rozmowę z:

- 1) osobą sprawdzaną, w celu usunięcia powstałych wątpliwości;
- 2) osobami nieobjętymi tym postępowaniem, w celu uzyskania informacji mogących mieć wpływ na ocenę dawania rękojmi zachowania tajemnicy przez osobę sprawdzaną.

6. Jeżeli w toku zwykłego postępowania sprawdzającego wystąpią wątpliwości niepozwalające 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. Z przebiegu wysłuchania sporządza się protokół, który podpisują osoba prowadząca wysłuchanie, osoba wysłuchana oraz pełnomocnik, jeżeli w nim uczestniczył.

7. Organ prowadzący zwykle postępowanie sprawdzające odstępuje od przeprowadzenia wysłuchania, jeżeli:

- 1) jego przeprowadzenie wiązałoby się z ryzykiem ujawnienia informacji niejawnych osobie nieuprawnionej;
- 2) postępowanie sprawdzające doprowadziło do niebudzącego wątpliwości ustalenia, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy;
- 3) ustalono występowanie wątpliwości, o których mowa w art. 24 ust. 2 pkt 7 lub 8.

8. W celu usunięcia wątpliwości, o których mowa w art. 24 ust. 2 pkt 7 lub 8, organ prowadzący postępowanie sprawdzające może zobowiązać osobę sprawdzaną do poddania się badaniu specjalistycznemu oraz udostępnienia jego wyników.

9. Prezes Rady Ministrów określi, w drodze rozporządzenia, szczegółowy zakres, warunki, sposób i tryb zobowiązania do poddania się badaniu specjalistycznemu i jego przeprowadzenia, uwzględniając pewność uzyskania przez lekarza wykonującego badanie wszystkich niezbędnych informacji i dokumentów niezbędnych do postawienia właściwej diagnozy oraz posiadanie przez niego niezbędnej wiedzy w zakresie ochrony informacji niejawnych i wpływu postawionej diagnozy na skuteczność tej ochrony.

**Art. 26.** 1. Poszerzone postępowanie sprawdzające obejmuje sprawdzenia w ewidencjach oraz sprawdzenia w ewidencjach niejawnych.

2. Jeżeli jest to konieczne w związku z uzyskanymi informacjami poszerzone postępowanie sprawdzające może obejmować także:

- 1) rozmowy, o których mowa w art. 25 ust. 5;
- 2) przeprowadzenie wywiadu w miejscach aktywności życiowej, w tym zamieszkania, osoby sprawdzanej;
- 3) uzyskanie informacji lub kopii dokumentów dotyczących stanu i historii obrotów na rachunku bankowym, a w szczególności salda po operacji, daty, kwoty, typu i tytułu operacji, w tym wszystkich jej szczegółów wraz z opisem, włącznie z danymi rachunku przeciwstawnego i jego właściciela, a także informacji lub kopii dokumentów dotyczących innych produktów bankowych lub innych instrumentów finansowych, jak również posiadanego majątku, prowadzonej działalności gospodarczej, dokonanych czynności majątkowych, w szczególności transakcji zbycia, nabycia lub zamiany majątku, ustanowienia hipoteki, posiadanych zobowiązań finansowych, prowadzonych postępowań karno-skarbowych oraz uzyskanych dochodów osoby sprawdzanej, jej małżonka lub partnera życiowego oraz osób, z którymi prowadzi ona wspólne gospodarstwo domowe lub które pozostają na jej utrzymaniu, albo są współwłaścicielami rachunku bankowego, a także innych osób, o ile w toku postępowania zostanie ustalone, że należące do nich środki lub inny majątek stanowiły źródło finansowania poziomu życia osoby sprawdzanej albo majątku, z którego ona bezpośrednio korzysta.

3. Do wywiadu w miejscach aktywności życiowej przepisy ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego i wydane na jej podstawie przepisy dotyczące wywiadu środowiskowego stosuje się odpowiednio.

4. Czynności, o których mowa w ust. 2 pkt 3, są wykonywane zgodnie z art. 105 ust. 1 pkt 2 lit. k ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2018 r. poz. 2187, 2243 i 2354). Przepisy art. 82 § 1 pkt 1, art. 182 § 1-3a, 5 i 6 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2018 r. poz. 800, z późn. zm.<sup>4</sup>) oraz art. 48 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2018 r. poz. 508 z późn. zm.<sup>5</sup>), dotyczące zakresu przekazywanych informacji, a także dotyczące uprawnień przysługujących organom podatkowym lub organom kontroli skarbowej, stosuje się do poszerzonych postępowań sprawdzających i służb prowadzących takie postępowania.

---

<sup>4</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. poz. 650, 723, 771, 1000, 1039, 1075, 1499, 1540, 1544, 1629 i 1693.

<sup>5</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. poz. 650, 723, 1000, 1039, 1499, 1544, 1577, 1654, 2193, 2245, 2354 oraz z 2019 r. poz. 53.

5. Poszerzone postępowanie sprawdzające obejmuje:

- 1) wysłuchanie, o którym mowa w art. 25 ust. 6,
- 2) zobowiązanie osoby sprawdzanej do poddania się badaniu specjalistycznemu oraz udostępnienia jego wyników, o którym mowa w art. 25 ust. 8  
- w przypadku wystąpienia okoliczności określonych w tych przepisach.

6. W przypadku osób ubiegających się o uzyskanie dostępu do informacji o klauzuli "ściśle tajne" poszerzone postępowanie sprawdzające obejmuje także, jeżeli jest to konieczne w wyniku uzyskanych wcześniej informacji, rozmowę z trzema osobami wskazanymi przez osobę sprawdzaną, w celu uzyskania innych informacji mogących mieć znaczenie dla oceny dawania rękojmi zachowania tajemnicy.

7. W celu wyjaśnienia wątpliwości, o których mowa w art. 24 ust. 2 pkt 1-6 oraz ust. 3, organ prowadzący postępowanie sprawdzające może, na pisemny wniosek osoby sprawdzanej, zlecić przeprowadzenie badania poligraficznego w tym zakresie.

8. Organ prowadzący postępowanie sprawdzające może zobowiązać osobę sprawdzaną do poddania się badaniu poligraficznemu w przypadku ustalenia wątpliwości, o których mowa w art. 24 ust. 2:

- 1) pkt 1-3;
- 2) pkt 6 lit. a-c – wyłącznie w zakresie związanym z niewłaściwym postępowaniem z informacjami niejawnymi.

9. Badanie, o którym mowa w ust. 7 lub 8, może zostać przeprowadzone wyłącznie przez ABW, SKW lub służbę, o której mowa w art. 23 ust. 8.

10. Badania, o którym mowa w ust. 7 lub 8, nie przeprowadza się w przypadku wystąpienia okoliczności, o których mowa w art. 25 ust. 7.

**Art. 27.** 1. Postępowanie sprawdzające może zostać zawieszona w przypadku:

- 1) trwającej powyżej 30 dni 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 lub umyślne przestępstwo skarbowe.

2. Zawieszona 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.

3. Postanowienie o zawieszeniu, podjęciu i odmowie podjęcia postępowania sprawdzającego organ prowadzący postępowanie sprawdzające doręcza wnioskodawcy, pełnomocnikowi ochrony i osobie sprawdzanej.

4. W okresie zawieszenia postępowania organ prowadzący postępowanie może podejmować czynności mające na celu ustalenie, czy zachodzą okoliczności mogące stanowić podstawę do podjęcia zawieszona postępowania lub jeżeli przeprowadzenie tych czynności jest niezbędne dla interesu ochrony informacji niejawnych.

**Art. 28.** Postępowanie sprawdzające kończy się:

- 1) wydaniem poświadczenia bezpieczeństwa;
- 2) decyzją o odmowie wydania poświadczenia bezpieczeństwa;

3) decyzją o umorzeniu postępowania.

**Art. 29.** 1. Po zakończeniu postępowania sprawdzającego z wynikiem pozytywnym organ prowadzący postępowanie wydaje poświadczenie bezpieczeństwa i przekazuje je osobie sprawdzanej, zawiadamiając o tym wnioskodawcę.

2. Poświadczenie bezpieczeństwa zawiera:

- 1) numer poświadczenia;
- 2) podstawę prawną;
- 3) określenie organu, który przeprowadził postępowanie sprawdzające;
- 4) datę i miejsce wydania;
- 5) imię, nazwisko i numer PESEL, a w przypadku jego braku – datę urodzenia osoby sprawdzanej;
- 6) wskazanie przeprowadzenia postępowania sprawdzającego wraz z klauzulą tajności informacji niejawnych, do których osoba sprawdzana może mieć dostęp;
- 7) stwierdzenie, że osoba sprawdzana daje rękojmię zachowania tajemnicy;
- 8) termin ważności;
- 9) imię, nazwisko, stopień służbowy, stanowisko służbowe i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo imię, nazwisko i podpis pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające;
- 10) pouczenie o treści ust. 5 i 6, w przypadku, gdy postępowanie sprawdzające było prowadzone przez służbę, o której mowa w art. 23 ust. 8.

3. Poświadczenie bezpieczeństwa wydaje się na okres:

- 1) 10 lat - w przypadku dostępu do informacji niejawnych o klauzuli "poufne";
- 2) 7 lat - w przypadku dostępu do informacji niejawnych o klauzuli "tajne";
- 3) 5 lat - w przypadku dostępu do informacji niejawnych o klauzuli "ściśle tajne".

4. Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o wyższej klauzuli tajności uprawnia do dostępu do informacji niejawnych o niższej klauzuli tajności, odpowiednio przez okresy, o których mowa w ust. 3, także w odniesieniu do poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych organizacji międzynarodowej, zwanego dalej „poświadczeniem bezpieczeństwa organizacji międzynarodowej”.

5. Poświadczenia bezpieczeństwa wydane w wyniku postępowania sprawdzającego przeprowadzonego przez służby, o których mowa w art. 23 ust. 8, zachowują ważność wyłącznie w okresie zatrudnienia w służbie, która przeprowadziła postępowanie sprawdzające.

6. Szef ABW, Szef SKW lub szef służby, o której mowa w art. 23 ust. 8, może uznać za odpowiednie także w zakresie dostępu do informacji niejawnych o klauzuli „tajne” lub „ściśle tajne” poświadczenie bezpieczeństwa wydane w wyniku postępowania sprawdzającego, przeprowadzonego przez służby, o których mowa w art. 23 ust. 8, posiadane przez osobę ubiegającą się o zatrudnienie lub przyjęcie do podległej mu służby.

7. Osobom wskazanym w art. 22 pkt 2 lit. b-d, wydaje się poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o takiej klauzuli, jaka została wskazana we wniosku o przeprowadzenie postępowania sprawdzającego.

8. Pełnomocnikowi ochrony, zastępcy pełnomocnika ochrony, administratorowi systemu lub inspektorowi bezpieczeństwa informatycznego oraz kandydatom na te stanowiska, w sytuacji, gdy pełnią lub będą pełnił swą funkcję w jednostce organizacyjnej przetwarzającej informacje niejawne wyłącznie o klauzuli „zastrzeżone”, wydaje się poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „poufne”.

9. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory:

- 1) poświadczenia bezpieczeństwa;
  - 2) poświadczeń bezpieczeństwa organizacji międzynarodowych
- uwzględniając we wzorach poświadczeń bezpieczeństwa dane określone w ust. 2 oraz zapewni zróżnicowanie wzorów poświadczeń bezpieczeństwa wydawanych przez ABW, SKW, służby określone w art. 23 ust. 8 oraz pełnomocników ochrony.

**Art. 30.** 1. Organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa, jeżeli:

- 1) nie zostały usunięte wątpliwości, o których mowa w art. 24 ust. 2 lub 3;
- 2) potwierdzono występowanie okoliczności, o których mowa w art. 24 ust. 2 lub 3;
- 3) osoba sprawdzana została skazana prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe;
- 4) osoba sprawdzana była zatrudniona lub współpracowała z organami bezpieczeństwa, o których mowa w art. 2 ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa wewnętrznego państwa z lat 1944-1990 oraz treści tych dokumentów (Dz. U. z 2017 r. poz. 2186 z późn. zm.<sup>6</sup>).

2. Organ prowadzący postępowanie sprawdzające może odmówić wydania poświadczenia bezpieczeństwa, jeżeli osoba sprawdzana została oskarżona lub nieprawomocnie skazana albo przedstawiono jej zarzut popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3.

3. Pełnomocnik ochrony odmawia wydania poświadczenia bezpieczeństwa w przypadku uzyskania w trybie określonym w art. 25 ust. 4, informacji o tym, że w opinii ABW lub SKW osoba sprawdzana nie daje rękojmi zachowania tajemnicy ze względu na występowanie okoliczności wywołujących wątpliwości, o których mowa w art. 24 ust. 2 lub 3.

4. Decyzja o odmowie wydania poświadczenia bezpieczeństwa zawiera:

- 1) podstawę prawną oraz uzasadnienie faktyczne i prawne;
- 2) wskazanie wnioskodawcy postępowania sprawdzającego;
- 3) określenie organu, który przeprowadził postępowanie sprawdzające;
- 4) datę i miejsce wydania;
- 5) imię, nazwisko i numer PESEL, a w przypadku jego braku – datę urodzenia osoby sprawdzanej;
- 6) wskazanie przeprowadzenia postępowania sprawdzającego oraz określenie rodzaju przeprowadzonego postępowania;
- 7) stwierdzenie, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy;
- 8) imię, nazwisko, stopień służbowy, stanowisko służbowe i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo imię, nazwisko i podpis pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające;
- 9) pouczenie o dopuszczalności i terminie wniesienia odwołania odpowiednio do Prezesa Rady Ministrów albo Ministra Koordynatora Służb Specjalnych, jeżeli został powołany, a także o treści ust. 10 w przypadku, gdy postępowanie sprawdzające było prowadzone przez ABW, SKW lub służbę, o której mowa w art. 23 ust. 8.

---

<sup>6</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 538, 650, 651, 730, 1000, 1349, 1669, 1735, 2270 oraz z 2019 r. poz. 8 i 9.

5. Uzasadnienie faktyczne w części zawierającej informacje niejawne podlega ochronie na zasadach określonych w ustawie.

6. Po zakończeniu postępowania sprawdzającego z wynikiem negatywnym organ prowadzący postępowanie wydaje decyzję o odmowie wydania poświadczenia bezpieczeństwa i doręcza ją osobie sprawdzanej. Informację o decyzji o odmowie wydania poświadczenia bezpieczeństwa oraz o prawnej podstawie tej decyzji przekazuje się kierownikowi jednostki organizacyjnej lub osobie uprawnionej do obsady stanowiska oraz podmiotom, które wydały tej osobie poświadczenia bezpieczeństwa lub upoważnienia do dostępu do informacji niejawnych o klauzuli "zastrzeżone", które były ważne w chwili zakończenia tego postępowania.

7. Kierownik jednostki organizacyjnej lub osoba uprawniona do obsady stanowiska, niezwłocznie po otrzymaniu informacji, o której mowa w ust. 6, uniemożliwia dostęp do informacji niejawnych osobie, której dotyczy ta informacja.

8. Postępowanie sprawdzające wobec osoby, której odmówiono wydania poświadczenia bezpieczeństwa, można przeprowadzić najwcześniej po upływie roku od daty doręczenia decyzji o odmowie wydania poświadczenia bezpieczeństwa.

9. Termin określony w ust. 8 może zostać skrócony:

1) jeżeli decyzja o odmowie wydania poświadczenia bezpieczeństwa została wydana wyłącznie w związku z przedstawieniem osobie sprawdzanej zarzutu popełnienia przestępstwa, postawieniem jej w stan oskarżenia lub skazaniem za przestępstwo umyślne, ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe, a postępowanie karne zostało następnie umorzone lub zakończone uniewinnieniem osoby sprawdzanej;

2) w przypadku ujawnienia i potwierdzenia występowania okoliczności, o których mowa w art. 145 § 1, art. 145a § 1 i art. 145b § 1 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

10. Z chwilą wydania decyzji o odmowie wydania poświadczenia bezpieczeństwa przez ABW, SKW lub służby, o których mowa w art. 23 ust. 8:

1) tracą ważność wszystkie posiadane przez tę osobę poświadczenia bezpieczeństwa oraz upoważnienia do dostępu do informacji niejawnych o klauzuli "zastrzeżone";

2) umarza się równolegle toczące się postępowania sprawdzające.

11. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór decyzji o odmowie wydania poświadczenia bezpieczeństwa uwzględniając we wzorze decyzji składniki określone w ust. 4 oraz zapewni zróżnicowanie wzorów decyzji wydawanych przez ABW, SKW, służby określone w art. 23 ust. 8 oraz pełnomocników ochrony.

**Art. 31.** 1. Umorzenie postępowania sprawdzającego następuje w przypadku:

- 1) śmierci osoby sprawdzanej;
- 2) rezygnacji osoby sprawdzanej z ubiegania się o stanowisko albo zajmowania stanowiska lub wykonywania prac związanych z dostępem do informacji niejawnych;
- 3) wycofania zgody na przeprowadzenie postępowania sprawdzającego;
- 4) odstąpienia przez kierownika jednostki organizacyjnej od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac, związanych z dostępem do informacji niejawnych;
- 5) gdy przeprowadzenie skutecznego postępowania sprawdzającego nie jest możliwe z przyczyn niezależnych od organu je prowadzącego, w szczególności w przypadku, gdy osoba sprawdzana nie przebywała na terytorium Rzeczypospolitej Polskiej przez okres umożliwiający uzyskanie informacji istotnych dla oceny dawania rękojmi zachowania tajemnicy;

6) gdy postępowanie z innej przyczyny stało się bezprzedmiotowe.

2. Decyzję o umorzeniu postępowania sprawdzającego organ je prowadzący doręcza wnioskodawcy, pełnomocnikowi ochrony oraz, w przypadkach, o których mowa w ust. 1 pkt 2-6, osobie sprawdzanej.

3. Postępowania sprawdzającego nie umarza się w przypadku, o którym mowa w ust. 1 pkt 4, jeżeli do organu prowadzącego postępowanie wpłynię wniosek o przeprowadzenie postępowania od innego kierownika jednostki organizacyjnej.

**Art. 32.** 1. Na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska, złożony co najmniej na 6 miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa, ale nie wcześniej niż 12 miesięcy przed upływem tego terminu, 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. 24 ust. 6, nie ma zastosowania.

4. W przypadku wniosku o przeprowadzenie postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa organizacji międzynarodowej wobec osoby posiadającej ważne poświadczenie bezpieczeństwa, wydane przez ABW, SKW, AW lub SWW, albo w przypadku wniosku wobec osoby posiadającej ważne poświadczenie bezpieczeństwa organizacji międzynarodowej ubiegającej się o wydanie poświadczenia bezpieczeństwa, wypełnienie ankiety nie jest wymagane, a poświadczenie bezpieczeństwa organizacji międzynarodowej lub poświadczenie bezpieczeństwa jest wydawane jedynie na okres ważności posiadanego przez tę osobę odpowiednio, poświadczenia bezpieczeństwa lub poświadczenia bezpieczeństwa organizacji międzynarodowej.

5. W przypadku osoby, która posiada ważne poświadczenie bezpieczeństwa wydane przez ABW, SKW lub służby, o których mowa w art. 23 ust. 8, lub poświadczenie bezpieczeństwa organizacji międzynarodowej, wniosek o wydanie poświadczenia uprawniającego do dostępu do informacji niejawnych o wyższej klauzuli tajności, realizowany może być bez konieczności wypełnienia ankiety, a poświadczenie jest wydawane na okres wynikający z przepisów ustawy, licząc od daty wydania posiadanego przez tę osobę poświadczenia bezpieczeństwa lub poświadczenia bezpieczeństwa organizacji międzynarodowej.

6. Warunkami wszczęcia postępowania, o którym mowa w ust. 4 lub 5, są:

- 1) pisemna zgoda osoby sprawdzanej;
- 2) potwierdzenie aktualności danych zawartych w ankiecie wypełnionej na potrzeby poprzednio prowadzonego postępowania sprawdzającego, ewentualne uzupełnienie albo aktualizacja danych w ankiecie.

**Art. 33.** 1. W przypadku, gdy w stosunku do osoby, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy, przeprowadza się kontrolne postępowanie sprawdzające. Osoba sprawdzana nie wypełnia nowej ankiety dla celów tego postępowania.

2. Kontrolne postępowanie sprawdzające przeprowadza organ właściwy do przeprowadzenia kolejnego postępowania sprawdzającego.

3. Wobec osoby posiadającej ważne poświadczenie bezpieczeństwa, ale niezatrudnionej w jednostce organizacyjnej, w której przetwarzane są informacje niejawne, albo zatrudnionej w takiej

jednostce organizacyjnej na stanowisku, z którym nie wiąże się dostęp do informacji niejawnych, postępowanie kontrolne przeprowadza służba, która wydała poświadczenie bezpieczeństwa. Przepis ust. 5 stosuje się odpowiednio.

4. Jeżeli w odniesieniu do osoby, o której mowa w ust. 3, nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy zostały w pierwszej kolejności uzyskane przez służbę, o której mowa w art. 23 ust. 8, w której osoba ta była zatrudniona, kontrolne postępowanie sprawdzające przeprowadza ta służba.

5. Niezależnie od właściwości do przeprowadzenia kontrolnego postępowania sprawdzającego, określonej w ust. 2-4, kontrolne postępowanie sprawdzające może zostać przeprowadzone przez ABW albo SKW:

1) w przypadku wątpliwości, o których mowa w art. 24 ust. 2 pkt 1-3;

2) w przypadku skazania osoby posiadającej poświadczenie bezpieczeństwa prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe albo gdy osoba ta została oskarżona lub nieprawomocnie skazana albo przedstawiono jej zarzut popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3,

3) w stosunku do kierownika przedsiębiorcy.

6. W przypadku ustania zatrudnienia na stanowisku związanym z dostępem do informacji niejawnych osoby, wobec której wszczęto kontrolne postępowanie sprawdzające, postępowanie takie jest kontynuowane przez służbę, która je wszczęła.

7. Postępowania kontrolnego nie wszczyna się, a wszczęte umarza, w stosunku do osoby, która złoży oświadczenie do organu, który wydał poświadczenie bezpieczeństwa, o zrzeczeniu się uprawnień do dostępu do informacji niejawnych. Organ, który wydał poświadczenie, informację o złożeniu oświadczenia przekazuje do ABW lub SKW. W przypadku wydania poświadczenia bezpieczeństwa przez ABW lub SKW – oświadczenie wysyła się bezpośrednio do ABW lub SKW.

**Art. 34.** 1. W celu weryfikacji nowych informacji wskazujących, że osoba nie daje rękojmi zachowania tajemnicy, właściwa służba może przeprowadzić sprawdzenia w ewidencjach, sprawdzenia w ewidencjach niejawnych oraz rozmowy, o których mowa w art. 25 ust. 5. 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.

2. W celu weryfikacji informacji mogących mieć istotne znaczenie dla oceny dawania rękojmi zachowania tajemnicy przez osobę posiadającą ważne poświadczenie bezpieczeństwa i zajmującą stanowisko związane z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą, ABW, SKW lub służby, o których mowa w art. 23 ust. 8, mogą przeprowadzić czynności weryfikujące, o których mowa w ust. 1, a także zobowiązać osobę do uaktualnienia niezbędnych informacji zawartych w ankiecie. Niewypełnienie tego zobowiązania może stanowić podstawę do wszczęcia kontrolnego postępowania sprawdzającego.

3. O wszczęciu, przedłużeniu i zakończeniu kontrolnego postępowania sprawdzającego zawiadamia się:

- 1) kierownika jednostki organizacyjnej lub osobę uprawnioną do obsady stanowiska;
- 2) pełnomocnika ochrony w jednostce organizacyjnej;
- 3) osobę sprawdzaną;
- 4) organ, który wydał poświadczenie bezpieczeństwa;
- 5) ABW lub SKW.



4. Po otrzymaniu zawiadomienia o wszczęciu kontrolnego postępowania sprawdzającego, kierownik jednostki organizacyjnej lub osoba uprawniona do obsady stanowiska uniemożliwia osobie sprawdzanej dostęp do informacji niejawnych.

5. Do kontrolnego postępowania sprawdzającego stosuje się przepisy art. 24 ust. 1-5 i 9, art. 25-27, art. 30, art. 31 ust. 1 pkt 1 i 4 oraz ust. 2. W toku tego postępowania można odstąpić od sprawdzeń w ewidencjach i sprawdzeń w ewidencjach niejawnych, jeżeli z innych ustaleń wynika, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy.

6. Wszystkie czynności przeprowadzone w toku kontrolnego postępowania sprawdzającego powinny być zakończone przed upływem 6 miesięcy od dnia wszczęcia tego postępowania.

7. W szczególnie uzasadnionych przypadkach, jeśli służba prowadząca kontrolne postępowanie sprawdzające nie zakończy go w terminie, o którym mowa w ust. 6, termin realizacji tego postępowania przedłuża się o kolejne 6 miesięcy. W przypadku realizacji kontrolnego postępowania sprawdzającego w wyniku przekazania sprawy do ponownego rozpatrzenia przez organ odwoławczy lub w wyniku orzeczenia sądu administracyjnego, za datę wszczęcia tego postępowania uważa się datę wpływu do organu prowadzącego postępowanie decyzji organu odwoławczego lub prawomocnego orzeczenia sądu wraz z aktami postępowania.

8. Kontrolne postępowanie sprawdzające kończy się:

- 1) decyzją o cofnięciu poświadczenia bezpieczeństwa;
- 2) poinformowaniem osób i organów, o których mowa 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;
- 3) decyzją o umorzeniu postępowania, w przypadku:
  - a) gdy postępowanie to nie zostanie zakończone przed upływem 6 miesięcy od dnia jego wszczęcia, lub 12 miesięcy w przypadku jego przedłużenia,
  - b) złożenia oświadczenia do organu, który wydał poświadczenie bezpieczeństwa, o zrzeczeniu się uprawnień do dostępu do informacji niejawnych.

9. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór decyzji o cofnięciu poświadczenia bezpieczeństwa, uwzględniając we wzorze decyzji składniki określone w art. 30 ust. 4 pkt 1 i 3-9 oraz zapewni zróżnicowanie wzorów decyzji wydawanych przez ABW, SKW oraz służby określone w art. 23 ust. 8.

**Art. 35.** 1. Nie przeprowadza się postępowania sprawdzającego, jeżeli osoba, której ma ono dotyczyć, przedstawi poświadczenie bezpieczeństwa odpowiednie do wymaganej klauzuli tajności. Przepisy art. 29 ust. 5-8 stosuje się odpowiednio.

2. Przed udostępnieniem informacji niejawnych osobie, o której mowa w ust. 1, o fakcie jej zatrudnienia na stanowisku, z którym może łączyć się dostęp do informacji niejawnych, kierownik jednostki organizacyjnej informuje:

- 1) ABW lub SKW, w przypadku poświadczenia bezpieczeństwa wydanego przez pełnomocnika ochrony;
- 2) służbę, która wydała poświadczenie bezpieczeństwa oraz dodatkowo ABW lub SKW, w przypadku poświadczenia bezpieczeństwa wydanego przez ABW lub SKW;
- 3) służbę, która wydała poświadczenie bezpieczeństwa, w przypadku, o którym mowa w art. 29 ust. 6.

3. Udostępnienie informacji niejawnych osobie, o której mowa w ust. 1, może nastąpić tylko w przypadku potwierdzenia przez poinformowane służby faktu posiadania przez tę osobę

odpowiedniego poświadczenia bezpieczeństwa oraz tego, że nie jest wobec niej prowadzone kontrolne postępowanie sprawdzające.

4. Służba, o której mowa w ust. 2, udziela odpowiedzi w terminie 7 dni od dnia otrzymania od kierownika jednostki organizacyjnej informacji o zatrudnieniu osoby na stanowisku, z którym może łączyć się dostęp do informacji niejawnych. Nieudzielenie odpowiedzi w tym terminie należy traktować jako potwierdzenie faktu posiadania przez tę osobę odpowiedniego poświadczenia bezpieczeństwa oraz tego, że nie jest wobec niej prowadzone kontrolne postępowanie sprawdzające.

5. Jeżeli z ratyfikowanych przez Rzeczpospolitą Polską umów międzynarodowych wynika obowiązek dopuszczenia do informacji niejawnych obywateli państw obcych mających wykonywać w Rzeczypospolitej Polskiej pracę w interesie innego państwa lub organizacji międzynarodowej, postępowania sprawdzającego nie przeprowadza się.

6. Postępowania sprawdzającego nie przeprowadza się wobec:

- 1) Prezydenta Rzeczypospolitej Polskiej oraz osoby wybranej na ten urząd;
- 2) Marszałka Sejmu;
- 3) Marszałka Senatu;
- 4) Prezesa Rady Ministrów.

7. 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. Oświadczenie przechowuje się odpowiednio w Kancelariach Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów, Sejmu albo Senatu.

8. Z zastrzeżeniem art. 36 postępowania sprawdzającego nie przeprowadza się wobec:

- 1) członka Rady Ministrów;
- 2) Prezesa Narodowego Banku Polskiego;
- 3) Prezesa Najwyższej Izby Kontroli;
- 4) Rzecznika Praw Obywatelskich;
- 5) Prezesa Urzędu Ochrony Danych Osobowych;
- 6) członka Rady Polityki Pieniężnej;
- 7) członka Krajowej Rady Radiofonii i Telewizji;
- 8) Prezesa Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu;
- 9) Szefa Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu i Prezesa Rady Ministrów;
- 10) posła i senatora;
- 11) sędziego sądu powszechnego i sądu wojskowego, Sądu Najwyższego, sądów administracyjnych i Naczelnego Sądu Administracyjnego, a także Trybunału Stanu i Trybunału Konstytucyjnego;
- 12) prokuratora.

9. Postępowania sprawdzającego nie przeprowadza się wobec posła do Parlamentu Europejskiego wybranego w Rzeczypospolitej Polskiej, jeżeli do wykonywania mandatu jest mu niezbędny dostęp do informacji niejawnych UE o klauzuli tajności nie wyższej, niż klauzula równorzędna klauzuli „poufne”.

**Art. 36.** 1. W stosunku do osób zajmujących lub kandydujących na stanowiska albo pełniących funkcje, o których mowa w art. 35 ust. 8, ubiegających się o dostęp do informacji niejawnych organizacji międzynarodowych, ABW albo SKW przeprowadzają poszerzone postępowanie sprawdzające.

2. Z wnioskiem o przeprowadzenie postępowania, o którym mowa w ust. 1, występuje:

- 1) osoba uprawniona do powołania na to stanowisko;
- 2) Marszałek Sejmu w stosunku do posłów lub jeżeli do powołania jest uprawniony Sejm;
- 3) Marszałek Senatu w stosunku do senatorów lub jeżeli do powołania jest uprawniony Senat;
- 4) prezes właściwego sądu powszechnego w stosunku do sędziego tego sądu;
- 5) prezes właściwego sądu wojskowego w stosunku do sędziego tego sądu;
- 6) Pierwszy Prezes Sądu Najwyższego w stosunku do sędziego tego sądu;
- 7) prezes właściwego sądu administracyjnego w stosunku do sędziego tego sądu;
- 8) prezes Naczelnego Sądu Administracyjnego w stosunku do sędziego tego sądu;
- 9) prezes Trybunału Stanu w stosunku do sędziego tego trybunału;
- 10) prezes Trybunału Konstytucyjnego w stosunku do sędziego tego trybunału;
- 11) Prokurator Generalny w stosunku do prokuratora Prokuratury Krajowej;
- 12) prokurator regionalny w stosunku do prokuratora prokuratury regionalnej;
- 13) prokurator okręgowy w stosunku do prokuratora prokuratury okręgowej;
- 14) prokurator rejonowy w stosunku do prokuratora prokuratury rejonowej.

3. W stosunku do osób kandydujących na stanowiska albo funkcje, o których mowa w art. 35 ust. 8 pkt 2-9, oraz posłów i senatorów, których obowiązki poselskie bądź senatorskie wymagają dostępu do informacji niejawnych o klauzuli "ściśle tajne", ABW przeprowadza poszerzone postępowanie sprawdzające. Z wnioskiem o przeprowadzenie tego postępowania występują osoby, o których mowa w ust. 2.

4. Postępowanie sprawdzające, o którym mowa w ust. 1, w stosunku do osób kandydujących na stanowiska, o których mowa w art. 35 ust. 8 pkt 2-9, powinno być zakończone przed upływem 14 dni od dnia złożenia wniosku o przeprowadzenie tego postępowania wraz z wypełnioną ankietą.

5. W przypadku zakończenia postępowania sprawdzającego prowadzonego na wniosek Marszałka Sejmu albo Marszałka Senatu decyzją o odmowie wydania poświadczenia bezpieczeństwa, Prezes Rady Ministrów lub Minister Koordynator Służb Specjalnych, jeżeli został powołany, przedstawia informację o powodach tej decyzji odpowiednio Marszałkowi Sejmu lub Marszałkowi Senatu.

6. W stosunku do posła do Parlamentu Europejskiego wybranego w Rzeczypospolitej Polskiej, jeżeli do wykonywania mandatu jest mu niezbędny dostęp do informacji niejawnych UE o klauzuli tajności wyższej, niż klauzula równorzędna klauzuli „poufne”, postępowanie sprawdzające przeprowadza ABW. Z wnioskiem o przeprowadzenie tego postępowania występuje właściwy organ wskazany w przepisach określających zasady postępowania z informacjami niejawnymi w Parlamencie Europejskim. Jeżeli do wykonywania mandatu jest mu niezbędny dostęp do informacji niejawnych o klauzuli „poufne” lub wyższej, poszerzone postępowanie sprawdzające przeprowadza ABW na wniosek Marszałka Sejmu.

**Art. 37.** 1. Szefowie: Kancelarii Prezydenta Rzeczypospolitej Polskiej, Kancelarii Sejmu, Kancelarii Senatu lub Kancelarii Prezesa Rady Ministrów albo minister właściwy dla określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego, Prezes Najwyższej Izby Kontroli lub kierownik urzędu centralnego, a w przypadku ich braku ABW albo SKW, mogą:

- 1) w szczególnie uzasadnionych przypadkach wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa;
- 2) wyrazić pisemną zgodę na udostępnienie informacji niejawnych o klauzuli "tajne" lub "ściśle tajne" osobie, wobec której wszczęto poszerzone postępowanie sprawdzające, z wyłączeniem osób, o których mowa w ust. 2.

2. Szef ABW albo Szef SKW mogą wyrazić pisemną zgodę na przetwarzanie informacji niejawnych:

- 1) kierownikowi jednostki organizacyjnej,
  - 2) pełnomocnikowi ochrony oraz zastępcy pełnomocnika ochrony,
  - 3) kierownikowi kancelarii tajnej oraz zastępcy kierownika kancelarii tajnej,
  - 4) administratorowi systemu oraz inspektorowi bezpieczeństwa informatycznego
- wobec których wszczęto kolejne poszerzone postępowanie sprawdzające.

3. Zgody, o której mowa w ust. 1 i 2, nie wydaje się w przypadku, gdyby mogło to spowodować szkodę dla interesu ochrony informacji niejawnych. Brak zgody nie wymaga uzasadnienia.

4. W przypadku wyrażenia zgody, o której mowa w ust. 1, jej kopię przekazuje się odpowiednio do ABW lub SKW. Obowiązek ten nie dotyczy służb, o których mowa w art. 23 ust. 8.

5. Zgodę na przetwarzanie informacji niejawnych o klauzuli "poufne" osobie, wobec której wszczęto postępowanie sprawdzające, może wyrazić, w formie pisemnej, kierownik jednostki organizacyjnej, w której ta osoba jest zatrudniona, z wyłączeniem osób, o których mowa w ust. 2. Kopię tej zgody przekazuje się do ABW lub SKW.

6. Zasady zwalniania od obowiązku zachowania w tajemnicy informacji niejawnych oraz sposób postępowania z aktami spraw zawierającymi informacje niejawne w postępowaniu przed sądami i innymi organami określają przepisy odrębnych ustaw.

## Rozdział 5

### Kancelarie tajne. Środki bezpieczeństwa fizycznego

**Art. 38.** 1. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli "tajne" lub "ściśle tajne", tworzy kancelarię tajną i zatrudnia jej kierownika. Kierownik jednostki organizacyjnej może zatrudnić także zastępcę kierownika kancelarii tajnej.

2. W stosunku do osoby ubiegającej się o zajęcie stanowiska kierownika kancelarii tajnej lub jego zastępcy w podmiocie kluczowym dla zapewnienia bezpieczeństwa państwa z punktu widzenia ochrony informacji niejawnych, przepisy art. 15 ust. 2 pkt 5 oraz art. 15 ust. 8-13 stosuje się odpowiednio.

3. W przypadku uzasadnionym względami organizacyjnymi kierownik jednostki organizacyjnej może utworzyć oddziały kancelarii tajnej. W odniesieniu do oddziału kancelarii tajnej przepisy dotyczące kancelarii tajnej stosuje się odpowiednio.

4. W uzasadnionych przypadkach, za zgodą odpowiednio ABW lub SKW, kancelaria tajna może obsługiwać inne jednostki organizacyjne w zakresie realizacji swoich zadań. Wzajemne prawa i obowiązki, w tym nadzór, podległość, obsadę i zasady przetwarzania informacji niejawnych określa porozumienie zawarte przez właściwych kierowników jednostek organizacyjnych.

5. W przypadku uzasadnionym względami organizacyjnymi oddział kancelarii tajnej może być obsługiwany przez innych upoważnionych pracowników jednostki organizacyjnej.

6. Kierownik jednostki organizacyjnej może wyrazić zgodę na przetwarzanie w kancelarii tajnej informacji niejawnych o klauzuli "poufne" lub "zastrzeżone".

7. Kierownik jednostki organizacyjnej informuje odpowiednio ABW lub SKW o utworzeniu lub likwidacji kancelarii tajnej w terminie 30 dni od jej utworzenia lub likwidacji, określając adres kancelarii tajnej oraz klauzule tajności przetwarzanych w niej informacji niejawnych.

8. W jednostkach organizacyjnych, o których mowa w art. 44 ust. 2, dopuszcza się organizowanie innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych. W uzasadnionych przypadkach obowiązki pełnomocnika ochrony, z wyłączeniem prowadzenia postępowań sprawdzających, może przejąć kierownik tej komórki organizacyjnej. Do komórek organizacyjnych, o których mowa w zdaniu pierwszym, przepisy art. 43 stosuje się odpowiednio.

9. Jeżeli z wymogów określonych przez organizację międzynarodową lub inne państwo wynika konieczność ustanowienia odrębnego systemu kancelaryjnego, kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne międzynarodowe o klauzuli równorzędnej klauzuli „poufne” lub wyższej, tworzy kancelarię tajną międzynarodową. Zasady organizacji i funkcjonowania kancelarii tajnej międzynarodowej określają wytyczne, o których mowa w art. 11 ust. 7.

**Art. 39.** 1. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „poufne” lub „zastrzeżone”, wskazuje komórki organizacyjne odpowiedzialne za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom, odpowiednio w dokumentacji określającej sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne” lub instrukcji określającej sposób i tryb przetwarzania informacji niejawnych o klauzuli „zastrzeżone”.

2. W uzasadnionych przypadkach komórki, o których mowa w ust. 1, w zakresie realizacji swoich zadań, mogą obsługiwać inne jednostki organizacyjne. Wzajemne prawa i obowiązki, w tym nadzór, podległość, obsadę i zasady przetwarzania informacji niejawnych określa porozumienie zawarte przez właściwych kierowników jednostek organizacyjnych.

3. W odniesieniu do komórek organizacyjnych, o których mowa w ust. 1, przepisy art. 38 ust. 7 stosuje się odpowiednio, chyba że kierownik jednostki organizacyjnej poinformował ABW lub SKW o zorganizowaniu kancelarii tajnej.

**Art. 40.** 1. Przed likwidacją komórki organizacyjnej odpowiedzialnej za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom, kierownik jednostki organizacyjnej rozlicza się z materiałów pozostających w jej dyspozycji.

2. Realizacja obowiązku, o którym mowa w ust. 1, może nastąpić w szczególności przez:

- 1) archiwizację lub zniszczenie materiałów, z zachowaniem przepisów o narodowym zasobie archiwalnym i archiwach;
- 2) przekazanie tych materiałów do następcy prawnego lub zwrot do ich wytwórcy, a w przypadku ich braku – do ABW lub SKW.

3. O zrealizowaniu obowiązku, o którym mowa w ust. 1, kierownik jednostki organizacyjnej informuje odpowiednio ABW lub SKW w terminie 30 dni.

**Art. 41.** 1. Organizacja pracy kancelarii tajnej zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „tajne” lub „ściśle tajne” pozostający w dyspozycji jednostki organizacyjnej oraz kto się zapoznał z tym materiałem.

2. W szczególnie uzasadnionych przypadkach kierownik jednostki organizacyjnej może ograniczyć otwieranie w kancelarii tajnej przesyłek oznaczonych klauzulą „ściśle tajne” lub „tajne”.

3. Przepis ust. 1 stosuje się odpowiednio do organizacji pracy komórek organizacyjnych, w których są rejestrowane materiały o klauzuli „poufne” i „zastrzeżone”.

4. Kancelaria tajna lub komórka, o której mowa w ust. 3, odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.

**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 tych informacji, w szczególności chroniące przed:

- 1) działaniem obcych służb specjalnych;
- 2) zamachem terrorystycznym lub sabotażem;
- 3) kradzieżą lub zniszczeniem materiału;
- 4) próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne;
- 5) nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień.

2. W przypadku przechowywania informacji niejawnych o klauzuli „poufne” lub wyższej zakres stosowania środków bezpieczeństwa fizycznego uzależnia się od poziomu zagrożeń.

3. Przy określaniu poziomu zagrożeń uwzględnia się w szczególności istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych. W uzasadnionych przypadkach przy określaniu poziomu zagrożeń uwzględnia się wskazania odpowiednio ABW lub SKW.

**Art. 43.** W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli "poufne" lub wyższej należy w szczególności:

- 1) zorganizować strefy ochronne;
- 2) wprowadzić system kontroli dostępu do stref ochronnych;
- 3) określić uprawnienia do przebywania w strefach ochronnych;
- 4) stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, zgodnie z wymaganiami określonymi w rozporządzeniach, o których mowa w art. 19 albo art. 44 ust. 1.

**Art. 44.** 1. Prezes Rady Ministrów określi, w drodze rozporządzenia:

- 1) rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń,
- 2) podstawowe kryteria i sposób określania poziomu zagrożeń oraz dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń,
- 3) zakres stosowania środków bezpieczeństwa fizycznego,
- 4) wymagania dla wyposażenia i urządzeń służących ochronie informacji niejawnych,
- 5) kryteria tworzenia stref ochronnych,
- 6) sposób i tryb przetwarzania informacji niejawnych,
- 7) wymagania w zakresie organizacji i funkcjonowania kancelarii tajnych,
- 8) wymagania w zakresie niszczenia materiałów niejawnych,
- 9) podstawowe zadania kierownika kancelarii tajnej,
- 10) podstawowe elementy, które powinien zawierać plan ochrony informacji niejawnych,
- 11) wzór karty zapoznania się z materiałem,
- 12) wzory urządzeń ewidencyjnych

– uwzględniając potrzebę racjonalizacji nakładów ponoszonych przez jednostki organizacyjne w zakresie tworzenia systemu bezpieczeństwa fizycznego informacji niejawnych, zgodnie z zasadami określonymi w ustawie.

2. Minister Obrony Narodowej, Szef ABW, Szef AW, Szef SKW, Szef SWW oraz Szef CBA może określić, w drodze zarządzenia, każdy w zakresie swojego działania:

- 1) szczegóły sposobu organizacji i funkcjonowania:

- a) kancelarii tajnych,
  - b) innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych;
- 2) sposób i tryb przetwarzania informacji niejawnych;
  - 3) dobór i zakres stosowania środków bezpieczeństwa fizycznego.

3. Ministrowie właściwi do spraw wewnętrznych, informatyzacji, administracji publicznej, spraw zagranicznych, finansów publicznych, budżetu i instytucji finansowych, Minister Sprawiedliwości, Prezes Narodowego Banku Polskiego, Prezes Najwyższej Izby Kontroli, Pierwszy Prezes Sądu Najwyższego, Prokurator Generalny, Szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów, Sejmu, Senatu oraz Komendant Główny Policji, Komendant Główny Straży Granicznej, Komendant SOP, Komendant Główny Państwowej Straży Pożarnej, a także Prezes Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, określą, w drodze zarządzenia, każdy w zakresie swojego działania:

- 1) szczególnie sposób organizacji i funkcjonowania kancelarii tajnych;
- 2) sposób i tryb przetwarzania informacji niejawnych.

4. Minister właściwy do spraw kultury i ochrony dziedzictwa narodowego określi, w drodze zarządzenia, szczególnie sposób i tryb przetwarzania informacji niejawnych wchodzących w skład zasobu archiwalnego archiwów państwowych oraz organizację komórek organizacyjnych tych archiwów odpowiedzialnych za przetwarzanie materiałów niejawnych.

5. Prezes Rady Ministrów określi, w drodze rozporządzenia:

- 1) tryb i sposób nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów,
- 2) sposób postępowania nadawców przesyłek zawierających informacje niejawne oraz wymogi, jakie muszą spełniać te przesyłki,
- 3) sposób postępowania podmiotów, które wykonują zadania przewoźników tych materiałów, z przesyłkami zawierającymi informacje niejawne,
- 4) sposób dokumentowania przyjmowania przez przewoźników przesyłek oraz ich wydawania adresatom, wraz z załącznikami w postaci wzorów niezbędnych formularzy,
- 5) warunki ochrony i sposoby zabezpieczenia przesyłek przez przewoźnika oraz warunki, jakie muszą spełniać wykorzystywane przez niego środki transportu i uczestniczące w konwojach osoby,
- 6) sposób postępowania w przypadku zaistnienia nieprzewidzianych okoliczności mogących mieć wpływ na bezpieczeństwo przesyłki,
- 7) warunki przewożenia materiałów poza granicami Rzeczypospolitej Polskiej – uwzględniając potrzebę zabezpieczenia materiałów przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem oraz szczególne warunki ochrony ze względu na rozmiary lub charakter materiału.

## Rozdział 6

### Bezpieczeństwo informatyczne

**Art. 45.** 1. Systemy informatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa informatycznego.

2. Systemy informatyczne, w których mają być przetwarzane informacje niejawne o klauzuli „poufne” lub wyższej, podlegają akredytacji bezpieczeństwa informatycznego udzielanej przez ABW albo SKW.

3. Systemy informatyczne, w których mają być przetwarzane informacje niejawne wyłącznie o klauzuli „zastrzeżone” podlegają akredytacji bezpieczeństwa informatycznego udzielanej przez kierownika jednostki organizacyjnej organizującej ten system.

4. W przypadku systemów informatycznych przeznaczonych do łącznego przetwarzania informacji niejawnych oraz informacji niejawnych międzynarodowych, akredytacji bezpieczeństwa informatycznego udziela ABW albo SKW.

5. Systemy informatyczne, w których mają być przetwarzane informacje niejawne międzynarodowe, podlegają akredytacji bezpieczeństwa informatycznego udzielanej przez ABW albo SKW. Akredytację prowadzi się z uwzględnieniem przepisów międzynarodowych regulujących zasady oraz wymagania przetwarzania tych informacji w systemach informatycznych.

6. Przetwarzanie informacji niejawnych w systemach informatycznych organizowanych na podstawie umów międzynarodowych odbywa się zgodnie z zasadami określonymi w tych umowach.

7. ABW i SKW określają zalecenia w zakresie bezpieczeństwa informatycznego.

8. W szczególnie uzasadnionych przypadkach ABW albo SKW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie informatycznym posiadającym akredytację bezpieczeństwa informatycznego.

**Art. 46.** 1. ABW albo SKW udziela albo odmawia udzielenia akredytacji bezpieczeństwa informatycznego systemowi informatycznemu, w którym mają być przetwarzane informacje niejawne o klauzuli „poufne” lub wyższej, w terminie 9 miesięcy od otrzymania kompletnej dokumentacji bezpieczeństwa systemu informatycznego. W uzasadnionych przypadkach, w szczególności wynikających z rozległości systemu informatycznego i stopnia jego skomplikowania, termin ten może być przedłużony o kolejne 9 miesięcy. Od odmowy udzielenia akredytacji nie służy odwołanie.

2. Akredytacji, o której mowa w ust. 1, udziela się na czas określony, jednak nie dłuższy niż 5 lat.

3. Potwierdzeniem udzielenia przez ABW albo SKW akredytacji, o której mowa w ust. 1, jest świadectwo akredytacji bezpieczeństwa informatycznego.

4. Świadectwo akredytacji bezpieczeństwa informatycznego zawiera:

- 1) oznaczenie organu;
- 2) datę wydania;
- 3) oznaczenie podmiotu występującego z wnioskiem o jego wydanie.
- 4) oznaczenie przedmiotu podlegającego akredytacji bezpieczeństwa systemu informatycznego;
- 5) powołanie podstawy prawnej;
- 6) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne;
- 7) wskazanie okresu ważności świadectwa;
- 8) imię, nazwisko, stanowisko służbowe i podpis upoważnionej osoby wydającej świadectwo.

5. Świadectwo akredytacji bezpieczeństwa informatycznego wydaje się na podstawie:

- 1) zatwierdzonej przez ABW albo SKW dokumentacji bezpieczeństwa systemu informatycznego;
- 2) wyników audytu bezpieczeństwa systemu informatycznego przeprowadzonego przez ABW albo SKW.

6. ABW albo SKW może odstąpić od przeprowadzenia audytu bezpieczeństwa systemu informatycznego, jeżeli system informatyczny jest przeznaczony do przetwarzania informacji niejawnych o klauzuli „poufne”.



7. W przypadku systemu informatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „tajne” ABW albo SKW może odstąpić od przeprowadzenia audytu bezpieczeństwa systemu informatycznego w przypadku ponownej akredytacji tego systemu.

8. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory świadectw akredytacji bezpieczeństwa informatycznego udzielanych przez ABW albo SKW, uwzględniając we wzorach świadectw zakres danych określonych w ust. 4 oraz zapewni zróżnicowanie wzorów świadectw wydawanych przez ABW oraz SKW.

**Art. 47.** 1. Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa informatycznego dla systemu informatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli "zastrzeżone", przez zatwierdzenie dokumentacji bezpieczeństwa systemu informatycznego potwierdzonej świadectwem akredytacji bezpieczeństwa informatycznego.

2. Akredytacji, o której mowa w ust. 1, udziela się na czas określony, jednak nie dłuższy niż 5 lat.

3. W przypadku gdy system, o którym mowa w ust. 1, będzie funkcjonował w więcej niż jednej jednostce organizacyjnej, akredytacji udziela kierownik jednostki organizującej system.

4. W ciągu 7 dni od udzielenia akredytacji bezpieczeństwa informatycznego, o której mowa w ust. 1, kierownik jednostki organizującej system przekazuje odpowiednio do ABW albo SKW dokumentację bezpieczeństwa systemu informatycznego wraz z kopią wydanego świadectwa akredytacji bezpieczeństwa informatycznego.

5. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu informatycznego ABW albo SKW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji bezpieczeństwa informatycznego, zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. W uzasadnionych przypadkach, w szczególności wynikających ze stopnia skomplikowania systemu, termin przedstawienia zaleceń może zostać przedłużony o dodatkowe 30 dni. Kierownik jednostki organizacyjnej w terminie 30 dni od otrzymania zaleceń informuje odpowiednio ABW albo SKW o ich realizacji.

6. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór świadectwa akredytacji bezpieczeństwa informatycznego, o którym mowa w ust. 1, uwzględniając konieczność zawarcia we wzorze świadectwa danych określonych w art. 46 ust. 4.

**Art. 48.** 1. Akredytacji bezpieczeństwa informatycznego dla systemu informatycznego przeznaczonego łącznie do przetwarzania informacji niejawnych oraz informacji niejawnych międzynarodowych, udziela ABW albo SKW w trybie określonym w art. 46.

2. Dla systemu informatycznego przeznaczonego do przetwarzania informacji niejawnych międzynarodowych, który jest już akredytowany przez kierownika jednostki organizacyjnej do przetwarzania informacji niejawnych wyłącznie o klauzuli „zastrzeżone”, wymagana jest ponowna akredytacja systemu informatycznego przez ABW albo SKW.

3. Akredytacji systemu informatycznego, o której mowa w ust. 2, udziela ABW albo SKW w trybie określonym w art. 46. Wydanie nowego świadectwa akredytacji bezpieczeństwa informatycznego przez ABW albo SKW skutkuje utratą ważności świadectwa wydanego przez kierownika jednostki organizacyjnej z dniem wydania świadectwa przez ABW albo SKW.

4. W przypadkach, o których mowa w ust. 1 i 2, ABW albo SKW może odstąpić od przeprowadzenia audytu bezpieczeństwa systemu informatycznego przeznaczonego do przetwarzania informacji niejawnych międzynarodowych o klauzuli tajności równorzędnej klauzuli:

- 1) „zastrzeżone” lub „poufne”,
  - 2) „tajne” w przypadku ponownej akredytacji tego systemu
- chyba że właściwe przepisy międzynarodowe regulujące zasady oraz wymagania przetwarzania informacji niejawnych międzynarodowych w systemach informatycznych stanowią inaczej.

**Art. 49.** 1. Podstawą projektowania systemu informatycznego oraz dokonywania wszelkich zmian w systemie informatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.

2. Kierownik jednostki organizacyjnej:

- 1) akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych;
- 2) jest odpowiedzialny za właściwą organizację bezpieczeństwa informatycznego w jednostce organizacyjnej.

3. Dla systemu informatycznego służącego do przetwarzania informacji niejawnych sporządza się dokumentację bezpieczeństwa systemu informatycznego.

4. Dokument szczególnych wymagań bezpieczeństwa w szczególności:

- 1) zawiera opis przebiegu oraz wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie informatycznym, przy czym przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie, innym niż dokument szczególnych wymagań bezpieczeństwa;
- 2) określa przyjęte w ramach zarządzania ryzykiem sposoby osiągnięcia i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu informatycznego;
- 3) opisuje aspekty budowy systemu informatycznego, jego zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu informatycznego lub wpływają na jego bezpieczeństwo.

5. Dokument szczególnych wymagań bezpieczeństwa:

- 1) opracowuje się na etapie projektowania systemu informatycznego i, w razie potrzeby, konsultuje z ABW albo SKW;
- 2) na bieżąco uzupełnia się na etapie wdrażania systemu informatycznego;
- 3) modyfikuje się na etapie eksploatacji systemu informatycznego przed dokonaniem zmian w tym systemie.

6. Dokument procedur bezpiecznej eksploatacji systemu informatycznego:

- 1) opracowuje się na etapie wdrażania systemu informatycznego;
- 2) modyfikuje na etapie eksploatacji systemu informatycznego przed dokonaniem zmian w tym systemie.

7. Kierownik jednostki organizacyjnej organizującej system informatyczny odpowiada za opracowanie oraz przekazanie odpowiednio ABW albo SKW dokumentacji bezpieczeństwa systemu informatycznego.

8. W przypadku systemu informatycznego funkcjonującego w więcej niż jednej jednostce organizacyjnej, po uzgodnieniu z jednostką organizacyjną organizującą system informatyczny, dokumentacja bezpieczeństwa systemu informatycznego może być uzupełniona o aneksy zawierające dane dotyczące konkretnych lokalizacji.

9. Dołączanie kolejnych elementów do systemu informatycznego posiadającego akredytację bezpieczeństwa informatycznego odbywa się na zasadach określonych w zatwierdzonej przez ABW lub SKW dokumentacji bezpieczeństwa systemu informatycznego.

10. Po otrzymaniu dokumentacji bezpieczeństwa systemu informatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli "poufne" lub wyższej lub informacji niejawnych międzynarodowych, ABW albo SKW przeprowadza na jej podstawie ocenę

bezpieczeństwa tego systemu. Pozytywny wynik oceny bezpieczeństwa systemu stanowi podstawę do zatwierdzenia przez ABW albo SKW dokumentacji bezpieczeństwa systemu informatycznego.

11. W systemie informatycznym służącym do przetwarzania informacji niejawnych o klauzuli „tajne” lub „ściśle tajne” są stosowane środki ochrony elektromagnetycznej, certyfikowane zgodnie z art. 50, odpowiednie do klauzuli tajności przekazywanych informacji oraz dobierane na podstawie wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie, z uwzględnieniem zaleceń w zakresie bezpieczeństwa informatycznego, określanych przez ABW lub SKW.

12. W systemie informatycznym służącym do przetwarzania informacji niejawnych o klauzuli „poufne”, środki ochrony elektromagnetycznej stosuje się tylko w przypadku, gdy wyniki przeprowadzonego szacowania ryzyka wskazują na zasadność ich zastosowania.

13. Prezes Rady Ministrów określi, w drodze rozporządzenia:

1) podstawowe wymagania bezpieczeństwa informatycznego, jakim powinny odpowiadać systemy informatyczne,

2) niezbędne dane, jakie powinna zawierać dokumentacja bezpieczeństwa systemów informatycznych.

– uwzględniając w szczególności wymagania w zakresie zarządzania ryzykiem oraz dotyczące zapewnienia poufności, integralności i dostępności informacji niejawnych przetwarzanych w systemach informatycznych.

**Art. 50.** 1. Środki ochrony elektromagnetycznej przeznaczone do ochrony informacji niejawnych o klauzuli "poufne" lub wyższej podlegają badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonych przez ABW albo SKW.

2. Urządzenia kryptograficzne i kryptograficzne narzędzia programowe przeznaczone do ochrony informacji niejawnych podlegają badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonych przez ABW albo SKW.

3. Certyfikację urządzenia lub narzędzia służącego do realizacji zabezpieczenia informatycznego, przeznaczonego do ochrony informacji niejawnych przeprowadza ABW albo SKW, na wniosek zainteresowanego podmiotu.

4. Ze względu na istotny interes bezpieczeństwa państwa, Szef ABW lub Szef SKW może odmówić rozpoczęcia bądź w dowolnym momencie przerwać, wstrzymać lub zakończyć odmową wydania właściwego certyfikatu trwający proces certyfikacji środka ochrony elektromagnetycznej, urządzenia kryptograficznego lub kryptograficznego narzędzia programowego albo urządzenia lub narzędzia służącego do realizacji zabezpieczenia informatycznego, przeznaczonego do ochrony informacji niejawnych.

5. Pozytywne wyniki ocen bezpieczeństwa uzyskane na podstawie wyników badań prowadzonych w ramach certyfikacji, o których mowa w ust. 1-3, stanowią podstawę do wydania przez ABW albo SKW certyfikatu ochrony elektromagnetycznej, certyfikatu ochrony kryptograficznej lub certyfikatu bezpieczeństwa informatycznego. Certyfikaty są wydawane na czas określony lub bezterminowo, w zależności od wyników ocen bezpieczeństwa. Od odmowy wydania certyfikatu nie służy odwołanie.

6. Certyfikacje, o których mowa w ust. 1-3, są prowadzone przez ABW albo SKW z pominięciem właściwości, o której mowa w art. 10 ust. 2 i 3.

7. W przypadku wystąpienia okoliczności uzasadniających podejrzenie faktycznej niezdolności do ochrony informacji niejawnych certyfikowanego środka, urządzenia lub narzędzia, o których mowa w ust. 1-3, Szef ABW albo Szef SKW mogą czasowo zawiesić lub skrócić okres ważności wydanego przez siebie odpowiednio certyfikatu ochrony elektromagnetycznej,

certyfikatu ochrony kryptograficznej lub certyfikatu bezpieczeństwa informatycznego. W przypadku czasowego zawieszenia ważności certyfikatu lub skrócenia jego ważności, zabronione jest przetwarzanie informacji niejawnych w akredytowanych systemach informatycznych w zakresie, w którym w systemach tych przetwarzane są informacje niejawne z zastosowaniem tego środka, urządzenia lub narzędzia.

8. Szef ABW albo Szef SKW może zlecić podmiotowi zewnętrznemu badanie środka, urządzenia lub narzędzia, o których mowa w ust. 1-3, służących do ochrony informacji niejawnych, na zasadach, warunkach i w zakresie przez siebie określonych.

9. Bez konieczności przeprowadzania badań i oceny Szef ABW albo Szef SKW może dopuścić do stosowania w systemie informatycznym przeznaczonym do przetwarzania informacji niejawnych o klauzuli "zastrzeżone" kryptograficzne urządzenia lub narzędzia programowe, jeżeli zostały one dopuszczone do ochrony informacji niejawnych przez uprawniony organ państwa będącego członkiem NATO, UE lub ESA lub uprawniony organ w NATO, UE lub ESA.

**Art. 51.** 1. Obowiązki akredytacji, o którym mowa w art. 45 ust. 2 i 3, nie podlegają elementy systemów informatycznych znajdujące się poza strefami ochronnymi oraz służące bezpośrednio do pozyskiwania i przekazywania w sposób niejawny informacji oraz utrwalania dowodów w trakcie realizacji czynności operacyjno-rozpoznawczych lub procesowych przez uprawnione do tego podmioty. Wyłączenie obowiązku akredytacji nie obejmuje interfejsów, o których mowa w art. 179 ust. 4a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2018 r. poz. 1954, 2245 i 2354), oraz systemów z nimi współpracujących.

2. Obowiązki akredytacji, o którym mowa w art. 45 ust. 2 i 3, oraz badań i oceny bezpieczeństwa w ramach procesów certyfikacji prowadzonych przez ABW albo SKW nie podlegają systemy informatyczne, urządzenia kryptograficzne lub kryptograficzne narzędzia programowe wykorzystywane przez ABW, SKW, AW lub SWW do uzyskiwania lub przetwarzania informacji niejawnych podczas wykonywania czynności operacyjno-rozpoznawczych poza granicami Rzeczypospolitej Polskiej oraz wydzielone stanowiska służące wyłącznie do odbierania i przetwarzania tych informacji na terytorium Rzeczypospolitej Polskiej.

**Art. 52.** 1. Kierownik jednostki organizacyjnej wyznacza:

- 1) osobę lub osoby pełniące funkcję inspektora bezpieczeństwa informatycznego;
- 2) osobę lub zespół osób pełniących funkcję administratora systemu.

2. Inspektorem bezpieczeństwa informatycznego albo administratorem systemu może być osoba spełniająca wymagania określone w art. 17, po ukończeniu specjalistycznych szkoleń z zakresu bezpieczeństwa informatycznego.

3. W stosunku do osoby ubiegającej się o objęcie funkcji inspektora bezpieczeństwa informatycznego albo administratora systemu w podmiocie kluczowym dla zapewnienia bezpieczeństwa państwa z punktu widzenia ochrony informacji niejawnych, przepisy art. 15 ust. 2 pkt 5 oraz ust. 8-13 stosuje się odpowiednio.

4. Funkcje inspektora bezpieczeństwa informatycznego oraz administratora systemu nie mogą być pełnione w ramach danego systemu przez tę samą osobę.

5. W uzasadnionych przypadkach, za zgodą ABW albo SKW, inspektor bezpieczeństwa teleinformatycznego lub administrator systemu może wykonywać zadania w więcej niż jednej jednostce organizacyjnej na podstawie porozumienia właściwych kierowników jednostek organizacyjnych.

**Art. 53.** 1. Rozwiązania informatyczne niebędące systemami informatycznymi, w których mają być przetwarzane informacje niejawne, podlegają ocenie bezpieczeństwa oraz dopuszczeniu do przetwarzania informacji niejawnych.

2. W przypadku wątpliwości dotyczących uznania rozwiązania informatycznego za niebędące systemem informatycznym, organem właściwym do ich rozstrzygnięcia jest Szef SKW.

3. Szef SKW określi tryb oceny i sposób dopuszczania rozwiązań informatycznych, o których mowa w ust. 1, uwzględniając w szczególności zasady ochrony informacji niejawnych w razie ogłoszenia mobilizacji i w czasie wojny.

## Rozdział 7

### Bezpieczeństwo przemysłowe

**Art. 54.** 1. Warunkiem dostępu przedsiębiorcy do informacji niejawnych w związku z wykonywaniem umów albo zadań wynikających z przepisów prawa, zwanych dalej "umowami", jest zdolność do ochrony informacji niejawnych.

2. Dokumentem potwierdzającym zdolność do ochrony informacji niejawnych o klauzuli "poufne" lub wyższej jest świadectwo bezpieczeństwa przemysłowego, zwane dalej "świadectwem", wydawane przez ABW albo SKW po przeprowadzeniu postępowania bezpieczeństwa przemysłowego.

3. W przypadku przedsiębiorcy wykonującego działalność jednoosobowo i osobiście zdolność do ochrony informacji niejawnych o klauzuli „poufne” lub wyższej potwierdza:

1) poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli "poufne" lub wyższej, wydawane przez ABW albo SKW;

2) zaświadczenie o odbytym szkoleniu w zakresie ochrony informacji niejawnych.

4. Przepisu ust. 3 nie stosuje się, jeżeli obowiązek uzyskania świadectwa wynika z ratyfikowanej przez Rzeczpospolitą Polską umowy międzynarodowej lub prawa wewnętrznego strony zawierającej umowę.

5. Do przedsiębiorcy wykonującego działalność jednoosobowo i osobiście nie stosuje się przepisów niniejszego rozdziału, z wyjątkiem ust. 7, 8 i 10 oraz art. 69 ust. 1 pkt 2.

6. Przepisy ust. 1-5 stosuje się także do przedsiębiorców będących podwykonawcami umów, jeżeli ich wykonywanie wiąże się z dostępem do informacji niejawnych.

7. Szef ABW albo Szef SKW może:

1) w szczególnie uzasadnionych przypadkach, wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych przedsiębiorcy wykonującemu działalność jednoosobowo i osobiście nieposiadającemu odpowiedniego poświadczenia bezpieczeństwa;

2) wyrazić pisemną zgodę na udostępnienie informacji niejawnych przedsiębiorcy, wobec którego wszczęto postępowanie bezpieczeństwa przemysłowego lub przedsiębiorcy wykonującemu działalność jednoosobowo i osobiście, gdy wszczęto wobec niego postępowanie sprawdzające.

8. Zgoda, o której mowa w ust. 7 pkt 2, traci ważność w przypadku zakończenia lub zawieszenia prowadzonego postępowania bezpieczeństwa przemysłowego, a w przypadku przedsiębiorcy wykonującego działalność jednoosobowo i osobiście - zakończenia lub zawieszenia postępowania sprawdzającego.

9. O odmowie wydania świadectwa bezpieczeństwa przemysłowego, zawieszeniu oraz umorzeniu postępowania bezpieczeństwa przemysłowego ABW lub SKW zawiadamia

niezwłocznie jednostki organizacyjne, które zawarły z przedsiębiorcą umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej.

10. O odmowie wydania lub o cofnięciu poświadczenia bezpieczeństwa przedsiębiorcy wykonującemu działalność jednoosobowo i osobiście oraz o zawieszeniu lub umorzeniu postępowania sprawdzającego wobec tego przedsiębiorcy, ABW lub SKW zawiadamia niezwłocznie jednostki organizacyjne, które zawarły z tym przedsiębiorcą umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej.

11. W szczególnie uzasadnionych przypadkach Szef ABW albo Szef SKW może wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych przedsiębiorcy nieposiadającemu odpowiedniego świadectwa i wobec którego nie jest prowadzone postępowanie bezpieczeństwa przemysłowego.

12. Zgody, o której mowa w ust. 7 i 11, nie wydaje się w przypadku, gdyby mogło to spowodować szkody dla interesu ochrony informacji niejawnych.

13. W przypadku gdy przedsiębiorca zamierza wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli "zastrzeżone", świadectwo nie jest wymagane. Przedsiębiorca ten jest obowiązany spełnić wymagania ustawy w zakresie ochrony informacji niejawnych o klauzuli "zastrzeżone", z wyjątkiem wymogu zatrudnienia pełnomocnika ochrony, jeżeli nie przetwarza tych informacji w użytkowanych przez niego obiektach.

**Art. 55.** 1. W zależności od stopnia zdolności do ochrony informacji niejawnych o klauzuli "poufne" lub wyższej wydaje się świadectwo odpowiednio:

1) pierwszego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, obejmującą:

a) zdolność do ich przetwarzania:

– w systemach informatycznych zorganizowanych przez kierownika tego przedsiębiorcy,  
– w użytkowanych przez niego obiektach, przez co rozumie się także obiekty wykorzystywane w trybie określonym w art. 38 ust. 4,

b) możliwość ich przetwarzania w ramach zawartej z inną jednostką organizacyjną umowy związanej z dostępem do informacji niejawnych o klauzuli "poufne" lub wyższej:

– w systemach informatycznych zorganizowanych przez kierownika tej jednostki organizacyjnej,  
– w obiektach użytkowanych przez tę jednostkę organizacyjną;

2) drugiego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, obejmującą zdolność do ich przetwarzania w zakresie wskazanym w pkt 1 lit. a tiret drugie oraz możliwość ich przetwarzania w zakresie wskazanym w pkt 1 lit. b;

3) trzeciego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji obejmującą możliwość ich przetwarzania w zakresie wskazanym w pkt 1 lit. b.

2. Świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli:

1) "ściśle tajne" potwierdza zdolność do ochrony informacji niejawnych o klauzuli:

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 o klauzuli:

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 o tej klauzuli przez okres 10 lat od daty wystawienia.

3. W przypadku przedsiębiorcy posiadającego świadectwo pierwszego stopnia, który w okresie jego ważności:

- 1) utracił zdolność do przetwarzania informacji niejawnych,
- 2) zrzekł się uprawnień do przetwarzania informacji niejawnych  
– w zakresie wskazanym w ust. 1 pkt 1 lit. a tiret pierwsze, zdolność do ochrony informacji niejawnych w zakresie właściwym dla świadectwa bezpieczeństwa przemysłowego drugiego stopnia przez okres wskazany w ust. 2 może zostać na wniosek tego przedsiębiorcy potwierdzona przez ABW lub SKW.

4. W przypadku przedsiębiorcy posiadającego świadectwo drugiego stopnia, który w okresie jego ważności:

- 1) utracił zdolność do przetwarzania informacji niejawnych,
- 2) zrzekł się uprawnień do przetwarzania informacji niejawnych  
– w zakresie wskazanym w ust. 1 pkt 1 lit. a tiret drugie, zdolność do ochrony informacji niejawnych w zakresie właściwym dla świadectwa trzeciego stopnia przez okres wskazany w ust. 2 może zostać na wniosek tego przedsiębiorcy potwierdzona przez ABW lub SKW.

5. Przedsiębiorca kieruje do ABW lub SKW wniosek, o którym mowa w ust. 3 lub 4, w terminie 30 dni od daty zaistnienia przesłanek do ubiegania się o potwierdzenie zdolności do ochrony informacji niejawnych w zakresie świadectwa drugiego lub trzeciego stopnia.

6. Przedsiębiorca posiadający świadectwo pierwszego stopnia, który utracił zdolność do przetwarzania informacji niejawnych w zakresie wskazanym w ust. 1 pkt 1 lit. a tiret pierwsze w związku ze wstrzymaniem, w trybie określonym w art. 45 ust. 8, przetwarzania informacji niejawnych w zorganizowanym przez kierownika tego przedsiębiorcy systemie informatycznym, posiada zdolność do ochrony informacji niejawnych w zakresie wskazanym w ust. 1 pkt 2 do momentu przekazania przez ABW lub SKW informacji o przywróceniu możliwości przetwarzania informacji niejawnych w tym systemie, nie dłużej jednak niż przez okres wskazany w ust. 2.

7. ABW albo SKW wydaje odrębne świadectwa potwierdzające zdolność do ochrony informacji niejawnych NATO, UE lub ESA, o klauzuli równorzędnej klauzuli:

- 1) "poufne" lub „tajne” ,
- 2) „ściśle tajne” – w przypadku świadectwa trzeciego stopnia, potwierdzającego zdolność do ochrony informacji niejawnych NATO oraz ESA  
– stosując odpowiednio przepisy ust. 2-6.

8. Świadectwo wygasa, jeżeli:

- 1) upłynął okres jego ważności;
- 2) przedsiębiorca zrzekł się uprawnień określonych w świadectwie i nie wystąpił do ABW lub SKW z wnioskiem o potwierdzenie uprawnień, o których mowa w ust. 3 lub 4;
- 3) przedsiębiorca został przejęty przez inny podmiot lub zlikwidowany;
- 4) przedsiębiorca uzyskał kolejne świadectwo tego samego stopnia potwierdzające zdolność do ochrony informacji niejawnych o klauzuli tajności nie niższej niż klauzula wskazana w dotychczas posiadanym świadectwie.

**Art. 56.** 1. Postępowanie bezpieczeństwa przemysłowego jest prowadzone na wniosek przedsiębiorcy, podpisany przez osoby upoważnione do składania oświadczeń woli w imieniu przedsiębiorcy albo przez kierownika przedsiębiorcy. Wniosek nie wymaga uzasadnienia.

2. We wniosku przedsiębiorca określa stopień świadectwa oraz klauzulę tajności informacji niejawnych, których zdolność do ochrony ma potwierdzać świadectwo.

3. Do wniosku przedsiębiorca dołącza kwestionariusz bezpieczeństwa przemysłowego, zwany dalej "kwestionariuszem", oraz ankiety lub kopie poświadczeń bezpieczeństwa osób określonych w art. 57 ust. 3.

4. ABW albo SKW może wezwać przedsiębiorcę do uzupełnienia braków formalnych we wniosku i jego załącznikach w terminie 30 dni od dnia otrzymania wezwania, pod rygorem pozostawienia wniosku bez rozpatrzenia.

**Art. 57.** 1. Postępowanie bezpieczeństwa przemysłowego obejmuje sprawdzenie przedsiębiorcy i postępowania sprawdzające wobec osób wymienionych w ust. 3.

2. Sprawdzenie przedsiębiorcy, w tym na podstawie danych uzyskanych w wyniku sprawdzeń w ewidencjach oraz sprawdzeń w ewidencjach niejawnych, obejmuje:

- 1) strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuację finansową, w tym uzyskanie – w uzasadnionych przypadkach – informacji lub kopii dokumentów dotyczących stanu i historii obrotów na rachunku bankowym przedsiębiorcy, a w szczególności salda po operacji, daty, kwoty, typu i tytułu operacji, w tym wszystkich jej szczegółów wraz z opisem, włącznie z danymi rachunku przeciwstawnego i jego właściciela, a także informacji lub kopii dokumentów dotyczących innych produktów bankowych lub innych instrumentów finansowych, jak również posiadanych zobowiązań finansowych, prowadzonej działalności gospodarczej, dokonanych czynności majątkowych, w szczególności transakcji zbycia, nabycia lub zamiany majątku, ustanowienia hipoteki, posiadanego zadłużenia, prowadzonych postępowań karno-skarbowych oraz uzyskanych dochodów;
- 2) strukturę organizacyjną;
- 3) system ochrony informacji niejawnych, w tym środki bezpieczeństwa fizycznego;
- 4) wszystkie osoby wchodzące w skład organów zarządzających i kontrolnych oraz osoby działające z ich upoważnienia, w szczególności wymienione w Krajowym Rejestrze Sądowym;
- 5) w szczególnie uzasadnionych przypadkach, osoby posiadające poświadczenia bezpieczeństwa.

3. W toku postępowania bezpieczeństwa przemysłowego oraz w okresie ważności świadectwa przeprowadza się postępowania sprawdzające wobec osób nieposiadających odpowiednich poświadczeń bezpieczeństwa lub kolejne postępowania sprawdzające wobec:

- 1) kierownika przedsiębiorcy;
- 2) pełnomocnika ochrony i jego zastępcy oraz osób przewidzianych na te stanowiska;
- 3) osób zatrudnionych w pionie ochrony;
- 4) administratora systemu informatycznego;
- 5) pozostałych osób wskazanych w kwestionariuszu, które powinny mieć dostęp do informacji niejawnych, zatrudnionych przez przedsiębiorcę.

4. Czynności, o których mowa w ust. 2 pkt 1, są wykonywane zgodnie z art. 105 ust. 1 pkt 2 lit. k ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe. Przepisy art. 82 § 1 pkt 1, art. 182 § 1-3a, 5 i 6 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa oraz art. 48 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej, dotyczące zakresu przekazywanych informacji, a także dotyczące uprawnień przysługujących organom podatkowym lub organom kontroli skarbowej, stosuje się do postępowań bezpieczeństwa przemysłowego i organów prowadzących takie postępowania.

5. Odpowiednie poświadczenie bezpieczeństwa, o którym mowa w ust. 3, oznacza poświadczenie upoważniające do dostępu do informacji niejawnych o klauzuli tajności:



- 1) wskazanej we wniosku o wydanie świadectwa bezpieczeństwa przemysłowego w stosunku do kierownika przedsiębiorcy, pełnomocnika ochrony i jego zastępcy oraz osób przewidzianych na te stanowiska oraz osób zatrudnionych w pionie ochrony;
- 2) nie niższej niż wskazana we wniosku o wydanie świadectwa bezpieczeństwa przemysłowego w stosunku do administratora systemu informatycznego;
- 3) nie wyższej niż wskazana we wniosku o wydanie świadectwa bezpieczeństwa przemysłowego w stosunku do pozostałych osób wskazanych w kwestionariuszu, które powinny mieć dostęp do informacji niejawnych, zatrudnionych przez przedsiębiorcę .

6. ABW lub SKW może przeprowadzić postępowanie sprawdzające w celu wydania osobie wskazanej w ust. 3, zatrudnionej u przedsiębiorcy ubiegającego się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych NATO, UE lub ESA, o klauzuli równorzędnej klauzuli „tajne” lub posiadającego takie świadectwo, poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych międzynarodowych tych organizacji o klauzuli równorzędnej klauzuli „ściśle tajne”, jeżeli posiadanie takiego poświadczenia jest niezbędne do wykonania:

- 1) umowy zawartej z jednostkami organizacyjnymi wymienionymi w art. 1 ust. 2 pkt 1-2, organami lub instytucjami organizacji międzynarodowej;
- 2) zadania wynikającego z przepisów prawa.

**Art. 58.** 1. Sprawdzenia przedsiębiorcy i osób wymienionych w art. 57 przeprowadza się na podstawie danych zawartych w kwestionariuszu oraz innych informacji uzyskanych w trakcie postępowania bezpieczeństwa przemysłowego pozwalających ocenić zdolność przedsiębiorcy do ochrony informacji niejawnych.

2. Kwestionariusz zawiera:

- 1) dane identyfikujące podmiot podlegający sprawdzeniu, w tym określenie jego statusu prawnego;
- 2) dane o strukturze kapitału i powiązaniach kapitałowych przedsiębiorcy;
- 3) dane o źródłach pochodzenia środków finansowych i sytuacji finansowej przedsiębiorcy;
- 4) dane o strukturze organizacyjnej przedsiębiorcy;
- 5) dane dotyczące wszystkich osób wchodzących w skład organów zarządzających i kontrolnych przedsiębiorcy oraz osób działających z ich upoważnienia;
- 6) dane o systemie ochrony informacji niejawnych przedsiębiorcy, w tym o stosowanych środkach bezpieczeństwa fizycznego;
- 7) wykaz osób zatrudnionych przez przedsiębiorcę posiadających poświadczenia bezpieczeństwa uprawniające do dostępu do informacji niejawnych;
- 8) wykaz osób zatrudnionych przez przedsiębiorcę, które powinny być poddane poszerzonemu postępowaniu sprawdzającemu;
- 9) wykaz osób, które ze strony przedsiębiorcy wykonują lub będą wykonywać funkcje związane z ochroną informacji niejawnych;
- 10) imię, nazwisko i podpis osoby upoważnionej do składania oświadczeń woli w imieniu przedsiębiorcy albo kierownika przedsiębiorcy.

3. Rada Ministrów określi, w drodze rozporządzenia, wzór kwestionariusza, uwzględniając w kwestionariuszu zakres danych określonych w ust. 2 oraz jego przejrzystość i czytelność dla przedsiębiorcy.

**Art. 59.** 1. ABW lub SKW, prowadząc postępowanie bezpieczeństwa przemysłowego, są obowiązane do:

- 1) kierowania się zasadami bezstronności i obiektywizmu;

- 2) rzetelnego udokumentowania czynności przeprowadzonych w toku postępowania;
- 3) wykazania najwyższej staranności co do zgodności postępowania z przepisami ustawy.

2. W razie niedających się usunąć wątpliwości w zakresie przesłanek stanowiących podstawę do odmowy wydania lub cofnięcia świadectwa bezpieczeństwa przemysłowego interes ochrony informacji niejawnych ma pierwszeństwo przed innymi prawnie chronionymi interesami.

3. W celu weryfikacji informacji uzyskanych w toku postępowania bezpieczeństwa przemysłowego lub sprawdzeń przedsiębiorcy oraz wynikających z nich wniosków i hipotez, mogących mieć wpływ na ocenę zdolności przedsiębiorcy do ochrony informacji niejawnych albo w celu ścigania za popełnienie przestępstwa lub przestępstwa skarbowego, służba prowadząca postępowanie może w treści dokonywanego sprawdzenia lub po zakończeniu postępowania przekazać właściwemu organowi informacje lub kopie dokumentów uzyskanych w jego trakcie.

**Art. 60.** 1. W przypadku postępowania bezpieczeństwa przemysłowego prowadzonego w celu wydania świadectwa trzeciego stopnia, zatrudnienie pełnomocnika ochrony nie jest wymagane, z wyjątkiem ubiegania się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli równorzędnej klauzuli "poufne" lub wyższej, stosowanej przez NATO, UE lub ESA.

2. Pełnomocnik ochrony jednostki organizacyjnej zawierającej z przedsiębiorcą umowę, z której wykonaniem łączy się dostęp do informacji niejawnych o klauzuli "poufne", może przeprowadzić zwykłe postępowanie sprawdzające oraz zorganizować szkolenie w zakresie ochrony informacji niejawnych wobec osób określonych w art. 57 ust. 3 pkt 5 w przypadku postępowania bezpieczeństwa przemysłowego prowadzonego w związku z wnioskiem o wydanie świadectwa trzeciego stopnia. Odpowiednie wnioski kierownik przedsiębiorcy składa do kierownika jednostki organizacyjnej, która zawiera z tym przedsiębiorcą umowę.

**Art. 61.** Postępowanie bezpieczeństwa przemysłowego powinno być zakończone w terminie nie dłuższym niż 9 miesięcy, z zastrzeżeniem art. 46 ust. 1, licząc od dnia wniesienia przez przedsiębiorcę opłaty za przeprowadzenie czynności sprawdzenia przedsiębiorcy.

**Art. 62.** 1. ABW albo SKW umarza postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 57 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.

2. Decyzję o umorzeniu postępowania bezpieczeństwa przemysłowego, w tym postępowań sprawdzających wobec osób wymienionych w art. 57 ust. 3, organ je prowadzący doręcza wnioskodawcy, pełnomocnikowi ochrony oraz – w przypadku postępowań sprawdzających – osobie sprawdzanej.

**Art. 63.** 1. ABW albo SKW zawiesza lub podejmuje postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 57 ust. 3 pkt 5, na wniosek przedsiębiorcy.

2. ABW albo SKW może z urzędu zawiesić postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 57 ust. 3, w przypadku:

- 1) wydania przez inny organ decyzji nakazującej przedsiębiorcy wstrzymanie prowadzenia działalności gospodarczej;
- 2) wszczęcia postępowania upadłościowego wobec przedsiębiorcy;
- 3) nieregulowania w terminie zobowiązań publicznoprawnych;

- 4) uzależnienia wyniku oceny zdolności przedsiębiorcy do ochrony informacji niejawnych od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd;
- 5) zawieszenia postępowania sprawdzającego prowadzonego wobec kierownika przedsiębiorcy;
- 6) gdy przeprowadzenie skutecznego postępowania bezpieczeństwa przemysłowego nie jest możliwe z innych przyczyn niezależnych od organu je prowadzącego.

3. Postanowienie o zawieszeniu, podjęciu oraz odmowie podjęcia postępowania bezpieczeństwa przemysłowego, w tym postępowań sprawdzających prowadzonych wobec osób wymienionych w art. 57 ust. 3, organ je prowadzący doręcza wnioskodawcy, pełnomocnikowi ochrony oraz – w przypadku postępowań sprawdzających – osobie sprawdzanej.

4. W okresie zawieszenia postępowania bezpieczeństwa przemysłowego ABW albo SKW może podejmować czynności mające na celu ustalenie zmian okoliczności mogących stanowić podstawę do podjęcia zawieszono postępowania lub jeżeli przeprowadzenie tych czynności jest niezbędne dla interesu ochrony informacji niejawnych.

5. ABW albo SKW podejmuje z urzędu postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 57 ust. 3, zawieszono na podstawie ust. 2, po ustaniu przyczyn zawieszenia.

**Art. 64.** 1. Postępowanie bezpieczeństwa przemysłowego kończy się wydaniem przez ABW albo SKW:

- 1) świadectwa zgodnie z wnioskiem przedsiębiorcy;
- 2) decyzji o odmowie wydania świadectwa;
- 3) decyzji o umorzeniu postępowania.

2. ABW albo SKW 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 lub źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy, w tym również legalności ich pochodzenia;
- 3) niezorganizowania, w terminie 6 miesięcy od daty wszczęcia postępowania, systemu ochrony informacji niejawnych w przypadku ubiegania się o świadectwo drugiego stopnia lub niezorganizowania w terminie, o którym mowa w art. 46 ust. 1, licząc od daty wszczęcia postępowania, systemu ochrony informacji niejawnych, w przypadku ubiegania się o świadectwo pierwszego stopnia;
- 4) stwierdzenia niedających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1-3 lub 5-6, w stosunku do osoby, która:
  - a) dysponuje bezpośrednio lub pośrednio większością głosów na zgromadzeniu wspólników albo na walnym zgromadzeniu sprawdzanego przedsiębiorcy, także jako zastawnik albo użytkownik, bądź w zarządzie tego przedsiębiorcy, a jeżeli przedsiębiorca prowadzi działalność w formie spółki osobowej, większością głosów w tej spółce, także na podstawie porozumień z innymi osobami,
  - b) jest uprawniona do powoływania lub odwoływania większości członków zarządu sprawdzanego przedsiębiorcy, także na podstawie porozumień z innymi osobami,
  - c) jest uprawniona do powoływania lub odwoływania większości członków rady nadzorczej sprawdzanego przedsiębiorcy, także na podstawie porozumień z innymi osobami,

- d) wywiera decydujący wpływ na działalność sprawdzanego przedsiębiorcy, w szczególności na podstawie zawartej ze sprawdzanym przedsiębiorcą umowy przewidującej zarządzanie nim lub przekazywanie przez niego zysku;
- 5) skazania prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe oskarżona lub nieprawomocnego skazania albo przedstawienia zarzutu popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3, osoby, o której mowa w pkt 4;
- 6) ustalenia okoliczności w odniesieniu do podmiotu zarejestrowanego poza granicami Rzeczypospolitej Polskiej posiadającego większość wkładów, udziałów lub akcji w kapitale sprawdzanego przedsiębiorcy, bądź spółki z kapitałem zagranicznym pełniącej w stosunku do sprawdzanego przedsiębiorcy rolę spółki dominującej w rozumieniu art. 4 § 1 pkt 4 ustawy z dnia 15 września 2000 r. – Kodeks spółek handlowych (Dz. U. z 2017 r. poz. 1577 z późn. zm.<sup>7</sup>) wywołujących niedające się usunąć wątpliwości dotyczące:
- a) finansowania działalności tego podmiotu lub spółki przez obce służby specjalne, organizacje terrorystyczne, organizacje, o których mowa w art. 13 Konstytucji Rzeczypospolitej Polskiej, lub zorganizowane grupy przestępcze,
  - b) uczestnictwa lub wspierania przez ten podmiot lub spółkę działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko bezpieczeństwu lub porządkowi ustrojowemu Rzeczypospolitej Polskiej lub bezpieczeństwu jej sojuszników,
  - c) uczestnictwa w międzynarodowym obrocie produktami podwójnego zastosowania bez wymaganych zezwoleń.

3. ABW albo SKW może odmówić wydania świadectwa, stwierdzając brak zdolności do ochrony informacji niejawnych, z powodu:

- 1) ujawnienia, w wyniku sprawdzenia osób wchodzących w skład organów zarządzających i kontrolnych oraz osób działających z ich upoważnienia, w toku postępowania bezpieczeństwa przemysłowego niedających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1-3 lub 5-6 albo skazania ich prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe oskarżona lub nieprawomocnego ich skazania albo przedstawienia im zarzutu popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3;
- 2) niepowiadomienia w terminie 30 dni o zmianie danych zawartych w kwestionariuszu w trakcie postępowania bezpieczeństwa przemysłowego;
- 3) zatajenia danych w kwestionariuszu lub podania w nim danych nieprawdziwych;
- 4) podania nieprawdziwych informacji o zmianach danych zawartych w kwestionariuszu;
- 5) upływu w toku prowadzonego postępowania bezpieczeństwa przemysłowego okresu ważności poświadczenia bezpieczeństwa kierownika przedsiębiorcy i niezłożenia w trybie art. 32 ust. 1 wniosku o przeprowadzenie kolejnego postępowania sprawdzającego, a także niezłożenia w terminie 30 dni od dnia powołania na stanowisko, wniosku o przeprowadzenie poszerzonego postępowania sprawdzającego oraz ankiety wypełnionej przez kierownika przedsiębiorcy;

---

<sup>7</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 398, 650, 1544, 2219, 2244 oraz z 2019 r. poz. 55 i 60.

- 6) stwierdzenia niedających się usunąć wątpliwości dotyczących legalności pochodzenia środków finansowych, które pozostają lub pozostawały w dyspozycji przedsiębiorcy;
- 7) braku możliwości ustalenia struktury kapitałowej lub źródeł pochodzenia środków finansowych pozostających w dyspozycji podmiotu posiadającego większość wkładów, udziałów lub akcji w kapitale sprawdzanego przedsiębiorcy, bądź spółki z kapitałem zagranicznym pełniącej w stosunku do sprawdzanego przedsiębiorcy rolę spółki dominującej w rozumieniu art. 4 § 1 pkt 4 ustawy z dnia 15 września 2000 r. – Kodeks spółek handlowych;
- 8) braku możliwości ustalenia w toku postępowania bezpieczeństwa przemysłowego beneficjenta rzeczywistego, o którym mowa w art. 2 ust. 2 pkt. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. 2018, poz. 723 z późn. zm.);
- 9) stwierdzenia niedających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1-3 lub 5-6 oraz ust. 3, a także w przypadku odmowy wydania poświadczenia bezpieczeństwa albo cofnięcia poświadczenia bezpieczeństwa, w stosunku do osoby:
  - a) posiadającej co najmniej 5% wkładów, udziałów lub akcji w kapitale sprawdzanego przedsiębiorcy,
  - b) będącej beneficjentem rzeczywistym, ustalonym w toku postępowania bezpieczeństwa przemysłowego,
  - c) która w trakcie trwania postępowania bezpieczeństwa przemysłowego posiadała większość wkładów, udziałów lub akcji w kapitale sprawdzanego przedsiębiorcy, w szczególności, gdy te wkłady, udziały lub akcje zostały zbyte albo przekazane osobie jej bliskiej lub zaufanej;
- 10) skazania prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe oskarżona lub nieprawomocnego skazania albo przedstawienia zarzutu popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3, osoby, o której mowa w pkt 9.

**Art. 65.** 1. ABW albo SKW, w okresie ważności świadectwa, może przeprowadzić sprawdzenie przedsiębiorcy w zakresie, o którym mowa w art. 57 ust. 2, w celu ustalenia, czy nie utracił on zdolności do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem. Sprawdzenie to musi być rzetelnie udokumentowane i prowadzone zgodnie z zasadami bezstronności, obiektywizmu i z zachowaniem najwyższej staranności. Dokumentację tej czynności dołącza się do akt postępowania bezpieczeństwa przemysłowego.

2. W przypadku, gdy świadectwo zostało wydane przez ABW, a przedsiębiorca realizuje umowę na rzecz 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 ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie lub sprawdzenia przedsiębiorcy w zakresie, o którym mowa w art. 57 ust. 2.

3. W kontroli lub sprawdzeniu, o których mowa w ust. 2, mogą uczestniczyć żołnierze lub funkcjonariusze SKW. Przed kontrolą lub sprawdzeniem upoważnieni żołnierze lub funkcjonariusze SKW mogą zapoznać się z aktami postępowania bezpieczeństwa przemysłowego w zakresie objętym kontrolą lub sprawdzeniem.

4. W przypadku wydania świadectwa przez SKW i realizacji przez przedsiębiorcę umów na rzecz innych jednostek organizacyjnych niż podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, przepisy ust. 2 i 3 stosuje się odpowiednio w stosunku do ABW i jej funkcjonariuszy.

**Art. 66.** 1. Wyniki sprawdzenia przedsiębiorcy o którym mowa w art. 65, lub ustalenia kontroli ochrony informacji niejawnych mogą stanowić podstawę wydania decyzji o cofnięciu świadectwa.

2. ABW albo SKW cofa świadectwo, stwierdzając utratę zdolności do ochrony informacji niejawnych, z powodu występowania okoliczności, o których mowa w art. 64 ust. 2 pkt 1, 2, 4, 5 lub 6.

3. ABW albo SKW może cofnąć świadectwo, stwierdzając utratę zdolności do ochrony informacji niejawnych, z powodu:

- 1) ujawnienia, w wyniku sprawdzeń osób wchodzących w skład organów zarządzających i kontrolnych oraz osób działających z ich upoważnienia, w okresie ważności świadectwa bezpieczeństwa przemysłowego niedających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1-3 lub 5-6 albo skazania ich prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe oskarżona lub nieprawomocnego ich skazania albo przedstawienia im zarzutu popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3;
- 2) stwierdzenia występowania okoliczności, o których mowa w art. 64 ust. 3 pkt 6-8, pkt 9 lit. a-b, lub 10;
- 3) stwierdzenia niedających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1-3 lub 5-6 oraz ust. 3, a także w przypadku odmowy wydania poświadczenia bezpieczeństwa albo cofnięcia poświadczenia bezpieczeństwa w stosunku do osoby, która w okresie ważności świadectwa bezpieczeństwa przemysłowego posiadała większość wkładów, udziałów lub akcji w kapitale sprawdzanego przedsiębiorcy, w szczególności, gdy te wkłady, udziały lub akcje zostały zbyte albo przekazane osobie jej bliskiej lub zaufanej;
- 4) skazania prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe oskarżona lub nieprawomocnego skazania albo przedstawienia zarzutu popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3, osoby, o której mowa w pkt 3;
- 5) niewykonania przez przedsiębiorcę obowiązku, o którym mowa w art. 69 ust. 1;
- 6) podania nieprawdziwych danych lub zatajenia danych w ramach przekazywanych ABW albo SKW informacji o zmianach danych zawartych w kwestionariuszu;
- 7) utraty funkcjonalności systemu ochrony informacji niejawnych, w tym upływu w okresie ważności świadectwa bezpieczeństwa przemysłowego ważności poświadczenia bezpieczeństwa kierownika przedsiębiorcy i niezłożenia wniosku o przeprowadzenie kolejnego postępowania sprawdzającego w trybie, o którym mowa w art. 32 ust. 1, a także niezłożenia w terminie 30 dni od dnia powołania na stanowisko wniosku o przeprowadzenie poszerzonego postępowania sprawdzającego oraz ankiety wypełnionej przez kierownika przedsiębiorcy lub nieprzesłania informacji o posiadaniu odpowiedniego poświadczenia bezpieczeństwa.

4. O cofnięciu świadectwa ABW albo SKW zawiadamia niezwłocznie jednostki organizacyjne, które zawarły z przedsiębiorcą umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej.

5. Przepisy art. 40 stosuje się odpowiednio w przypadku:

- 1) cofnięcia świadectwa;
- 2) wygaśnięcia świadectwa na skutek upływu okresu jego ważności, zrzeczenia się uprawnień określonych w świadectwie i niewystąpienia z wnioskiem o potwierdzenie uprawnień na podstawie art. 55 ust. 4 lub 5 albo przejęcia przez inny podmiot lub likwidacji;
- 3) zrzeczenia się przez przedsiębiorcę uprawnień do przetwarzania informacji niejawnych w trybie art. 55 ust. 4 pkt. 2;
- 4) utraty zdolności przedsiębiorcy do przetwarzania informacji niejawnych o określonej klauzuli tajności.

**Art. 67.** 1. Świadectwo, decyzja o odmowie wydania świadectwa oraz decyzja o cofnięciu świadectwa zawiera:

- 1) oznaczenie organu, który wydał, odmówił wydania bądź cofnął świadectwo;
- 2) wskazanie miejsca i daty wydania;
- 3) nazwę podmiotu, adres jego siedziby, numer identyfikacji podatkowej (NIP), a także numer w Krajowym Rejestrze Sądowym – jeżeli go posiada;
- 4) podstawę prawną;
- 5) stwierdzenie wydania świadectwa, odmowy wydania lub jego cofnięcia;
- 6) w przypadku wydania świadectwa - jego stopień, klauzulę tajności oraz termin ważności;
- 7) imię, nazwisko, stopień służbowy, stanowisko służbowe i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub 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 odwołania do Ministra Koordynatora Służb Specjalnych, a w przypadku gdy minister ten nie-został powołany, do Prezesa Rady Ministrów.

3. Uzasadnienie faktyczne w części zawierającej informacje niejawne podlega ochronie na zasadach określonych w niniejszej ustawie.

**Art. 68.** Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory:

- 1) świadectwa;
  - 2) decyzji o odmowie wydania świadectwa;
  - 3) decyzji o cofnięciu świadectwa
- uwzględniając zakres danych określonych w art. 67 ust. 1 i 2 oraz zapewniając zróżnicowanie wzorów świadectw i decyzji wydawanych przez ABW i SKW.

**Art. 69.** 1. Przedsiębiorca, w czasie trwania postępowania bezpieczeństwa przemysłowego, a także w okresie ważności świadectwa, ma obowiązek informowania w terminie 30 dni odpowiednio ABW lub SKW o:

- 1) zmianach danych zawartych w kwestionariuszu, ogłoszeniu upadłości, likwidacji lub rozwiązaniu jednostki organizacyjnej albo innej formie zakończenia przez nią działalności;
- 2) zawarciu umowy związanej z dostępem do informacji niejawnych o klauzuli "poufne" lub wyższej, ze szczególnym uwzględnieniem nazwy i adresu jednostki organizacyjnej, z którą zawarto umowę, przedmiotu umowy oraz najwyższej klauzuli tajności informacji niejawnych,

do których dostęp będzie wiązał się z wykonaniem umowy, a także o jej wypowiedzeniu oraz zakończeniu wykonywania;

3) zawarciu umowy z podwykonawcą, związanej z dostępem do informacji niejawnych o klauzuli "poufne" lub wyższej, jej wypowiedzeniu oraz zakończeniu wykonywania.

2. Przedsiębiorca, w czasie realizacji umowy, ma obowiązek niezwłocznego informowania osoby odpowiedzialnej za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę obowiązku ochrony wytworzonych w związku z realizacją umowy lub przekazanych mu informacji niejawnych, 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 umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej zawarto z jednostką organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną, ABW, po uzyskaniu od przedsiębiorcy informacji o zawarciu umowy związanej z dostępem do informacji niejawnych o klauzuli "poufne" lub wyższej, przekazuje ją SKW.

4. W przypadku, gdy umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej zawarto z jednostką organizacyjną inną niż podległa Ministrowi Obrony Narodowej lub przez niego nadzorowana, SKW, po uzyskaniu od przedsiębiorcy informacji o zawarciu umowy związanej z dostępem do informacji niejawnych o klauzuli "poufne" lub wyższej, przekazuje ją ABW.

**Art. 70.** 1. Jednostka organizacyjna zlecająca realizację umowy związanej z dostępem do informacji niejawnych o klauzuli "poufne" lub wyższej jest odpowiedzialna za wprowadzenie do umowy instrukcji bezpieczeństwa przemysłowego, określającej:

1) szczegółowe wymagania dotyczące ochrony informacji niejawnych o klauzuli "poufne" lub wyższej, które zostaną przekazane przedsiębiorcy w związku z wykonywaniem umowy, odpowiednie do liczby 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 ustawy, a także nieprzestrzegania wymagań określonych w instrukcji bezpieczeństwa przemysłowego.

2. Instrukcja bezpieczeństwa przemysłowego określa w szczególności:

1) klauzule tajności poszczególnych materiałów lub rodzajów materiałów, które zostaną wytworzone przez przedsiębiorcę w związku z wykonywaniem umowy;

2) sposób postępowania z materiałami niejawnymi, które zostaną przekazane przedsiębiorcy lub przez niego wytworzone w związku z wykonywaniem umowy oraz tryb postępowania z nimi po zakończeniu umowy.

3. Kierownik jednostki organizacyjnej zawierającej umowę związaną z dostępem do informacji niejawnych o klauzuli "poufne" lub wyższej wyznacza osobę odpowiedzialną za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę obowiązku ochrony wytworzonych w związku z realizacją umowy lub przekazanych mu informacji niejawnych.

4. Jeżeli w związku z wykonywaniem umowy zostaną wytworzone informacje niejawne, odpowiednią klauzulę tajności nadaje osoba uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału, zgodnie ze wskazaniem zawartymi w instrukcji bezpieczeństwa przemysłowego, a w przypadku ich braku, po uzgodnieniu z osobą odpowiedzialną za



nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę obowiązku ochrony wytworzonych w związku z realizacją umowy lub przekazanych mu informacji niejawnych.

5. Jednostka organizacyjna, która zawarła umowę związaną z dostępem do informacji niejawnych o klauzuli "poufne" lub wyższej, ma obowiązek:

- 1) niezwłocznego informowania odpowiednio ABW lub SKW o:
  - a) nazwie i adresie siedziby przedsiębiorcy, z którym zawarto umowę,
  - b) przedmiocie umowy,
  - c) najwyższej koniecznej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonywaniem umowy,
  - d) naruszeniu przepisów o ochronie informacji niejawnych u przedsiębiorcy, z którym zawarto umowę,
  - e) zakończeniu wykonywania umowy;
- 2) niezwłocznego przekazania odpowiednio ABW lub SKW:
  - a) kopii instrukcji bezpieczeństwa przemysłowego,
  - b) kopii świadectwa lub poświadczenia bezpieczeństwa przedsiębiorcy, z którym zawarto umowę.

6. W przypadku, gdy umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej zawarła z przedsiębiorcą jednostka organizacyjna podległa Ministrowi Obrony Narodowej lub przez niego nadzorowana, a świadectwo zostało wydane przez ABW, obowiązek, o którym mowa w ust. 5, jest realizowany także wobec SKW.

7. W przypadku, gdy umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej zawarła z przedsiębiorcą jednostka organizacyjna inna niż podległa Ministrowi Obrony Narodowej lub przez niego nadzorowana, a świadectwo zostało wydane przez SKW, obowiązek, o którym mowa w ust. 5, jest realizowany także wobec ABW.

## Rozdział 8

### Postępowanie odwoławcze i skargowe

**Art. 71.** 1. Od decyzji o odmowie wydania poświadczenia bezpieczeństwa, o cofnięciu poświadczenia bezpieczeństwa albo o umorzeniu postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego, wydanej przez ABW, SKW lub służbę, o której mowa w art. 23 ust. 8, osobie sprawdzanej przysługuje odwołanie do organu odwoławczego, którym jest Minister Koordynator Służb Specjalnych, a w przypadku gdy minister ten nie został powołany, Prezes Rady Ministrów. Odwołanie nie wymaga uzasadnienia.

2. Od decyzji o umorzeniu postępowania bezpieczeństwa przemysłowego, odmowie wydania oraz o cofnięciu świadectwa przedsiębiorcy przysługuje odwołanie do organu odwoławczego.

3. Odwołanie wnosi się w terminie 14 dni od dnia doręczenia osobie sprawdzanej decyzji, o której mowa w ust. 1, lub przedsiębiorcy decyzji, o której mowa w ust. 2, za pośrednictwem organu, który przeprowadził postępowanie sprawdzające, kontrolne postępowanie sprawdzające lub postępowanie bezpieczeństwa przemysłowego.

4. Organ, który przeprowadził postępowanie sprawdzające, kontrolne postępowanie sprawdzające, lub postępowanie bezpieczeństwa przemysłowego jest obowiązany przesłać odwołanie, o którym mowa w ust. 1, wraz z aktami postępowania sprawdzającego, kontrolnego

postępowania sprawdzającego lub postępowania bezpieczeństwa przemysłowego organowi odwoławczemu, w terminie 14 dni od dnia, w którym otrzymał odwołanie.

5. Rozpatrzenie odwołania powinno nastąpić nie później niż w ciągu 3 miesięcy od dnia jego otrzymania.

6. Wniesienie odwołania nie wstrzymuje wykonania decyzji.

**Art. 72.** 1. Organ odwoławczy stwierdza, w drodze postanowienia:

- 1) niedopuszczalność odwołania, o którym mowa w art. 71 ust. 1 i 2;
  - 2) uchybienie terminowi do wniesienia odwołania, o którym mowa w art. 71 ust. 3.
2. Postanowienie, o którym mowa w ust. 1, jest ostateczne i zawiera w szczególności:

- 1) oznaczenie organu odwoławczego;
- 2) datę wydania;
- 3) oznaczenie osoby sprawdzanej albo przedsiębiorcy;
- 4) powołanie podstawy prawnej;
- 5) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne;
- 6) pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego;
- 7) podpis, z podaniem imienia i nazwiska oraz stanowiska służbowego, osoby upoważnionej do jego wydania.

3. Organ odwoławczy, w celu uzupełnienia dowodów i materiałów w postępowaniu sprawdzającym, kontrolnym postępowaniu sprawdzającym lub postępowaniu bezpieczeństwa przemysłowego, może, z urzędu lub na żądanie osoby sprawdzanej albo przedsiębiorcy, zlecić właściwemu podmiotowi przeprowadzenie dodatkowych czynności, w tym badania specjalistycznego, o którym mowa w art. 25 ust. 8 oraz badania poligraficznego, o którym mowa w art. 26 ust. 7.

4. Organ odwoławczy wydaje decyzję, w której:

- 1) utrzymuje w mocy decyzję organu, który przeprowadził postępowanie sprawdzające, kontrolne postępowanie sprawdzające lub postępowanie bezpieczeństwa przemysłowego albo wydał decyzję o cofnięciu świadectwa;
- 2) uchyla decyzję organu, który przeprowadził kontrolne postępowanie sprawdzające zakończone decyzją o cofnięciu poświadczenia bezpieczeństwa albo wydał decyzję o cofnięciu świadectwa;
- 3) uchyla decyzję organu, który przeprowadził postępowanie sprawdzające lub postępowanie bezpieczeństwa przemysłowego, i nakazuje mu wydanie poświadczenia bezpieczeństwa albo świadectwa;
- 4) uchyla decyzję organu, który przeprowadził postępowanie sprawdzające, kontrolne postępowanie sprawdzające lub postępowanie bezpieczeństwa przemysłowego albo wydał decyzję o cofnięciu świadectwa, i przekazuje sprawę do ponownego rozpatrzenia.

5. Decyzja organu odwoławczego zawiera w szczególności:

- 1) oznaczenie organu odwoławczego;
- 2) datę wydania;
- 3) oznaczenie osoby sprawdzanej albo przedsiębiorcy;
- 4) powołanie podstawy prawnej;
- 5) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne;
- 6) pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego;
- 7) podpis, z podaniem imienia i nazwiska oraz stanowiska służbowego osoby upoważnionej do jej wydania.

6. Organ odwoławczy, po wydaniu decyzji lub postanowienia, niezwłocznie zwraca właściwemu organowi akta postępowania sprawdzającego, kontrolnego postępowania sprawdzającego lub postępowania bezpieczeństwa przemysłowego.

7. Decyzje i postanowienia doręcza się na piśmie osobie sprawdzanej albo przedsiębiorcy i właściwemu organowi, który przeprowadził postępowanie sprawdzające, kontrolne postępowanie sprawdzające lub postępowanie bezpieczeństwa przemysłowego albo wydał decyzję o cofnięciu świadectwa, zawiadamiając o rozstrzygnięciu zawartym w decyzji lub postanowieniu osobę uprawnioną do obsady stanowiska.

8. Do postępowania odwoławczego przepisy art. 27, art. 30 ust. 4, art. 31, art. 62, art. 63 oraz art. 67 ust. 3 stosuje się odpowiednio.

9. Do postępowania, o którym mowa w art. 156 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, przepisy niniejszego rozdziału stosuje się odpowiednio.

**Art. 73.** 1. Na postanowienie o zawieszeniu postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego oraz postanowienie o odmowie podjęcia zawieszono postępowania sprawdzającego lub zawieszono kontrolnego postępowania sprawdzającego, a także na postanowienie o odmowie wszczęcia postępowania, osobie sprawdzanej przysługuje zażalenie do organu odwoławczego. Zażalenie nie wymaga uzasadnienia.

2. Na postanowienie o zawieszeniu z urzędu postępowania bezpieczeństwa przemysłowego oraz na postanowienie o odmowie podjęcia tego postępowania, przedsiębiorcy przysługuje zażalenie do organu odwoławczego. Zażalenie nie wymaga uzasadnienia.

3. Do zażalenia, o którym mowa w ust. 1 i 2, stosuje się odpowiednio przepisy, o których mowa w art. 71 ust. 3-6 oraz art. 72 ust. 1-2 i 5-8.

4. Organ odwoławczy wydaje postanowienie, w którym:

- 1) utrzymuje w mocy postanowienie organu, który zawiesił postępowanie sprawdzające, kontrolne postępowanie sprawdzające lub postępowanie bezpieczeństwa przemysłowego;
- 2) uchyla postanowienie organu, który zawiesił postępowanie sprawdzające, kontrolne postępowanie sprawdzające lub postępowanie bezpieczeństwa przemysłowego.

**Art. 74.** 1. Od wydanej przez pełnomocnika ochrony decyzji o odmowie wydania poświadczenia bezpieczeństwa, o cofnięciu poświadczenia bezpieczeństwa albo o umorzeniu postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego, w wyniku zwykłego postępowania sprawdzającego, osobie sprawdzanej służy, z wyłączeniem postępowań sprawdzających prowadzonych przez służby, o których mowa w art. 23 ust. 8, odwołanie odpowiednio do Szefa ABW lub Szefa SKW.

2. Do postępowania odwoławczego prowadzonego przed Szefem ABW lub Szefem SKW stosuje się odpowiednio przepisy ustawy dotyczące postępowania odwoławczego prowadzonego przed Ministrem Koordynatorem Służb Specjalnych, a w przypadku gdy minister ten nie został powołany, przed Prezesem Rady Ministrów.

3. Do rozpatrywania przez Szefa ABW albo Szefa SKW zażaleń na postanowienia wydane przez pełnomocnika ochrony w toku zwykłego postępowania sprawdzającego, z wyłączeniem postępowań sprawdzających prowadzonych przez służby, o których mowa w art. 23 ust. 8, przepis art. 73 stosuje się odpowiednio.

4. Odwołanie do Szefa ABW lub Szefa SKW składa się za pośrednictwem pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające.

**Art. 75.** 1. Osobie sprawdzanej lub przedsiębiorcy przysługuje skarga do sądu administracyjnego na decyzję lub postanowienie wydane w toku postępowania odwoławczego w terminie 30 dni od dnia doręczenia tej decyzji lub postanowienia.

2. Sąd administracyjny rozpatruje skargę na posiedzeniu niejawnym.

3. Odpis sentencji wyroku z uzasadnieniem doręcza się tylko właściwemu organowi odwoławczemu. Skarżącemu doręcza się odpis sentencji wyroku oraz uzasadnienie z wyłączeniem tej części uzasadnienia faktycznego, która zawiera informacje niejawne. Osobie uprawnionej do obsady stanowiska doręcza się tylko odpis wyroku.

4. Akta postępowania sprawdzającego, kontrolnego postępowania sprawdzającego lub postępowania bezpieczeństwa przemysłowego są zwracane przez sąd administracyjny niezwłocznie po uprawomocnieniu się wyroku.

5. Do skargi kasacyjnej stosuje się odpowiednio ust. 2-4.

## Rozdział 9

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

**Art. 76.** 1. Akta postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, pozostające w dyspozycji ABW, SKW oraz służb, o których mowa w art. 23 ust. 8, są udostępniane do wglądu lub przekazywane:

- 1) właściwemu organowi w celu rozpatrzenia odwołania lub zażalenia;
- 2) sądowi administracyjnemu w związku z rozpatrywaniem skargi.

2. Akta, o których mowa w ust. 1, są udostępniane do wglądu lub przekazywane na pisemne żądanie:

- 1) sądowi lub prokuratorowi dla celów postępowania karnego;
- 2) właściwemu organowi w celu przeprowadzenia kontroli prawidłowości postępowania, z wyłączeniem postępowań, prowadzonych przez służby, o których mowa w art. 23 ust. 8;
- 3) ABW lub SKW, w przypadku przejęcia postępowania sprawdzającego, kontrolnego postępowania sprawdzającego lub postępowania bezpieczeństwa przemysłowego do dalszej realizacji w trybie art. 10 ust. 5 pkt 3 lub 4;
- 4) Inspektorowi Nadzoru Wewnętrznego w celu realizacji zadania określonego w art. 11a ust. 3 pkt 9 ustawy z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych (Dz. U. z 2018 r. poz. 2216 oraz z 2019 r. poz. 15).

3. Materiały zgromadzone w aktach postępowań, o których mowa w ust. 1, mogą zostać:

- 1) udostępnione lub przekazane do wglądu:
  - a) właściwemu organowi dla celów postępowania karnego, karno-skarbowego lub postępowania określonego przepisami ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa,
  - b) ABW, SKW albo służbom, o których mowa w art. 23 ust. 8, dla celów postępowania sprawdzającego, kontrolnego postępowania sprawdzającego, postępowania bezpieczeństwa przemysłowego i sprawdzeń przedsiębiorcy;
- 2) wykorzystane na potrzeby realizacji ustawowych zadań ABW, SKW albo służb, o których mowa w art. 23 ust. 8.

4. W przypadkach, o których mowa w ust. 3 pkt 1 lit. b oraz w ust. 3 pkt 2, służba, w której dyspozycji pozostają akta, o których mowa w ust. 1, może ich nie udostępnić lub nie przekazać do wglądu, ze względu na ważny interes tej służby.

5. Materiały zgromadzone w aktach zwykłych postępowań sprawdzających lub kontrolnych postępowań sprawdzających przeprowadzonych przez pełnomocników ochrony, z wyłączeniem zwykłych postępowań sprawdzających lub kontrolnych postępowań sprawdzających prowadzonych przez ABW, SKW albo służby, o których mowa w art. 23 ust. 8, są udostępniane do wglądu lub przekazywane w przypadkach określonych w ust. 1-3, a także innemu pełnomocnikowi ochrony dla celów postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego.

6. Materiały zgromadzone w aktach zwykłych postępowań sprawdzających lub kontrolnych postępowań sprawdzających przeprowadzonych przez pełnomocników ochrony, z wyłączeniem zwykłych postępowań sprawdzających lub kontrolnych postępowań sprawdzających prowadzonych przez ABW, SKW albo służby, o których mowa w art. 23 ust. 8, są udostępniane do wglądu osobie sprawdzanej na jej wniosek.

7. Udostępnione akta i materiały po ich wykorzystaniu do realizacji celów określonych ustawą są niezwłocznie zwracane organowi, który je udostępnił, z wyłączeniem przypadków, o których mowa w ust. 2 pkt 3.

8. Po zakończeniu postępowania sprawdzającego, kontrolnego postępowania sprawdzającego lub postępowania bezpieczeństwa przemysłowego akta tych postępowań są przechowywane przez co najmniej 20 lat, z uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r. poz. 217, 357, 398, 650 oraz z 2019 r. poz. 55) oraz aktów wykonawczych wydanych na jej podstawie:

- 1) jako wyodrębniona część w archiwach ABW, SKW albo służb, o których mowa w art. 23 ust. 8, które przeprowadziły te postępowania;
- 2) przez pełnomocnika ochrony lub w pionie ochrony, w przypadku akt zwykłych postępowań sprawdzających przeprowadzonych przez tego pełnomocnika.

9. W przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji jednostki organizacyjnej akta, o których mowa w ust. 8, przejmuje następca prawny, a w przypadku jego braku – odpowiednio ABW albo SKW.

10. Ze względu na istotny interes bezpieczeństwa państwa informacje uzyskane przez ABW, SKW albo służby, o których mowa w art. 23 ust. 8, w związku z postępowaniami sprawdzającymi, kontrolnymi postępowaniami sprawdzającymi lub postępowaniami bezpieczeństwa przemysłowego, o ile nie narusza to interesów służby, która przeprowadziła te postępowania – mogą zostać przekazane:

- 1) Prezydentowi Rzeczypospolitej Polskiej;
- 2) Prezesowi Rady Ministrów;
- 3) Marszałkowi Sejmu;
- 4) Ministrowi Koordynatorowi Służb Specjalnych, jeżeli został powołany;
- 5) Ministrowi Obrony Narodowej, Ministrowi Sprawiedliwości oraz ministrom właściwym do spraw wewnętrznych i do spraw zagranicznych – za zgodą Prezesa Rady Ministrów.

**Art. 77.** 1. ABW i SKW prowadzą ewidencję osób:

- 1) wobec których prowadzono postępowania sprawdzające oraz kontrolne postępowania sprawdzające, z wyłączeniem osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w służbach, o których mowa w art. 23 ust. 8;
- 2) którym wydano:

- a) zgodę na dostęp do informacji niejawnych, o której mowa w art. 37 ust. 1 i 5 oraz art. 54 ust. 7, a także zgodę na dostęp do informacji niejawnych międzynarodowych, o której mowa w art. 11 ust. 4 lub 5,
- b) upoważnienie do dostępu do informacji niejawnych o klauzuli "zastrzeżone" wydane kierownikowi jednostki organizacyjnej oraz przedsiębiorcy wykonującemu działalność jednoosobowo i osobiście;
- 3) którym przysługuje dostęp do informacji niejawnych na podstawie art. 35 ust. 5, 6 lub 8 - zawierającą dane, o których mowa w art. 16 ust. 1 pkt 13.

2. Dane z ewidencji, o których mowa w ust. 1, oraz wykazów, o których mowa w art. 16 ust. 1 pkt 13, są udostępniane na pisemne żądanie:

- 1) w przypadkach określonych w art. 76 ust. 2 i 10;
- 2) ABW, SKW oraz służbom, o których mowa w art. 23 ust. 8, dla celów postępowania sprawdzającego, kontrolnego postępowania sprawdzającego oraz postępowania bezpieczeństwa przemysłowego i sprawdzeń przedsiębiorcy, o których mowa w art. 65 ust. 1;
- 3) ABW, w związku z realizacją obowiązków, o których mowa w art. 10 ust. 1 pkt 8;
- 4) innym podmiotom, które wykażą interes prawny w uzyskaniu takiej informacji i jeżeli nie będzie stało to w sprzeczności z interesem ochrony informacji niejawnych – wyłącznie w celu potwierdzenia faktu posiadania lub braku uprawnień do dostępu do informacji niejawnych.

## Rozdział 10

### Ochrona informacji niejawnych w razie ogłoszenia mobilizacji i w czasie wojny

**Art. 78.** W razie ogłoszenia mobilizacji i w czasie wojny nie stosuje się przepisów określonych w art. 4, art. 21-34, art. 38 ust. 4, art. 45-48, art. 49 ust. 7-11, art. 50 ust. 1 i 3 oraz w art. 54-70.

**Art. 79. 1.** Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac w jednostce organizacyjnej, związanych z dostępem do informacji niejawnych o klauzuli "zastrzeżone" lub wyższej może nastąpić w przypadku:

- 1) posiadania poświadczenia bezpieczeństwa, a w razie jego braku po uzyskaniu pisemnego upoważnienia kierownika jednostki organizacyjnej, które zachowuje ważność w kolejnych jednostkach organizacyjnych oraz
- 2) po odbyciu szkolenia w zakresie ochrony informacji niejawnych.

2. W przypadku dostępu do informacji niejawnych o klauzuli "tajne" lub wyższej kierownik jednostki organizacyjnej o wydaniu upoważnienia, o którym mowa w ust. 1 pkt 1, niezwłocznie informuje ABW albo SKW.

3. ABW albo SKW może zgłosić zastrzeżenia dotyczące dostępu do informacji niejawnych osoby, której wydano upoważnienie, o którym mowa w ust. 1 pkt 1. W przypadku zgłoszenia zastrzeżeń, kierownik jednostki organizacyjnej uniemożliwia tej osobie dostęp do informacji niejawnych.

4. Osoby nieposiadające obywatelstwa polskiego nie mogą być dopuszczone do pracy lub pełnienia służby na stanowiskach albo wykonywania czynności zleconych, z którymi łączy się dostęp do informacji niejawnych o klauzuli "tajne" lub "ściśle tajne".

5. Przepisu ust. 4 nie stosuje się do:

- 1) osób zajmujących stanowiska związane z kierowaniem wykonywania przez przedsiębiorcę

- umowy związanej z dostępem do informacji niejawnych lub związane z bezpośrednim wykonywaniem takiej umowy albo wykonujących zadania na rzecz obronności lub bezpieczeństwa państwa, związane z dostępem do informacji niejawnych u przedsiębiorcy;
- 2) osób, które w imieniu przedsiębiorcy, o którym mowa w pkt 1, uczestniczą w czynnościach zmierzających do zawarcia umowy, jeżeli czynności te są związane z dostępem do informacji niejawnych;
  - 3) osób zatrudnionych w pionie ochrony przedsiębiorcy, o którym mowa w pkt 1, z wyjątkiem osoby zajmującej stanowisko pełnomocnika ochrony oraz zastępcy pełnomocnika ochrony;
  - 4) żołnierzy i personelu cywilnego wojsk obcych, pełniących służbę przy jednostkach i komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, przydzielonych lub skierowanych do wykonywania zadań na rzecz tych jednostek i komórek bądź też w międzynarodowych jednostkach dyslokowanych na terytorium Rzeczypospolitej Polskiej.

**Art. 80.** 1. Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa informatycznego dla systemu informatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli "zastrzeżone" lub wyższej przez zatwierdzenie dokumentacji bezpieczeństwa systemu informatycznego.

2. W przypadku gdy system, o którym mowa w ust. 1, będzie funkcjonował w więcej niż jednej jednostce organizacyjnej, akredytacji udziela kierownik jednostki organizującej system.

3. Bezpośrednio po udzieleniu akredytacji bezpieczeństwa informatycznego, kierownik jednostki organizującej system, informuje o tym fakcie odpowiednio ABW albo SKW, a następnie przekazuje dokumentację bezpieczeństwa systemu informatycznego.

4. ABW albo SKW przeprowadza ocenę bezpieczeństwa systemu, o którym mowa w ust. 3. ABW albo SKW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji bezpieczeństwa informatycznego, zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych.

**Art. 81.** 1. Warunkiem dostępu przedsiębiorcy do informacji niejawnych w związku z wykonywaniem umów albo zadań wynikających z przepisów prawa, zwanych dalej "umowami", jest zdolność do ochrony informacji niejawnych.

2. Dokumentem potwierdzającym zdolność do ochrony informacji niejawnych jest świadectwo bezpieczeństwa przemysłowego, a w razie jego braku, o zdolności do ochrony informacji niejawnych o klauzuli "zastrzeżone" lub wyższej decyduje kierownik jednostki organizacyjnej, na rzecz którego będzie wykonywana umowa, poprzez wydanie pisemnego upoważnienia, po odbyciu przeszkolenia w zakresie ochrony informacji niejawnych.

3. W przypadku dostępu do informacji niejawnych o klauzuli "tajne" lub wyższej kierownik jednostki organizacyjnej o wydaniu upoważnienia, o którym mowa w ust. 2, informuje ABW albo SKW, które dokonuje oceny zdolności przedsiębiorcy do ochrony informacji niejawnych.

4. W zależności od wyniku oceny zdolności przedsiębiorcy do ochrony informacji niejawnych, ABW albo SKW może:

- 1) przekazać kierownikowi jednostki organizacyjnej zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych;
- 2) nakazać cofnięcie upoważnienia, o którym mowa w ust. 2.

5. W przypadku przedsiębiorcy wykonującego działalność jednoosobowo i osobiście zdolność do ochrony informacji niejawnych potwierdza poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli tajności "poufne" lub wyższej, a w razie jego braku, uzyskane pisemne upoważnienie kierownika jednostki organizacyjnej, na rzecz którego będzie wykonywana umowa, po odbyciu przeszkolenia w zakresie ochrony informacji niejawnych.

6. O wydaniu upoważnienia, o którym mowa w ust. 5, kierownik jednostki organizacyjnej informuje ABW albo SKW, które dokonuje oceny zasadności wydanego upoważnienia.

7. W zależności od wyniku oceny zdolności do ochrony informacji niejawnych przedsiębiorcy wykonującego działalność jednoosobowo i osobiście, ABW albo SKW może nakazać cofnięcie upoważnienia, o którym mowa w ust. 5.

## **Rozdział 11**

### **Zmiany w przepisach obowiązujących**

**Art. 82.** W ustawie z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2018 r. poz. 1459, 1669, 2182, 2245 oraz z 2019 r. poz. 55) w art. 176 ust. 1a otrzymuje brzmienie:

„1a. Osoby, o których mowa w ust. 1, które mają lub mogą mieć dostęp do informacji niejawnych, podlegają, na zasadach określonych w przepisach o ochronie informacji niejawnych, właściwemu postępowaniu sprawdzającemu. Postępowanie sprawdzające przeprowadza Służba Kontrwywiadu Wojskowego, na pisemny wniosek kierownika jednostki organizacyjnej przewidzianej do militaryzacji, do której nadano przydziały organizacyjno-mobilizacyjne.”.

**Art. 83.** W ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe:

1) w art. 105:

a) w ust. 1 w pkt 2 lit. k otrzymuje brzmienie:

„k) Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Policji, Żandarmerii Wojskowej, Straży Granicznej, Służby Więziennej, Służby Ochrony Państwa oraz ich posiadających pisemne upoważnienie funkcjonariuszy lub żołnierzy, w zakresie wskazanym w art. 26 ust. 1 pkt 3 oraz w art. 26 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412, 650, 1000, 1083 i 1669), w celu przeprowadzenia postępowań, o których mowa w przepisach tej ustawy;”;

b) po ust. 4 dodaje się ust. 4 w brzmieniu:

„4. Do instytucji, o których mowa w ust. 4, stosuje się odpowiednio ust. 1 oraz art. 110 pkt 6.”;

2) w art. 110 pkt 6 otrzymuje brzmienie:

„6) Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Policji, Żandarmerii Wojskowej, Straży Granicznej, Służby Więziennej, Służby Ochrony Państwa w związku z postępowaniami, o których mowa w przepisach o ochronie informacji niejawnych;”.

**Art. 84.** W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w art. 44 po pkt 5 dodaje się pkt 6 w brzmieniu:



„6) która nie pełniła służby zawodowej, nie pracowała i nie była współpracownikiem organów bezpieczeństwa państwa, wymienionych w art. 5 ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu.”.

**Art. 85.** W ustawie z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (Dz. U. z 2018 r. poz. 1516 i 1669) w art. 3 po pkt 5 dodaje się pkt 6 w brzmieniu:

„6) która nie pełniła służby zawodowej, nie pracowała i nie była współpracownikiem organów bezpieczeństwa państwa, wymienionych w art. 5 ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu.”.

**Art. 86.** W ustawie z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. z 2018 r. poz. 1542, 1669, 2245 i 2399) w art. 161 ust. 5 otrzymuje brzmienie:

„5. Informacje zawarte w oświadczeniu, o którym mowa w ust. 1 stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone”, określonej w przepisach ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, chyba że funkcjonariusz, który złożył oświadczenie wyraził pisemną zgodę na ich ujawnienie. Oświadczenie przechowuje się przez 6 lat.”

**Art. 87.** W ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w art. 105 w ust. 2 po pkt 2 dodaje się pkt 3 w brzmieniu:

„3) Agencji Bezpieczeństwa Wewnętrznego lub Służbie Kontrwywiadu Wojskowego, w związku z postępowaniami bezpieczeństwa przemysłowego, o których mowa w przepisach o ochronie informacji niejawnych”.

**Art. 88.** W ustawie z dnia 6 marca 2018 r. Prawo przedsiębiorców (Dz. U. poz. 646, z późn. zm.) w art. 65 dodaje się pkt 4 w brzmieniu:

„4) prowadzonej na podstawie przepisów o ochronie informacji niejawnych.”.

**Art. 89.** W ustawie z dnia 22 marca 2018 r. o komornikach sądowych (Dz. U. poz. 771, 1443, 1669 i 2244) w art. 27 po ust. 4 dodaje się ust. 5 w brzmieniu:

„5. Komornik jest obowiązany do przekazania Agencji Bezpieczeństwa Wewnętrznego, Służbie Kontrwywiadu Wojskowego, Agencji Wywiadu, Służbie Wywiadu Wojskowego, Centralnemu Biuru Antykorupcyjnemu, Policji, Żandarmerii Wojskowej, Straży Granicznej, Służbie Ochrony Państwa i Służbie Więziennej pozostających w jego dyspozycji informacji oraz kopii dokumentów, w zakresie niezbędnym do przeprowadzenia postępowań, o których mowa w przepisach o ochronie informacji niejawnych.”.

## **Rozdział 12**

### **Przepisy przejściowe i końcowe**

**Art. 90.** Wymogi, o których mowa w art. 14 ust. 2 i 3, stosuje się do kierowników jednostek organizacyjnych, którzy objęli swoje funkcję po wejściu w życie ustawy.

**Art. 91.** 1. Kierownik jednostki organizacyjnej, w której przed dniem wejścia w życie ustawy zatrudniono pełnomocnika ochrony lub zastępcę pełnomocnika ochrony, informuje o tym fakcie, w terminie do 3 miesięcy od tej daty, odpowiednio ABW lub SKW, z jednoczesnym przesłaniem

danych, o których mowa w art. 15 ust. 7, oraz odpowiednio wniosku o wydanie pozytywnej opinii, o której mowa w art. 15 ust. 2 pkt 5.

2. ABW lub SKW w terminie 12 miesięcy od dnia otrzymania informacji oraz odpowiednio wniosku, o których mowa w ust. 1, potwierdza spełnianie, przez pełnomocnika ochrony lub zastępcę pełnomocnika ochrony wymogów przewidzianych przez przepisy ustawy albo odmawia takiego potwierdzenia, oraz wydaje opinię, o której mowa w art. 15 ust. 2 pkt 5. Przepisy art. 15 ust. 8-13 stosuje się odpowiednio, z wyłączeniem terminu, o którym mowa w art. 15 ust. 10.

**Art. 92.** 1. Kierownik jednostki organizacyjnej podmiotu kluczowego dla zapewnienia bezpieczeństwa państwa z punktu widzenia ochrony informacji niejawnych, w którym przed dniem wejścia w życie niniejszej ustawy zatrudniono inspektora bezpieczeństwa informatycznego, administratora systemu, kierownika kancelarii tajnej lub jego zastępcę, informują o tym fakcie, w terminie do 3 miesięcy od tej daty, odpowiednio ABW lub SKW, z jednoczesnym przesłaniem wniosku, o którym mowa w art. 15 ust. 8.

2. ABW lub SKW w terminie 12 miesięcy od dnia otrzymania wniosku, o którym mowa w ust. 1, wydaje opinię, o której mowa w art. 15 ust. 2 pkt 5. Przepisy art. 15 ust. 8-13 stosuje się odpowiednio, z wyłączeniem terminu, o którym mowa w art. 15 ust. 10.

**Art. 93.** Kierownik jednostki organizacyjnej w której są przetwarzane informacje niejawne o klauzuli „poufne” lub „zastrzeżone”, informuje odpowiednio ABW lub SKW o wskazaniu komórki organizacyjnej odpowiedzialnej za właściwe rejestrowanie, przechowywanie, obieg i wydawanie uprawnionym osobom materiałów o klauzuli „poufne” lub „zastrzeżone”, w terminie do 3 miesięcy od dnia wejścia w życie ustawy, chyba że kierownik jednostki organizacyjnej poinformował ABW lub SKW o zorganizowaniu kancelarii tajnej.

**Art. 94.** Do postępowań sprawdzających, kontrolnych postępowań sprawdzających, postępowań bezpieczeństwa przemysłowego, czynności, o których mowa w art. 33 ust. 5 i art. 65 ust. 1 ustawy uchylanej w art. 100, a także do postępowań odwoławczych, wszczętych i niezakończonych przed dniem wejścia w życie ustawy stosuje się przepisy niniejszej ustawy. Złożenie ankiety lub kwestionariusza zgodnych z nowymi wzorami nie jest wymagane.

**Art. 95.** Wymóg, o którym mowa w art. 23 ust. 7, nie dotyczy osób zajmujących stanowiska wymienione w tym przepisie w dniu wejścia w życie ustawy.

**Art. 96.** 1. Poświadczenie bezpieczeństwa wydane na podstawie ustawy uchylanej w art. 100 zachowuje ważność przez okres wskazany w tym dokumencie.

2. Do poświadczenia bezpieczeństwa wydanego przez służby, o których mowa w art. 23 ust. 5 ustawy uchylanej w art. 100, przepisy art. 29 ust. 5 i 6 stosuje się odpowiednio.

3. Przepis art. 30 ust. 1 pkt 4 nie stanowi podstawy do:

- 1) odmowy wydania poświadczenia bezpieczeństwa w postępowaniu sprawdzającym wszczętym przed wejściem w życie niniejszej ustawy;
- 2) cofnięcia poświadczenia bezpieczeństwa w kontrolnym postępowaniu sprawdzającym wszczętym przed wejściem w życie niniejszej ustawy;
- 3) wszczęcia kontrolnego postępowania sprawdzającego i cofnięcia poświadczenia bezpieczeństwa w stosunku do osoby posiadającej poświadczenia bezpieczeństwa wydane na podstawie ustawy uchylanej w art. 100.

4. Świadczenie akredytacji bezpieczeństwa teleinformatycznego, a także certyfikat ochrony elektromagnetycznej, certyfikat ochrony kryptograficznej oraz certyfikat bezpieczeństwa teleinformatycznego wydany na podstawie ustawy uchylanej w art. 100 zachowuje ważność przez okres wskazany w tym świadectwie lub certyfikacie.

5. Świadczenie akredytacji bezpieczeństwa teleinformatycznego oraz certyfikat bezpieczeństwa teleinformatycznego, wydany na podstawie ustawy uchylanej w art. 100, są traktowane odpowiednio jak świadectwo akredytacji bezpieczeństwa informatycznego oraz certyfikat bezpieczeństwa informatycznego w rozumieniu przepisów ustawy.

6. Świadczenie bezpieczeństwa przemysłowego wydane na podstawie ustawy uchylanej w art. 100 zachowuje ważność przez okres wskazany w tym dokumencie.

7. Do świadectwa bezpieczeństwa przemysłowego wydanego na podstawie ustawy uchylanej w art. 100 przed dniem wejścia w życie ustawy stosuje się art. 55 ust. 3-5.

**Art. 97.** Wydane przez ABW lub SKW przed wejściem w życie ustawy zaświadczenie o odbyciu specjalistycznego szkolenia, o którym mowa w art. 52 ust. 4 ustawy uchylanej w art. 100, zachowuje ważność przez okres 5 lat od dnia wejścia w życie niniejszej ustawy.

**Art. 98.** 1. Upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone”, wydane przed wejściem w życie ustawy zachowuje ważność przez okres 3 miesiące od dnia wejścia w życie ustawy.

2. Kierownik jednostki organizacyjnych oraz przedsiębiorca wykonujący działalność jednoosobowo i osobiście, w terminie 3 miesiące od dnia wejścia w życie ustawy, występują do ABW lub SKW o wydanie upoważnienia do dostępu do informacji niejawnych o klauzuli „zastrzeżone”.

**Art. 99.** Dotychczasowe przepisy wykonawcze wydane na podstawie art. 13 ust. 4, art. 20 ust. 2 pkt 1 i 2, art. 47 ust. 1 i 3-5, art. 48 ust. 13, art. 49 ust. 9, art. 53, art. 61 ust. 2 oraz art. 68 ust. 1 ustawy uchylanej w art. 100 zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie upoważnień w brzmieniu określonym ustawą, jednak nie dłużej niż 12 miesięcy od wejścia w życie ustawy i mogą być zmieniane.

**Art. 100.** Traci moc ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412).

**Art. 101.** Ustawa wchodzi w życie z dniem 1 października 2019 r.