Projekt

U S T A W A

z dnia

o ochronie informacji niejawnych oraz o zmianie niektórych ustaw[1)]

Rozdział 1
Przepisy ogólne

Art. 1. 1. Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogło 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", w szczególności zasady:

1) organizowania ochrony informacji niejawnych;
2) klasyfikowania informacji niejawnych;
3) przetwarzania informacji niejawnych;
4) postępowania sprawdzającego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej odpowiednio „postępowaniem sprawdzającym" lub „kontrolnym postępowaniem sprawdzającym";
5) postępowania 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 teleinformatycznych;
8) stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

2. Przepisy ustawy mają zastosowanie do:

1) organów władzy publicznej, w szczególności:
   a) Sejmu i Senatu Rzeczypospolitej Polskiej,
   b) Prezydenta Rzeczypospolitej Polskiej,

c) organów administracji rządowej,
d) organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych,
e) sądów i trybunałów,
f) organów kontroli państwowej i ochrony prawa;

2) 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 lub nadzorowanych przez organy władzy publicznej;
6) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umowy lub wykonujących umowy związane z dostępem do informacji niejawnych albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

3. Przepisy ustawy o ochronie informacji niejawnych nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych, z zastrzeżeniem art. 5.

Art. 2. W rozumieniu ustawy:

1) jednostką organizacyjną – jest podmiot wymieniony w art. 1 ust. 2;
2) rękojmią zachowania tajemnicy – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
3) dokumentem – jest każda utrwalona informacja niejawna;
4) materiałem – jest dokument lub przedmiot albo dowolna jego część chronione jako informacja niejawna, a zwłaszcza urządzenie,

wyposażenie lub broń wyprodukowana albo będąca w trakcie produkcji, a także składnik użyty do ich wytworzenia;

5) 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;
6) systemem teleinformatycznym – jest system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.[2)]);
7) dokumentem szczególnych wymagań bezpieczeństwa – jest systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;
8) dokumentem procedur bezpiecznej eksploatacji systemu teleinformatycznego – jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp;
9) dokumentacją bezpieczeństwa systemu teleinformatycznego – jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;
10) akredytacją bezpieczeństwa teleinformatycznego – jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;
11) certyfikacją – jest proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych;
12) audytem bezpieczeństwa systemu teleinformatycznego – jest weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego;
13) przedsiębiorcą – jest przedsiębiorca w rozumieniu art. 4 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2007 r. Nr 155, poz. 1095, z późn. zm.[3)]) 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;

14) kierownikiem przedsiębiorcy – jest członek jednoosobowego zarządu lub innego jednoosobowego organu zarządzającego, a jeżeli organ jest wieloosobowy – cały organ albo członek lub członkowie tego organu wyznaczeni co najmniej uchwałą zarządu do pełnienia funkcji kierownika przedsiębiorcy, z wyłączeniem pełnomocników ustanowionych przez ten organ lub jednostkę; w przypadku spółki jawnej i spółki cywilnej kierownikiem przedsiębiorcy są wspólnicy prowadzący sprawy spółki, w przypadku spółki partnerskiej – wspólnicy prowadzący sprawy spółki albo zarząd, a w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej – komplementariusze prowadzący sprawy spółki; w przypadku osoby fizycznej prowadzącej działalność gospodarczą kierownikiem przedsiębiorcy jest ta osoba; za kierownika przedsiębiorcy uważa się również likwidatora, a także syndyka lub zarządcę ustanowionego w postępowaniu upadłościowym; kierownik przedsiębiorcy jest kierownikiem jednostki organizacyjnej w rozumieniu przepisów ustawy;
15) ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
16) szacowaniem ryzyka – jest całościowy proces analizy i oceny ryzyka;
17) zarządzaniem ryzykiem – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji z uwzględnieniem ryzyka;
18) zatrudnieniem – jest również odpowiednio powołanie, mianowanie lub wyznaczenie.

Art. 3. Do postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, w zakresie nieuregulowanym w ustawie, mają zastosowanie przepisy: art. 6 – 8, art. 12, art. 14 – 16, art. 24 § 1 pkt 1 – 6 i § 2 – 4, art. 26 § 1, art. 28 i 29, art. 30 § 1 – 3, art. 35 § 1, art. 39, art. 41 – 47, art. 50 i 55, art. 57 – 60, art. 61 § 3 i 4, art. 63 § 4, art. 64, 65 i 72, art. 75 § 1, art. 77 § 1, art. 97 § 1 pkt 4 i § 2, art. 98, 101, 103 i 104, art. 105 § 2, art. 107, art. 109 § 1, art. 112, art. 113 § 1, art. 125

§ 1, art. 156 – 158 oraz art. 217 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071, z późn. zm.[4)]).

Art. 4. 1. Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych.

2. 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.

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

Rozdział 2
Klasyfikowanie informacji niejawnych

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

1) zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
2) zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
3) zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
4) osłabi gotowość obronną Rzeczypospolitej Polskiej;
5) może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych

czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;

6) może zagrozić życiu lub zdrowiu żołnierzy, funkcjonariuszy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;

7) może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.[5)]), 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;

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 zagrozi bezpieczeństwu obywateli;

4) utrudni wykonywanie zadań przez służby lub instytucje odpowiedzialne za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
5) utrudni wykonywanie zadań przez służby lub instytucje odpowiedzialne za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz przez organy wymiaru sprawiedliwości;
6) zagrozi 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 szkodliwie wpłynąć 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.

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

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

2. Informacje niejawne podlegają ochronie w sposób określony w ustawie do czasu zniesienia lub zmiany klauzuli tajności na zasadach określonych w ust. 3, z zastrzeżeniem ust. 6. Osoba, o której mowa w ust. 1, może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.

3. Zniesienie lub zmiana klauzuli tajności jest możliwa wyłącznie w przypadku wyrażenia pisemnej zgody przez osobę, o której mowa w ust. 1, albo jej przełożonego w sytuacji ustania lub zmiany ustawowych przesłanek ochrony, o których mowa w art. 5, z zastrzeżeniem ust. 5.

4. Kierownicy jednostek organizacyjnych przeprowadzają nie rzadziej niż raz na pięć lat przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.

5. Pisemną zgodę na wykonanie czynności, o których mowa w ust. 3, w przypadku informacji niejawnych o klauzuli „ściśle tajne”, wyraża kierownik jednostki organizacyjnej, w której materiałowi została nadana klauzula tajności.

6. 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.

7. Uprawnienia w zakresie zniesienia lub zmiany klauzuli tajności materiału przechodzą, w przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji jednostki organizacyjnej, na jej następcę prawnego. W razie braku następcy prawnego uprawnienia w tym zakresie przechodzą na Agencję Bezpieczeństwa Wewnętrznego, zwaną dalej „ABW”, lub Służbę Kontrwywiadu Wojskowego, zwaną dalej „SKW”, z zastrzeżeniem art. 10 ust. 2 i 3.

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

9. 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.

10. W rozporządzeniu, o którym mowa w ust. 9, Prezes Rady Ministrów uwzględni potrzebę oznaczania materiałów w sposób zapewniający ich odróżnienie od materiałów jawnych, mając na uwadze rodzaje klauzul tajności i materiałów oraz sposób odrębnego oznaczania części materiału, o którym mowa w ust. 8.

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

1) dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji państwowych, 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 państwowym uprawnionym do ich wykonywania na podstawie ustawy;

3) informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

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, podlegających obowiązkowi przekazania 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 2007 r. Nr 63, poz. 424, z późn. zm.[6)]),

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 2007 r. Nr 63, poz. 425, z późn. zm.[7)])

– chyba że dostęp do określonych dokumentów został zastrzeżony w trybie art. 39 ustawy wymienionej w pkt 1.

Art. 8. Informacje niejawne, którym przyznano określoną klauzulę tajności:

1) mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności;

2) muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do przyznanej klauzuli tajności;

3) muszą być chronione, odpowiednio do przyznanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

Art. 9. 1. Odbiorca materiału, w przypadku stwierdzenia wyraźnego zawyżenia lub zaniżenia klauzuli tajności, zwraca się do osoby, która ją nadała, albo przełożonego tej osoby z wnioskiem o dokonanie stosownej zmiany.

2. W przypadku odmowy dokonania zmiany lub nieudzielenia odpowiedzi w ciągu 30 dni od daty doręczenia wniosku, o którym mowa w ust. 1, odbiorca może zwrócić się odpowiednio do ABW lub SKW o rozstrzygnięcie sporu. Rozstrzygnięcie to jest ostateczne.

3. Jeżeli stroną sporu, o którym mowa w ust. 2, jest ABW lub SKW, to spór rozstrzyga Prezes Rady Ministrów.

4. Prezes Rady Ministrów może upoważnić Szefa Kancelarii Prezesa Rady Ministrów, sekretarza stanu albo podsekretarza stanu w Kancelarii Prezesa Rady Ministrów do wykonywania czynności, o których mowa w ust. 3.

Rozdział 3
Organizacja ochrony informacji niejawnych

Art. 10. 1. ABW i SKW, nadzorując funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości określonej w ust. 2 i 3:

1) prowadzą kontrole ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;
2) realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;
3) prowadzą postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego;
4) zapewniają ochronę informacji niejawnych wymienianych przez Rzeczpospolitą Polską z innymi państwami lub organizacjami międzynarodowymi;
5) prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych.

2. SKW realizuje zadania w odniesieniu do:

1) Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

2) ataszatów obrony w placówkach zagranicznych;
3) żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione w pkt 1 i 2.

3. ABW realizuje zadania w odniesieniu do jednostek organizacyjnych i osób będących podmiotami ustawy, niewymienionych w ust. 2.

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 i wydawania dokumentów upoważniających do dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego, zwanej dalej „NATO", Unii Europejskiej lub innych organizacji międzynarodowych, zwanych dalej „informacjami niejawnymi międzynarodowymi".

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

4. 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:

1) wglądu w dokumenty związane z ochroną informacji niejawnych międzynarodowych;
2) wstępu do obiektów i pomieszczeń przeznaczonych do przetwarzania informacji niejawnych międzynarodowych;
3) dostępu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych;
4) uzyskiwania wyjaśnień i informacji dotyczących ochrony informacji niejawnych międzynarodowych.

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

6. 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.

7. W rozporządzeniu, o którym mowa w ust. 6, Prezes Rady Ministrów uwzględni rolę Szefa ABW w nadzorze nad systemem ochrony informacji niejawnych

wymienianych z 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 w dokumenty związane z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej;
3) żądania udostępnienia do kontroli systemów teleinformatycznych służących do przetwarzania tych informacji;
4) przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji;
5) żądania od kierowników i pracowników kontrolowanych jednostek organizacyjnych udzielania ustnych i pisemnych wyjaśnień;
6) zasięgania, w związku z przeprowadzaną kontrolą, informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek;
7) powoływania oraz korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych;
8) uczestniczenia w posiedzeniach kierownictwa, organów zarządzających lub nadzorczych, a także organów opiniodawczo-doradczych w sprawach dotyczących problematyki ochrony tych informacji w kontrolowanej jednostce organizacyjnej.

2. Jeżeli w czasie wykonywania kontroli, o której mowa w ust. 1, zostanie w znacznym stopniu uprawdopodobnione podejrzenie możliwości przetwarzania informacji niejawnych w systemach teleinformatycznych nieposiadających akredytacji bezpieczeństwa teleinformatycznego, 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.

3. Postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego, z wyłączeniem postępowań, o których mowa w art. 23 ust. 5, podlegają kontroli w zakresie prawidłowości ich realizacji. Kontrolę tę prowadzą:

1) Prezes Rady Ministrów – w odniesieniu do postępowań zrealizowanych przez ABW lub SKW;
2) odpowiednio ABW lub SKW – w odniesieniu do postępowań zrealizowanych przez pełnomocników ochrony.

4. Do czynności, o których mowa w ust. 1 i 3, dokonywanych przez ABW lub SKW albo przez Prezesa Rady Ministrów mają zastosowanie odpowiednio przepisy art. 30 – 39 ust. 2 – 4, art. 40 ust. 2 – 4, art. 41 – 49 ust. 2 – 6, art. 50 ust. 1 – 3, art. 64 ust. 1 i art. 98 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.[8)]), z tym że przewidziane w tej ustawie uprawnienia i obowiązki:

1) Najwyższej Izby Kontroli – wykonują odpowiednio ABW i SKW albo Kancelaria Prezesa Rady Ministrów;
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 upoważniony pracownik Kancelarii Prezesa Rady Ministrów.

5. Czynności, o których mowa w ust. 1 pkt 1 – 5 i 8, dokonywane przez ABW w stosunku do Kancelarii Sejmu Rzeczypospolitej Polskiej, Kancelarii Senatu Rzeczypospolitej Polskiej oraz Kancelarii Prezydenta Rzeczypospolitej Polskiej są wykonywane w uzgodnieniu odpowiednio z Marszałkiem Sejmu Rzeczypospolitej Polskiej, Marszałkiem Senatu Rzeczypospolitej Polskiej oraz Szefem Kancelarii Prezydenta Rzeczypospolitej Polskiej. Uzgodnienia dokonuje Prezes Rady Ministrów, a w przypadku braku uzgodnienia czynność nie może być wykonana.

6. Prezes Rady Ministrów określi, w drodze rozporządzenia:

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 – 5 i 8, w stosunku do Kancelarii Sejmu Rzeczypospolitej Polskiej, Kancelarii Senatu Rzeczypospolitej Polskiej 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, wystąpienia pokontrolnego i informacji o wynikach kontroli.

7. W rozporządzeniu, o którym mowa w ust. 6, Prezes Rady Ministrów uwzględni, aby zakres i sposób prowadzenia kontroli umożliwiał sprawne i obiektywne ustalenie stanu faktycznego zabezpieczenia informacji niejawnych w kontrolowanej jednostce organizacyjnej oraz jego rzetelne udokumentowanie.

Art. 13. 1. Kierownicy jednostek organizacyjnych współdziałają ze służbami i instytucjami uprawnionymi do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, w szczególności udostępniają funkcjonariuszom, pracownikom albo żołnierzom tych służb i instytucji, po przedstawieniu przez nich pisemnego upoważnienia, pozostające w ich dyspozycji informacje i dokumenty niezbędne do realizacji czynności w ramach tych postępowań.

2. Służby i instytucje uprawnione do prowadzenia poszerzonych postępowań sprawdzających, w zakresie koniecznym do wykonywania swoich zadań, w celu ochrony informacji niejawnych mogą zwracać się do innych instytucji, służb i organów o udzielenie niezbędnej pomocy przy wykonywaniu czynności w ramach prowadzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego.

3. Szefowie służb i instytucji określonych w art. 23 ust. 2 i 5 udostępniają upoważnionym funkcjonariuszom, pracownikom albo żołnierzom służb i instytucji, o których mowa w ust. 1, na potrzeby prowadzonych przez te służby i instytucje postępowań sprawdzających lub kontrolnych postępowań sprawdzających, pozostające w ich dyspozycji informacje i dokumenty wyłącznie w przypadku, gdy w ich opinii osoba objęta postępowaniem sprawdzającym lub kontrolnym postępowaniem sprawdzającym nie daje

rękojmi zachowania tajemnicy; w przeciwnym przypadku informują, że nie posiadają informacji i dokumentów świadczących, że osoba ta nie daje tej rękojmi.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia:

1) szczegółowy zakres, warunki, sposób i tryb przekazywania przez kierowników jednostek organizacyjnych służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego informacji, o których mowa w ust. 1 i 3, oraz udostępniania im dokumentów niezbędnych dla celów tych postępowań;

2) szczegółowy zakres, warunki, sposób i tryb udzielania przez Centralne Biuro Antykorupcyjne, zwane dalej „CBA", Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy kontroli skarbowej niezbędnej pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego przy wykonywaniu czynności w ramach tych postępowań.

5. W rozporządzeniu, o którym mowa w ust. 4, Prezes Rady Ministrów uwzględni zakres danych, jakiego powinny zawierać wnioski o udzielenie informacji lub pomocy, a także możliwość wykorzystywania systemów teleinformatycznych 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. Kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony", który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

3. Pełnomocnikiem ochrony może być osoba, która posiada:

1) obywatelstwo polskie;

2) wykształcenie wyższe;

3) odpowiednie poświadczenie bezpieczeństwa wydane przez ABW lub SKW, a także przez były Urząd Ochrony Państwa lub byłe Wojskowe Służby Informacyjne;
4) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych przeprowadzonym przez ABW lub SKW, a także przez byłe Wojskowe Służby Informacyjne.

4. Kierownik jednostki organizacyjnej może zatrudnić zastępcę lub zastępców pełnomocnika ochrony, z zastrzeżeniem spełnienia przez te osoby warunków, o których mowa w ust. 3.

5. Szczegółowy zakres czynności zastępcy pełnomocnika ochrony określa kierownik jednostki organizacyjnej.

Art. 15. 1. Do zadań pełnomocnika ochrony należy:
1) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;
2) zapewnienie ochrony systemów teleinformatycznych, 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, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji;
6) prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
7) prowadzenie postępowań sprawdzających;
8) prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji

niejawnych, oraz osób, którym odmówiono wydania lub cofnięto poświadczenie bezpieczeństwa, obejmującego wyłącznie:

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 procedurę, datę jego wydania oraz numer;

9) przekazywanie odpowiednio ABW lub SKW do ewidencji, o których mowa w art. 73 ust. 1, danych, o których mowa w art. 73 ust. 2, osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, na podstawie wykazu, o którym mowa w pkt 8.

2. 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.

3. Zadanie, o którym mowa w ust. 1 pkt 9, nie dotyczy pełnomocników ochrony w służbach i instytucjach uprawnionych do realizacji poszerzonych postępowań sprawdzających, o których mowa w art. 23 ust. 2 i 5.

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

Art. 16. Pracownikiem pionu ochrony w jednostce organizacyjnej może być osoba, która posiada:

1) obywatelstwo polskie, z wyjątkiem pracowników pionu ochrony zatrudnionych u przedsiębiorców;

2) odpowiednie poświadczenie bezpieczeństwa lub upoważnienie, o którym mowa w art. 21 ust. 4 pkt 1;

3) zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.

Art. 17. 1. W przypadku 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 informuje niezwłocznie również odpowiednio ABW lub SKW.

Art. 18. 1. Minister Obrony Narodowej określi, w drodze rozporządzenia:

1) szczegółowe zadania pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych jemu podległych i 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.

2. W rozporządzeniu, o którym mowa w ust. 1, Minister Obrony Narodowej uwzględni 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, o których mowa w art. 1 ust. 2 pkt 2.

Rozdział 4
Szkolenia w zakresie ochrony informacji niejawnych

Art. 19. 1. Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania z:

1) przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych;
2) zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka;
3) sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.

2. Szkolenie, o którym mowa w ust. 1:

1) przeprowadzają odpowiednio ABW lub SKW – wobec pełnomocników ochrony i ich zastępców oraz osób przewidzianych na te stanowiska, przedsiębiorców wykonujących działalność jednoosobowo, a także wobec kierowników przedsiębiorców, u których nie zatrudniono pełnomocników ochrony;
2) przeprowadzają odpowiednio ABW lub SKW – wspólnie z pełnomocnikiem ochrony wobec kierownika jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „ściśle tajne” lub „tajne”;

3) organizuje pełnomocnik ochrony – w stosunku do pozostałych osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w jednostce organizacyjnej;

4) przeprowadza ABW – wobec posłów i senatorów.

3. Szkolenie 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.

4. Koszty szkolenia przeprowadzonego przez ABW lub SKW, z wyłączeniem szkolenia, o którym mowa w ust. 2 pkt 4, oraz z zastrzeżeniem ust. 5, pokrywa jednostka organizacyjna, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje czynności zlecone.

5. Jednostki organizacyjne, o których mowa w art. 1 ust. 2 pkt 2 oraz w art. 23 ust. 5 pkt 4, nie pokrywają kosztów szkoleń przeprowadzonych przez ABW lub SKW.

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

Art. 20. 1. Szkolenie, o którym mowa w art. 19 ust. 1, kończy się wydaniem zaświadczenia. Odbierając zaświadczenie, osoba przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.

2. Prezes Rady Ministrów określi, w drodze rozporządzenia:

1) wzory zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych;

2) sposób rozliczania kosztów, o których mowa w art. 19 ust. 4.

3. W rozporządzeniu, o którym mowa w ust. 2, Prezes Rady Ministrów uwzględni odrębności wynikające z wydawania zaświadczeń przez ABW i SKW oraz pełnomocników ochrony oraz sposób ustalania kosztów na potrzeby ich rozliczania w ten sposób, że ich wysokość nie może przekroczyć 25 % przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłoszonego przez Prezesa Głównego Urzędu Statystycznego na

podstawie art. 7 ust. 1 ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich (Dz. U. Nr 108, poz. 685, z późn. zm.[9)]).

Rozdział 5
Bezpieczeństwo osobowe

Art. 21. 1. Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej może nastąpić, z zastrzeżeniem art. 34, po:

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

2. 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", z zastrzeżeniem ust. 3.

3. Wymogu określonego w ust. 2 nie stosuje się do osób:

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

4. Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić po:

1) pisemnym upoważnieniu przez kierownika jednostki organizacyjnej, jeżeli dana osoba nie posiada poświadczenia bezpieczeństwa;

2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.

Art. 22. 1. W zależności od stanowiska lub wykonywania czynności zleconych, o które ubiega się osoba, zwana dalej „osobą sprawdzaną", przeprowadza się:

1) zwykłe postępowanie sprawdzające – przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „poufne", z zastrzeżeniem pkt 2 lit. b – d;
2) poszerzone postępowanie sprawdzające:
   a) przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne",
   b) wobec pełnomocników ochrony, zastępców pełnomocników ochrony oraz kandydatów na te stanowiska,
   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 organizacji międzynarodowych lub o dostęp, który ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską.

2. W odniesieniu do osób wskazanych w ust. 1 pkt 2 lit. b – d wydaje się poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o takiej klauzuli, jaka została wskazana we wniosku lub poleceniu.

Art. 23. 1. Pełnomocnik ochrony przeprowadza zwykłe postępowanie sprawdzające na pisemne polecenie kierownika jednostki organizacyjnej.

2. ABW lub SKW przeprowadzają poszerzone postępowania sprawdzające na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej na podstawie odrębnych przepisów do obsady stanowiska lub zlecenia prac, a także wobec własnych pracowników, funkcjonariuszy, żołnierzy oraz osób ubiegających się o przyjęcie do służby lub pracy, a także wobec osób wykonujących czynności zlecone lub ubiegających się o wykonywanie tych czynności.

3. ABW przeprowadza poszerzone postępowania sprawdzające wobec:

1) Szefa SKW, Szefa Agencji Wywiadu, zwanej dalej „AW", Szefa CBA, Szefa Biura Ochrony Rządu, Komendanta Głównego Policji,

Dyrektora Generalnego Służby Więziennej, Komendanta Głównego Straży Granicznej oraz osób przewidzianych na te stanowiska;

2) pełnomocników ochrony, zastępców pełnomocników ochrony oraz osób przewidzianych na te stanowiska w SKW, AW, CBA, Biurze Ochrony Rządu, Policji, Służbie Więziennej oraz Straży Granicznej.

4. SKW przeprowadza poszerzone postępowania sprawdzające wobec:

1) Szefa ABW, Szefa Służby Wywiadu Wojskowego, zwanej dalej „SWW", Komendanta Głównego Żandarmerii Wojskowej oraz osób przewidzianych na te stanowiska;

2) pełnomocników ochrony, zastępców pełnomocników ochrony oraz osób przewidzianych na te stanowiska w ABW, SWW oraz Żandarmerii Wojskowej.

5. Postępowania sprawdzające oraz kontrolne postępowania sprawdzające wobec własnych pracowników, funkcjonariuszy, żołnierzy oraz osób ubiegających się o przyjęcie do służby lub pracy, a także wobec osób wykonujących lub ubiegających się o wykonywanie czynności zleconych, przeprowadzają samodzielnie, z zastrzeżeniem ust. 3 i 4:

1) AW;
2) CBA;
3) Biuro Ochrony Rządu;
4) Policja;
5) Służba Więzienna;
6) SWW;
7) Straż Graniczna;
8) Żandarmeria Wojskowa.

6. W zakresie postępowań sprawdzających oraz kontrolnych postępowań sprawdzających przeprowadzanych przez służby i instytucje, o których mowa w ust. 5, przysługują tym służbom i instytucjom uprawnienia ABW oraz SKW.

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

2. W toku postępowania sprawdzającego ustala się, czy istnieją wątpliwości dotyczące:

1) uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko Rzeczypospolitej Polskiej;
2) zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu;
3) przestrzegania porządku konstytucyjnego Rzeczypospolitej Polskiej, a przede wszystkim, czy osoba sprawdzana uczestniczyła lub uczestniczy w działalności partii politycznych lub innych organizacji, o których mowa w art. 13 Konstytucji Rzeczypospolitej Polskiej, albo współpracowała lub współpracuje z takimi partiami lub organizacjami;
4) ukrywania lub niezgodnego z prawdą podawania w ankiecie bezpieczeństwa osobowego lub postępowaniu sprawdzającym przez osobę sprawdzaną informacji mających znaczenie dla ochrony informacji niejawnych;
5) występowania związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji;
6) niewłaściwego postępowania z informacjami niejawnymi, jeżeli:
   a) doprowadziło to bezpośrednio do ujawnienia tych informacji osobom nieuprawnionym,
   b) było wynikiem celowego działania,
   c) stwarzało realne zagrożenie ich nieuprawnionego ujawnienia i nie miało charakteru incydentalnego,
   d) dopuściła się go osoba szczególnie zobowiązana na podstawie ustawy do ochrony informacji niejawnych: pełnomocnik ochrony, jego zastępca lub kierownik kancelarii tajnej.

3. W toku poszerzonego postępowania sprawdzającego ustala się ponadto, czy istnieją wątpliwości dotyczące:

1) poziomu życia osoby sprawdzanej wyraźnie przewyższającego uzyskiwane przez nią dochody;
2) informacji o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej

do zajmowania stanowiska albo wykonywania prac związanych z dostępem do informacji niejawnych;

3) uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych.

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 do wykazania najwyższej staranności w toku prowadzonego postępowania sprawdzającego co do jego zgodności z przepisami ustawy.

6. Wszystkie czynności przeprowadzone w toku postępowań sprawdzających muszą być rzetelnie udokumentowane i powinny być zakończone przed upływem 3 miesięcy od dnia:

1) złożenia do pełnomocnika ochrony wypełnionej ankiety bezpieczeństwa osobowego, zwanej dalej „ankietą", lub

2) złożenia wniosku o przeprowadzenie postępowania sprawdzającego wraz z wypełnioną ankietą.

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. Ustawa zezwala – w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy – na zbieranie i przetwarzanie informacji o osobach trzecich, określonych w ankiecie bezpieczeństwa osobowego, bez wiedzy i zgody tych osób. Informacje o osobach trzecich mogą być zbierane i przetwarzane wyłącznie w zakresie określonym w ust. 2.

10. Ankieta bezpieczeństwa osobowego, po wypełnieniu, stanowi tajemnicę prawnie chronioną i podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „poufne" w przypadku poszerzonego postępowania sprawdzającego lub „zastrzeżone" w przypadku zwykłego postępowania sprawdzającego. Wzór ankiety wraz z instrukcją jej wypełnienia stanowi załącznik do ustawy.

Art. 25. 1. Zwykłe postępowanie sprawdzające obejmuje:

1) sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, w szczególności w Krajowym Rejestrze Karnym, danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie, a także sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy;
2) sprawdzenie w ewidencjach i kartotekach niedostępnych powszechnie danych zawartych w ankiecie oraz innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

2. Sprawdzenie, o którym mowa w ust. 1 pkt 2, jest prowadzone na pisemny wniosek pełnomocnika ochrony przez ABW lub SKW.

3. W toku sprawdzenia, o którym mowa w ust. 1 pkt 2, ABW lub SKW ma prawo przeprowadzić rozmowę z osobą sprawdzaną w celu usunięcia nieścisłości lub sprzeczności zawartych w uzyskanych informacjach.

4. ABW lub SKW przekazuje pełnomocnikowi ochrony pisemną informację o wynikach czynności, o których mowa w ust. 1 pkt 2 oraz w ust. 3.

5. Jeżeli jest to konieczne w wyniku uzyskanych informacji, zwykłe postępowanie sprawdzające obejmuje ponadto rozmowę z osobą 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.

7. Organ prowadzący zwykłe postępowanie sprawdzające odstępuje od przeprowadzenia czynności, o której mowa w ust. 6, jeżeli:

1) jej przeprowadzenie wiązałoby się z ujawnieniem informacji niejawnych;

2) postępowanie sprawdzające doprowadziło do niebudzącego wątpliwości ustalenia, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy.

Art. 26. 1. Poszerzone postępowanie sprawdzające obejmuje czynności, o których mowa w art. 25 ust. 1, a ponadto, jeżeli jest to konieczne w wyniku uzyskanych informacji, postępowanie to obejmuje:

1) rozmowę z przełożonymi osoby sprawdzanej oraz z innymi osobami;
2) przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej;
3) sprawdzenie stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, w szczególności wobec Skarbu Państwa.

2. Do czynności, o której mowa w ust. 1 pkt 2, przepisy ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego i wydane na jej podstawie przepisy dotyczące wywiadu środowiskowego stosuje się odpowiednio.

3. Czynności, o których mowa w ust. 1 pkt 3, są realizowane zgodnie z art. 105 ust. 1 pkt 2 lit. k ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665, z późn. zm.[10)]). Przepisy art. 82 § 1 i 2 oraz art. 182 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2005 r. Nr 8, poz. 60, z późn. zm.[11)]) oraz art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65, z późn. zm.[12)]) stosuje się odpowiednio.

4. Do poszerzonego postępowania sprawdzającego przepisy art. 25 ust. 6 – 8 stosuje się odpowiednio.

5. W przypadku osób ubiegających się o uzyskanie dostępu do informacji o klauzuli „ściśle tajne” poszerzone postępowanie sprawdzające obejmuje także, jeżeli jest to konieczne 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.

6. W celu dokonania ustaleń, o których mowa w art. 24 ust. 3 pkt 2 i 3, organ prowadzący poszerzone postępowanie sprawdzające może zobowiązać osobę sprawdzaną do poddania się specjalistycznym badaniom oraz udostępnienia wyników tych badań. Lekarzowi przeprowadzającemu to badanie udostępnia się dokumentację medyczną

osoby sprawdzanej w zakresie dotyczącym zdiagnozowania wątpliwości, o których mowa w art. 24 ust. 3 pkt 2 i 3.

Art. 27. 1. Postępowanie sprawdzające może zostać zawieszone 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;
4) gdy przeprowadzenie skutecznego postępowania sprawdzającego nie jest możliwe z innych przyczyn niezależnych od organu je prowadzącego.

2. Zawieszone 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. O zawieszeniu postępowania sprawdzającego oraz o jego podjęciu organ prowadzący postępowanie sprawdzające zawiadamia wnioskodawcę, pełnomocnika ochrony i osobę sprawdzaną.

4. Do zażalenia na postanowienie w sprawie zawieszenia postępowania sprawdzającego przepisy art. 35, 37 i 38 stosuje się odpowiednio.

Art. 28. Postępowanie sprawdzające kończy się:

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

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

2. Poświadczenie bezpieczeństwa powinno zawierać:

1) numer poświadczenia;
2) podstawę prawną;
3) wskazanie wnioskodawcy postępowania sprawdzającego;
4) określenie organu, który przeprowadził postępowanie sprawdzające;
5) datę i miejsce wystawienia;
6) imię, nazwisko i datę urodzenia osoby sprawdzanej;
7) rodzaj przeprowadzonego postępowania sprawdzającego ze wskazaniem klauzuli tajności informacji niejawnych, do których osoba sprawdzana może mieć dostęp;
8) stwierdzenie, że osoba sprawdzana daje rękojmię zachowania tajemnicy;
9) termin ważności;
10) imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające.

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 poświadczeń bezpieczeństwa organizacji międzynarodowych.

5. Poświadczenia bezpieczeństwa wydane w wyniku przeprowadzenia postępowań sprawdzających, o których mowa w art. 23 ust. 5, zachowują ważność wyłącznie w okresie pracy lub służby w organie, który przeprowadził postępowanie sprawdzające.

6. Prezes Rady Ministrów określi, w drodze rozporządzenia, z uwzględnieniem ust. 2 pkt 1 – 10, wzory:

1) poświadczenia bezpieczeństwa;
2) poświadczeń bezpieczeństwa upoważniających do dostępu do informacji niejawnych organizacji międzynarodowych.

Art. 30. 1. Organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa, jeżeli nie zostaną usunięte wątpliwości, o których mowa w art. 24 ust. 2, a także jeżeli w trakcie poszerzonego postępowania sprawdzającego nie zostaną usunięte wątpliwości, o których mowa w art. 24 ust. 3.

2. Organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa, jeżeli osoba sprawdzana została skazana prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, a fakt skazania wywołuje wątpliwości, o których mowa w art. 24 ust. 2 i 3.

3. Decyzja o odmowie wydania poświadczenia bezpieczeństwa powinna zawierać:

1) podstawę prawną oraz uzasadnienie faktyczne i prawne;
2) wskazanie wnioskodawcy postępowania sprawdzającego;
3) określenie organu, który przeprowadził postępowanie sprawdzające;
4) datę i miejsce wystawienia;
5) imię, nazwisko i datę urodzenia osoby sprawdzanej;
6) wskazanie rodzaju przeprowadzonego postępowania sprawdzającego ze wskazaniem klauzuli informacji niejawnych, do których osoba sprawdzana miała mieć dostęp;
7) stwierdzenie, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy;
8) imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające;
9) pouczenie o dopuszczalności i terminie wniesienia odwołania odpowiednio do Prezesa Rady Ministrów albo Szefa ABW lub Szefa SKW.

4. Można odstąpić od uzasadnienia faktycznego decyzji lub je ograniczyć w zakresie, w jakim wiązałoby się to z udostępnieniem osobie sprawdzanej informacji niejawnych.

5. Po zakończeniu postępowania sprawdzającego z wynikiem negatywnym organ prowadzący postępowanie wydaje decyzję o odmowie wydania poświadczenia bezpieczeństwa i doręcza ją osobie sprawdzanej, zawiadamiając o tym wnioskodawcę oraz pełnomocnika ochrony.

6. Osoba uprawniona do obsady stanowiska jest obowiązana, niezwłocznie po otrzymaniu zawiadomienia o odmowie wydania poświadczenia bezpieczeństwa w zakresie dostępu do informacji niejawnych, uniemożliwić dostęp do informacji niejawnych osobie, której odmowa dotyczy, z zastrzeżeniem art. 21 ust. 4.

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

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

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

1) śmierci osoby sprawdzanej;
2) rezygnacji osoby sprawdzanej z ubiegania się albo zajmowania stanowiska lub wykonywania prac związanych z dostępem do informacji niejawnych;
3) odstąpienia przez kierownika jednostki organizacyjnej od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac związanych z dostępem do informacji niejawnych;
4) gdy postępowanie z innej przyczyny stało się bezprzedmiotowe.

2. O umorzeniu postępowania sprawdzającego organ je prowadzący zawiadamia wnioskodawcę, pełnomocnika ochrony oraz, w przypadkach, o których mowa w ust. 1 pkt 2 – 4, osobę sprawdzaną.

Art. 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, 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. Jeżeli wobec osoby posiadającej ważne poświadczenie bezpieczeństwa, wydane przez ABW, SKW, AW lub SWW, zostanie skierowany wniosek o przeprowadzenie postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa organizacji międzynarodowej, wypełnienie ankiety bezpieczeństwa osobowego nie jest wymagane, a poświadczenie bezpieczeństwa organizacji międzynarodowej jest wydawane jedynie na okres ważności posiadanego przez tę osobę poświadczenia bezpieczeństwa.

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

2. Postępowanie, o którym mowa w ust. 1, przeprowadza organ właściwy do przeprowadzenia kolejnego postępowania sprawdzającego, z zastrzeżeniem ust. 3.

3. W przypadkach uzasadnionych względami bezpieczeństwa państwa kontrolne postępowanie sprawdzające może zostać przeprowadzone przez ABW lub SKW.

4. Przepisu ust. 3 nie stosuje się do kontrolnych postępowań sprawdzających prowadzonych wobec osób, które posiadają poświadczenie bezpieczeństwa wydane w wyniku przeprowadzenia postępowania sprawdzającego, o którym mowa w art. 23 ust. 5.

5. W celu weryfikacji informacji, o których mowa w ust. 1, właściwy organ może przeprowadzić niezbędne czynności sprawdzające. Pełnomocnik ochrony może przeprowadzić w tym trybie czynności, o których mowa w art. 25 ust. 1 pkt 1, a służby i instytucje uprawnione do prowadzenia poszerzonych postępowań sprawdzających także czynności, o których mowa w art. 25 ust. 1 pkt 2. 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.

6. O wszczęciu kontrolnego postępowania sprawdzającego zawiadamia się:

1) kierownika jednostki organizacyjnej lub osobę uprawnioną do obsady stanowiska;
2) pełnomocnika ochrony w jednostce organizacyjnej;
3) osobę sprawdzaną.

7. Po otrzymaniu zawiadomienia, o którym mowa w ust. 6, kierownik jednostki organizacyjnej lub osoba uprawniona do obsady stanowiska uniemożliwia osobie sprawdzanej dostęp do informacji niejawnych.

8. 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 art. 31 ust. 2.

9. Wszystkie czynności przeprowadzone w toku kontrolnych postępowań sprawdzających muszą być rzetelnie udokumentowane i powinny być zakończone przed upływem 6 miesięcy od dnia wszczęcia postępowania.

10. W szczególnie uzasadnionych przypadkach niezakończenia kontrolnego postępowania sprawdzającego w terminie, o którym mowa w ust. 9, organ prowadzący postępowanie jednorazowo przedłuża je o kolejne 6 miesięcy, zawiadamiając o tym osoby, o których mowa w ust. 6.

11. Kontrolne postępowanie sprawdzające kończy się:

1) decyzją o cofnięciu poświadczenia bezpieczeństwa;
2) poinformowaniem osób wymienionych w ust. 6 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 gdy postępowanie to nie zostanie zakończone przed upływem 12 miesięcy od dnia jego wszczęcia.

12. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór decyzji o cofnięciu poświadczenia bezpieczeństwa, z uwzględnieniem składników decyzji, o których mowa w art. 30 ust. 3 pkt 1 i 3 – 9.

Art. 34. 1. Nie przeprowadza się postępowania sprawdzającego, jeżeli osoba, której ma ono dotyczyć, przedstawi poświadczenie bezpieczeństwa odpowiednie do wymaganej klauzuli tajności, z wyjątkiem poświadczeń bezpieczeństwa wydanych w wyniku przeprowadzenia postępowań sprawdzających, o których mowa w art. 23 ust. 5.

2. O zatrudnieniu na stanowisku, z którym może łączyć się dostęp do informacji niejawnych osoby, o której mowa w ust. 1, przedstawiającej odpowiednie poświadczenie bezpieczeństwa, kierownik jednostki organizacyjnej informuje w terminie 7 dni organ, który wydał poświadczenie bezpieczeństwa, oraz odpowiednio ABW lub SKW.

3. Od obowiązku określonego w ust. 2 są zwolnieni kierownicy jednostek organizacyjnych podmiotów, o których mowa w art. 23 ust. 5.

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

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

1) w szczególnie uzasadnionych przypadkach, z zastrzeżeniem art. 4 ust. 2, 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.

6. W stanach nadzwyczajnych Prezydent Rzeczypospolitej Polskiej lub Prezes Rady Ministrów, każdy w swoim zakresie, może wyrazić zgodę na odstąpienie od przeprowadzenia postępowania sprawdzającego.

7. W przypadkach, o których mowa w ust. 5 i 6, kopię zgody na udostępnienie informacji niejawnych lub odstąpienie od przeprowadzenia postępowania sprawdzającego przekazuje się odpowiednio do ABW lub SKW.

8. Obowiązek, o którym mowa w ust. 7, nie dotyczy służb i instytucji uprawnionych do realizacji poszerzonych postępowań sprawdzających, o których mowa w art. 23 ust. 5.

9. Zgodę na udostępnienie 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, pełni służbę lub wykonuje czynności zlecone.

10. Postępowania sprawdzającego nie przeprowadza się, z zastrzeżeniem ust. 11 – 13, wobec:

1) Prezydenta Rzeczypospolitej Polskiej oraz osoby wybranej na ten urząd;
2) Marszałka Sejmu Rzeczypospolitej Polskiej;
3) Marszałka Senatu Rzeczypospolitej Polskiej;
4) Prezesa Rady Ministrów;
5) członka Rady Ministrów;
6) Prezesa Narodowego Banku Polskiego;
7) Prezesa Najwyższej Izby Kontroli;
8) Rzecznika Praw Obywatelskich;
9) Generalnego Inspektora Ochrony Danych Osobowych;
10) członka Rady Polityki Pieniężnej;
11) członka Krajowej Rady Radiofonii i Telewizji;
12) Prezesa Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu;
13) Szefa Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu i Prezesa Rady Ministrów;
14) posła i senatora;
15) sędziego sądu powszechnego i sądu wojskowego, Sądu Najwyższego, sądów administracyjnych i Naczelnego Sądu Administracyjnego, a także Trybunału Stanu i Trybunału Konstytucyjnego oraz prokuratora i asesora prokuratury pełniącego czynności prokuratorskie.

11. W stosunku do osób zajmujących lub kandydujących na stanowiska albo pełniących funkcje, o których mowa w ust. 10 pkt 5 – 15, ubiegających się o dostęp do informacji niejawnych organizacji międzynarodowych lub o dostęp, który ma wynikać

z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską, ABW lub SKW, przeprowadzają poszerzone postępowanie sprawdzające. Z wnioskiem o przeprowadzenie tego postępowania występuje osoba uprawniona do powołania na to stanowisko lub Marszałek Sejmu w stosunku do posłów lub jeżeli do powołania jest uprawniony Sejm albo Marszałek Senatu w stosunku do senatorów lub jeżeli do powołania jest uprawniony Senat.

12. W stosunku do kandydatów na stanowiska, o których mowa w ust. 10 pkt 6 – 13, oraz wobec posłów lub 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 występuje osoba uprawniona do powołania na to stanowisko lub Marszałek Sejmu w stosunku do posłów lub jeżeli do powołania jest uprawniony Sejm albo Marszałek Senatu w stosunku do senatorów lub jeżeli do powołania jest uprawniony Senat.

13. Postępowanie sprawdzające, o którym mowa w ust. 12, w stosunku do osób kandydujących na stanowiska, o których mowa w ust. 10 pkt 6 – 13, powinno być zakończone przed upływem 14 dni od dnia złożenia wniosku o przeprowadzenie tego postępowania wraz z wypełnioną ankietą, o której mowa w art. 24 ust. 10.

14. W przypadku zakończenia postępowania sprawdzającego prowadzonego na wniosek Marszałka Sejmu lub Marszałka Senatu decyzją o odmowie wydania poświadczenia bezpieczeństwa, Prezes Rady Ministrów przedstawia informację o powodach tej decyzji odpowiednio Marszałkowi Sejmu albo Marszałkowi Senatu.

15. 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.

Rozdział 6

Postępowanie odwoławcze i skargowe, wznowienie postępowania

Art. 35. 1. Od decyzji o odmowie wydania poświadczenia bezpieczeństwa, o cofnięciu poświadczenia bezpieczeństwa albo o umorzeniu postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego, wydanej przez podmioty, o których mowa w art. 23 ust. 2 i 5, osobie sprawdzanej przysługuje odwołanie do Prezesa Rady Ministrów. Odwołanie nie wymaga uzasadnienia.

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

3. Podmioty, o których mowa w art. 23 ust. 2 i 5, są zobowiązane przesłać odwołanie wraz z aktami postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego Prezesowi Rady Ministrów w terminie 14 dni od dnia, w którym otrzymały odwołanie.

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

5. Wniesienie odwołania nie wstrzymuje wykonania decyzji.

Art. 36. 1. Prezes Rady Ministrów stwierdza, w drodze postanowienia:

1) niedopuszczalność odwołania;
2) uchybienie terminu do wniesienia odwołania.

2. Postanowienie w tej sprawie jest ostateczne i powinno zawierać w szczególności:

1) oznaczenie organu;
2) datę wydania;
3) oznaczenie osoby sprawdzanej;
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. Prezes Rady Ministrów może na żądanie osoby sprawdzanej lub z urzędu zlecić właściwemu organowi lub służbie przeprowadzenie dodatkowych czynności w celu uzupełnienia dowodów i materiałów w postępowaniu sprawdzającym lub kontrolnym postępowaniu sprawdzającym.

4. Prezes Rady Ministrów wydaje decyzję, w której:

1) utrzymuje w mocy decyzję organu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające;

2) uchyla decyzję organu, który przeprowadził kontrolne postępowanie sprawdzające zakończone cofnięciem poświadczenia bezpieczeństwa;
3) uchyla decyzję organu, który przeprowadził postępowanie sprawdzające i nakazuje mu wydanie poświadczenia bezpieczeństwa;
4) uchyla decyzję organu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające i przekazuje sprawę do ponownego rozpatrzenia;
5) stwierdza nieważność decyzji organu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające.

5. Decyzja powinna zawierać:
1) datę wydania;
2) oznaczenie osoby sprawdzanej;
3) powołanie podstawy prawnej;
4) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne;
5) pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego.

6. Po wydaniu decyzji lub postanowienia Prezes Rady Ministrów niezwłocznie zwraca właściwemu organowi akta, o których mowa w art. 38 ust. 4.

7. Decyzje i postanowienia doręcza się na piśmie osobie sprawdzanej i właściwemu organowi, zawiadamiając o rozstrzygnięciu zawartym w decyzji lub postanowieniu osobę uprawnioną do obsady stanowiska.

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

Art. 37. 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 w trybie art. 23 ust. 2 i 5, 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 Prezesem Rady Ministrów, z zastrzeżeniem ust. 3.

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

Art. 38. 1. Osobie sprawdzanej przysługuje skarga do sądu administracyjnego na decyzję lub postanowienie organu odwoławczego w terminie 30 dni od dnia doręczenia.

2. Sąd administracyjny rozpatruje skargę na posiedzeniu niejawnym.

3. Wyrok wydany na posiedzeniu niejawnym uzasadnia się tylko w przypadku uwzględnienia skargi. Odpis sentencji wyroku z uzasadnieniem doręcza się tylko właściwemu organowi odwoławczemu. Skarżącemu oraz osobie uprawnionej do obsady stanowiska doręcza się odpis wyroku.

4. Po wydaniu wyroku sąd administracyjny niezwłocznie zwraca akta postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego.

5. Do skargi kasacyjnej stosuje się odpowiednio ust. 2 i 3.

Art. 39. 1. Prezes Rady Ministrów, pełnomocnicy ochrony lub podmioty wymienione w art. 23 ust. 2 i 5 wznawiają postępowanie sprawdzające lub kontrolne postępowanie sprawdzające, zakończone decyzją ostateczną, odpowiednio o odmowie wydania albo o cofnięciu poświadczenia bezpieczeństwa, jeżeli decyzja 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, a postępowanie karne zostało następnie umorzone lub zakończone uniewinnieniem osoby sprawdzanej.

2. Wznowienie postępowania następuje z urzędu lub na wniosek osoby sprawdzanej.

3. Wniosek o wznowienie postępowania wnosi się do organu, który wydał w sprawie decyzję w pierwszej instancji, w terminie 30 dni od dnia, w którym osoba sprawdzana dowiedziała się o okoliczności stanowiącej podstawę do wznowienia postępowania.

4. Rozpatrzenie wniosku powinno nastąpić nie później niż w ciągu 3 miesięcy od dnia jego otrzymania.

5. Organ właściwy do wznowienia postępowania stwierdza, w drodze postanowienia, uchybienie terminu do złożenia wniosku o wznowienie postępowania.

6. Postanowienie, o którym mowa w ust. 5, jest ostateczne i powinno zawierać:

1) oznaczenie organu;
2) datę wydania;
3) oznaczenie osoby sprawdzanej;
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.

7. Wznowienie postępowania następuje w drodze postanowienia.

8. Postanowienie stanowi podstawę do przeprowadzenia przez właściwy organ postępowania co do przyczyn wznowienia oraz co do rozstrzygnięcia istoty sprawy.

9. Odmowa wznowienia postępowania następuje w drodze decyzji.

Art. 40. Organ, o którym mowa w art. 39 ust. 1, po przeprowadzeniu postępowania określonego w art. 39 ust. 8, wydaje decyzję, w której:

1) odmawia uchylenia decyzji o odmowie wydania lub o cofnięciu poświadczenia bezpieczeństwa, gdy stwierdzi brak podstaw do jej uchylenia na podstawie art. 39 ust. 1;
2) odmawia uchylenia decyzji o utrzymaniu w mocy decyzji o odmowie wydania lub o cofnięciu poświadczenia bezpieczeństwa, gdy stwierdzi brak podstaw do jej uchylenia na podstawie art. 39 ust. 1;
3) uchyla decyzję o odmowie wydania poświadczenia bezpieczeństwa, gdy stwierdzi istnienie podstaw do jej uchylenia na podstawie art. 39 ust. 1, i wydaje nową decyzję rozstrzygającą o istocie sprawy;
4) uchyla decyzję o utrzymaniu w mocy decyzji o odmowie wydania poświadczenia bezpieczeństwa oraz poprzedzającą ją decyzję o odmowie wydania poświadczenia, gdy stwierdzi istnienie podstaw do jej uchylenia na podstawie art. 39 ust. 1, i przekazuje sprawę do ponownego rozpatrzenia;

5) uchyla decyzję o cofnięciu poświadczenia bezpieczeństwa, gdy stwierdzi istnienie podstaw do jej uchylenia na podstawie art. 39 ust. 1;
6) uchyla decyzję o utrzymaniu w mocy decyzji o cofnięciu poświadczenia bezpieczeństwa oraz poprzedzającą ją decyzję o cofnięciu poświadczenia bezpieczeństwa, gdy stwierdzi istnienie podstaw do jej uchylenia na podstawie art. 39 ust. 1.

Art. 41. 1. Od decyzji o odmowie wznowienia postępowania, o którym mowa w art. 23 ust. 2 – 5, oraz od decyzji o odmowie uchylenia decyzji wydanej w wyniku postępowania, o którym mowa w art. 23 ust. 2 – 5, osobie sprawdzanej przysługuje odwołanie do Prezesa Rady Ministrów.

2. Od decyzji pełnomocnika ochrony o odmowie wznowienia postępowania, o którym mowa w art. 23 ust. 1 i art. 60 ust. 2, oraz od decyzji pełnomocnika ochrony o odmowie uchylenia decyzji wydanej w wyniku postępowania, o którym mowa w art. 23 ust. 1 i art. 60 ust. 2, osobie sprawdzanej przysługuje odwołanie odpowiednio do Szefa ABW albo Szefa SKW.

3. Od decyzji Prezesa Rady Ministrów o odmowie wznowienia postępowania, o którym mowa w art. 35, oraz od decyzji o odmowie uchylenia decyzji wydanej w wyniku postępowania, o którym mowa w art. 35, nie służy odwołanie, jednakże osoba sprawdzana niezadowolona z decyzji może zwrócić się do Prezesa Rady Ministrów z wnioskiem o ponowne rozpatrzenie sprawy.

4. Od decyzji Szefa ABW albo Szefa SKW o odmowie wznowienia postępowania, o którym mowa w art. 37, oraz od decyzji o odmowie uchylenia decyzji wydanej w wyniku postępowania, o którym mowa w art. 37, nie służy odwołanie, jednakże osoba sprawdzana niezadowolona z decyzji może zwrócić się odpowiednio do Szefa ABW albo Szefa SKW z wnioskiem o ponowne rozpatrzenie sprawy.

Rozdział 7
Kancelarie tajne. Środki bezpieczeństwa fizycznego

Art. 42. 1. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „tajne” lub „ściśle tajne”, tworzy kancelarię, zwaną dalej „kancelarią tajną”, i zatrudnia jej kierownika.

2. W przypadku uzasadnionym względami organizacyjnymi kierownik jednostki organizacyjnej może utworzyć więcej niż jedną kancelarię tajną.

3. W uzasadnionych przypadkach, za zgodą odpowiednio ABW lub SKW, można utworzyć kancelarię tajną obsługującą dwie lub więcej jednostek organizacyjnych. Podległość, obsada i zasady finansowania takiej kancelarii zostaną określone przez właściwych kierowników jednostek organizacyjnych.

4. Kancelaria tajna stanowi wyodrębnioną komórkę organizacyjną, w zakresie ochrony informacji niejawnych podległą pełnomocnikowi ochrony, obsługiwaną przez pracowników pionu ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom.

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

6. Kierownik jednostki organizacyjnej informuje odpowiednio ABW lub SKW o utworzeniu i likwidacji kancelarii tajnej, z określeniem klauzuli tajności przetwarzanych w niej informacji niejawnych.

Art. 43. 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 z tym materiałem się zapoznał.

2. Przepis ust. 1 stosuje się odpowiednio do organizacji pracy innych niż kancelaria tajna komórek, w których są rejestrowane materiały o klauzuli „poufne".

3. Kierownik jednostki organizacyjnej zatwierdza, opracowane przez pełnomocnika ochrony, zasady obiegu informacji niejawnych o klauzuli „poufne" w podległych komórkach organizacyjnych.

4. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej, zatwierdza opracowaną przez pełnomocnika ochrony dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą.

5. Kierownik jednostki organizacyjnej zatwierdza, opracowaną przez pełnomocnika ochrony, instrukcję dotyczącą zasad obiegu informacji niejawnych o klauzuli „zastrzeżone" w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego do ich ochrony.

6. Kancelaria tajna lub komórka, o której mowa w ust. 2, odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.

Art. 44. 1. W jednostkach organizacyjnych, o których mowa w art. 47 ust. 3, 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.

2. Do komórek organizacyjnych, o których mowa w ust. 1, przepisy art. 46 stosuje się odpowiednio.

Art. 45. 1. Jednostki organizacyjne, w których są przetwarzane informacje niejawne, stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, 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 niż posiadane uprawnienia.

2. Zakres stosowania środków bezpieczeństwa fizycznego uzależnia się od poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą.

3. W określeniu poziomu zagrożeń, o którym mowa w ust. 2, uwzględnia się w szczególności występujące rodzaje zagrożeń, klauzule tajności i liczbę informacji niejawnych. W uzasadnionych przypadkach w określeniu poziomu zagrożeń uwzględnia się wskazania odpowiednio ABW lub SKW.

Art. 46. 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 wejść i wyjść ze stref ochronnych;

3) określić uprawnienia do przebywania w strefach ochronnych;
4) stosować wyposażenie i urządzenia, którym przyznano certyfikaty.

Art. 47. 1. Rada Ministrów określi, w drodze rozporządzenia:
1) podstawowe kryteria i sposób określania poziomu zagrożeń oraz dobór środków bezpieczeństwa fizycznego właściwych do wskazanego poziomu zagrożeń;
2) wymagania w zakresie organizacji i funkcjonowania kancelarii tajnych oraz obiegu informacji niejawnych;
3) rodzaje zagrożeń, które należy uwzględnić w określaniu poziomu zagrożeń;
4) podstawowe elementy, które powinien zawierać plan ochrony informacji niejawnych;
5) zakres stosowania środków bezpieczeństwa fizycznego;
6) kryteria tworzenia stref ochronnych;
7) strukturę organizacyjną kancelarii tajnej, z uwzględnieniem możliwości tworzenia jej oddziałów;
8) podstawowe zadania kierownika kancelarii;
9) tryb obiegu informacji niejawnych;
10) wzór karty zapoznania z dokumentem;
11) wzory dzienników ewidencji.

2. W rozporządzeniu, o którym mowa w ust. 1, Rada Ministrów uwzględni potrzebę racjonalizacji nakładów ponoszonych przez jednostki organizacyjne w zakresie tworzenia systemu bezpieczeństwa fizycznego informacji niejawnych, zgodnie z zasadami określonymi w ustawie.

3. Ministrowie właściwi do spraw wewnętrznych, administracji publicznej, spraw zagranicznych, finansów publicznych, budżetu i instytucji finansowych, Minister Obrony Narodowej, Minister Sprawiedliwości, Prezes Narodowego Banku Polskiego, Prezes Najwyższej Izby Kontroli, Pierwszy Prezes Sądu Najwyższego, Prokurator Generalny, Szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu oraz Prezesa Rady Ministrów, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Służby Kontrwywiadu Wojskowego, Szef Służby Wywiadu Wojskowego, Szef Centralnego Biura Antykorupcyjnego, Komendant Główny Policji, Komendant Główny Straży Granicznej, Szef Biura Ochrony Rządu, a także Prezes Instytutu Pamięci Narodowej –

Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, określą, w drodze zarządzenia, każdy w zakresie swojego działania, szczególny sposób organizacji i funkcjonowania kancelarii tajnych oraz komórek organizacyjnych, o których mowa w art. 44 ust. 1, sposób obiegu informacji niejawnych oraz dobór i stosowanie środków bezpieczeństwa fizycznego.

4. 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.

5. W rozporządzeniu, o którym mowa w ust. 4, Prezes Rady Ministrów uwzględni potrzebę zabezpieczenia materiałów przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem oraz szczególne warunki ochrony ze względu na rozmiary lub charakter materiału.

Rozdział 8
Bezpieczeństwo teleinformatyczne

Art. 48. 1. Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego.

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

3. ABW lub SKW udziela akredytacji bezpieczeństwa teleinformatycznego systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej.

4. ABW lub SKW udzielają lub odmawiają udzielenia akredytacji, o której mowa w ust. 3, w terminie 6 miesięcy od otrzymania kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego. W uzasadnionych przypadkach, w szczególności wynikających z rozległości systemu i stopnia jego skomplikowania, termin ten może być przedłużony o kolejne 6 miesięcy.

5. Potwierdzeniem udzielenia przez ABW lub SKW akredytacji, o której mowa w ust. 3, jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego, w szczególności zawierające warunki jego ważności.

6. Świadectwo, o którym mowa w ust. 5, wydaje się na podstawie:

1) zatwierdzonej przez ABW lub SKW dokumentacji bezpieczeństwa systemu teleinformatycznego;

2) wyników audytu bezpieczeństwa systemu teleinformatycznego przeprowadzonego przez ABW lub SKW.

7. ABW lub SKW może odstąpić od przeprowadzenia audytu bezpieczeństwa systemu teleinformatycznego, o którym mowa w ust. 6 pkt 2, jeżeli system jest przeznaczony do przetwarzania informacji niejawnych o klauzuli „poufne”.

8. Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa teleinformatycznego systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.

9. W przypadku gdy system, o którym mowa w ust. 8, będzie funkcjonował w więcej niż jednej jednostce organizacyjnej, akredytacji, o której mowa w ust. 8, udziela kierownik jednostki organizującej system.

10. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego, o której mowa w ust. 8, kierownik jednostki organizacyjnej przekazuje odpowiednio ABW lub SKW dokumentację bezpieczeństwa systemu teleinformatycznego.

11. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego ABW lub SKW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji bezpieczeństwa teleinformatycznego, zalecenia

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

Art. 49. 1. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty budowy, zasady działania i eksploatacji, które mają związek lub wpływają na bezpieczeństwo systemu. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym od szczególnych wymagań bezpieczeństwa dokumencie.

2. Dokument szczególnych wymagań bezpieczeństwa opracowuje się na etapie projektowania, w razie potrzeby konsultuje z ABW lub SKW, bieżąco uzupełnia na etapie wdrażania i modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

3. Dokument procedur bezpiecznej eksploatacji określa sposób i tryb postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp.

4. Dokument procedur bezpiecznej eksploatacji opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

5. Podstawą dokonania wszelkich zmian w systemie teleinformatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.

6. Kierownik jednostki organizacyjnej, w której będzie funkcjonował system teleinformatyczny, odpowiada za opracowanie oraz przekazanie odpowiednio ABW lub SKW dokumentacji bezpieczeństwa systemu teleinformatycznego.

7. W przypadku gdy system teleinformatyczny będzie funkcjonował w więcej niż jednej jednostce organizacyjnej, za opracowanie oraz przekazanie odpowiednio

ABW lub SKW dokumentacji bezpieczeństwa systemu teleinformatycznego odpowiada kierownik jednostki organizującej system.

8. Kierownik jednostki organizacyjnej akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego.

9. W terminie 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej ABW lub SKW przeprowadza na jej podstawie ocenę bezpieczeństwa tego systemu. Pozytywny wynik oceny stanowi podstawę do zatwierdzenia przez ABW lub SKW dokumentacji bezpieczeństwa systemu teleinformatycznego. W uzasadnionych przypadkach, w szczególności wynikających ze stopnia skomplikowania systemu, termin przeprowadzenia oceny może być przedłużony o kolejne 30 dni.

10. Prezes Rady Ministrów określi, w drodze rozporządzenia, podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne, oraz sposób opracowywania dokumentacji bezpieczeństwa systemów teleinformatycznych.

11. W rozporządzeniu, o którym mowa w ust. 10, Prezes Rady Ministrów uwzględni w szczególności wymagania w zakresie zarządzania ryzykiem oraz dotyczące zapewnienia poufności, integralności i dostępności informacji niejawnych przetwarzanych w systemach teleinformatycznych.

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

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

3. ABW lub SKW, na wniosek zainteresowanego podmiotu, przeprowadza proces certyfikacji urządzenia lub narzędzia realizującego zabezpieczenia teleinformatyczne, przeznaczonego do ochrony informacji niejawnych.

4. Pozytywne wyniki ocen bezpieczeństwa na podstawie wyników badań prowadzonych w ramach procesów certyfikacji, o których mowa w ust. 1 – 3, stanowią podstawę do wydania przez ABW lub SKW certyfikatu ochrony elektromagnetycznej, certyfikatu ochrony kryptograficznej lub certyfikatu bezpieczeństwa teleinformatycznego.

Certyfikaty są wydawane, w zależności od wyników ocen bezpieczeństwa, na okres nie krótszy niż 3 lata.

5. ABW i SKW wzajemnie informują się o przypadkach zawieszenia lub unieważnienia certyfikatów, o których mowa w ust. 4.

6. Procesy certyfikacji, o których mowa w ust. 1 – 3, są prowadzone przez ABW lub SKW z pominięciem właściwości, o której mowa w art. 10 ust. 2 i 3.

7. Szef ABW lub Szef SKW może zlecić podmiotowi zewnętrznemu badanie cząstkowe urządzenia lub narzędzia służącego do ochrony informacji niejawnych, na zasadach i warunkach przez siebie określonych. W przypadku środka ochrony elektromagnetycznej zlecane badania mogą być pełne.

8. Bez konieczności przeprowadzania badań i oceny Szef ABW lub Szef SKW może dopuścić do stosowania w systemie teleinformatycznym przeznaczonym do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" urządzenia lub narzędzia kryptograficzne, jeżeli otrzymały stosowny certyfikat wydany przez krajową władzę bezpieczeństwa państwa będącego członkiem NATO lub Unii Europejskiej lub inny uprawniony organ w NATO lub w Unii Europejskiej.

Art. 51. 1. Obowiązkowi akredytacji, o którym mowa w art. 48 ust. 1, nie podlegają systemy teleinformatyczne 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. Nr 171, poz. 1800, z późn. zm.[13)]), oraz systemów z nimi współpracujących.

2. Obowiązkowi akredytacji, o którym mowa w art. 48 ust. 1, oraz badań i oceny bezpieczeństwa w ramach procesów certyfikacji prowadzonych przez ABW lub SKW nie podlegają systemy teleinformatyczne, urządzenia lub narzędzia kryptograficzne wykorzystywane przez 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) pracownika lub pracowników pionu ochrony pełniących funkcję inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;
2) osobę lub zespół osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa dla systemu teleinformatycznego, zwane dalej „administratorem systemu".

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

3. ABW i SKW udzielają kierownikom jednostek organizacyjnych pomocy niezbędnej do realizacji ich zadań, w szczególności wydając zalecenia w zakresie bezpieczeństwa teleinformatycznego.

4. Stanowiska lub funkcje, o których mowa w ust. 1, mogą zajmować lub pełnić osoby spełniające wymagania, o których mowa w art. 16, po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez ABW lub SKW.

5. Koszty szkoleń, o których mowa w ust. 4, pokrywa jednostka organizacyjna, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje prace zlecone, z zastrzeżeniem ust. 6.

6. Jednostki organizacyjne, o których mowa w art. 1 ust. 2 pkt 2 oraz w art. 23 ust. 5 pkt 4, nie pokrywają kosztów szkoleń przeprowadzonych przez ABW lub SKW.

7. Wzajemne prawa i obowiązki podmiotu przeprowadzającego szkolenie i uczestnika szkolenia, o którym mowa w ust. 4, określa umowa zawarta między tym podmiotem a jednostką organizacyjną, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje czynności zlecone.

Art. 53. 1. Za przeprowadzenie czynności, o których mowa w art. 48 ust. 3 – 6 oraz art. 50 ust. 1 – 4, pobiera się opłaty.

2. Z opłat, o których mowa w ust. 1, są zwolnione jednostki organizacyjne będące jednostkami budżetowymi.

3. Przedsiębiorcy obowiązani na podstawie odrębnych ustaw do wykonywania zadań publicznych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego są zwolnieni z opłat za przeprowadzenie czynności, o których mowa w art. 48 ust. 3 – 6, w przypadku akredytacji bezpieczeństwa teleinformatycznego systemów teleinformatycznych niezbędnych do wykonania tych zadań.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, wysokość opłat, o których mowa w ust. 1, z uwzględnieniem kosztów ponoszonych na przeprowadzenie czynności, o których mowa w art. 48 ust. 3 – 6 oraz art. 50 ust. 1 – 4.

Rozdział 9
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", wydane przez ABW lub SKW po przeprowadzeniu postępowania bezpieczeństwa przemysłowego.

3. 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, wydane przez ABW lub SKW, i zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych wydane przez ABW lub SKW.

4. Przepisu ust. 3 nie stosuje się, gdy obowiązek uzyskania świadectwa wynika z ratyfikowanych przez Rzeczpospolitą Polską umów międzynarodowych lub prawa wewnętrznego strony zawierającej umowę.

5. Do przedsiębiorcy, o którym mowa w ust. 3, nie stosuje się przepisów niniejszego rozdziału, z wyjątkiem art. 60 oraz art. 61 ust. 1 w części dotyczącej postępowań sprawdzających.

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

7. Szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu lub Prezesa Rady Ministrów albo minister właściwy dla określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego lub kierownik urzędu centralnego, a w przypadku ich braku – Szef ABW lub Szef SKW, mogą wyrazić pisemną zgodę na udostępnienie informacji niejawnych o klauzuli „poufne" lub wyższej przedsiębiorcy, wobec którego wszczęto postępowanie bezpieczeństwa przemysłowego lub postępowanie sprawdzające. Potwierdzoną za zgodność kopię zgody przekazuje się odpowiednio do ABW lub SKW.

8. W szczególnie uzasadnionych przypadkach podmioty, o których mowa w ust. 7, mogą wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych przedsiębiorcy nieposiadającemu odpowiedniego świadectwa lub poświadczenia bezpieczeństwa w przypadku przedsiębiorcy, o którym mowa w ust. 3 i wobec którego nie jest prowadzone postępowanie bezpieczeństwa przemysłowego lub nie jest prowadzone postępowanie sprawdzające.

9. W przypadku gdy przedsiębiorca zamierza wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone", świadectwo nie jest wymagane.

10. Przedsiębiorca, o którym mowa w ust. 9, jest obowiązany spełnić wymagania ustawy w zakresie ochrony informacji niejawnych o klauzuli „zastrzeżone", z wyjątkiem zatrudnienia pełnomocnika ochrony, gdy wykonuje umowę z dostępem do tych informacji, z wyłączeniem możliwości ich przetwarzania 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 pełną zdolność przedsiębiorcy do ochrony tych informacji;
2) drugiego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych;

3) trzeciego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach.

2. Świadectwo potwierdzające zdolność do ochrony informacji niejawnych 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. ABW lub SKW wydaje odrębne świadectwa potwierdzające zdolność do ochrony informacji niejawnych o klauzulach stanowiących zagraniczne odpowiedniki klauzul „tajne" lub „poufne" stosowanych przez organizacje międzynarodowe. Przepis ust. 2 stosuje się odpowiednio.

4. Świadectwo wygasa, jeżeli:

1) upłynął okres jego ważności, o którym mowa w ust. 2;
2) przedsiębiorca zrzekł się uprawnień określonych w świadectwie;
3) przedsiębiorca został przejęty przez inny podmiot lub zlikwidowany.

Art. 56. 1. Postępowanie bezpieczeństwa przemysłowego jest prowadzone na wniosek 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 bezpieczeństwa osobowego lub kopie poświadczeń bezpieczeństwa osób określonych w art. 57 ust. 3.

4. ABW lub SKW może wezwać przedsiębiorcę do uzupełnienia braków formalnych we wniosku i jego załącznikach w terminie 30 dni, 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 zawartych w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie, obejmuje:

1) strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuację finansową;
2) strukturę organizacyjną;
3) system ochrony informacji niejawnych, w tym środki bezpieczeństwa fizycznego;
4) wszystkie osoby wchodzące w skład organów zarządzających, kontrolnych oraz osoby działające z ich upoważnienia;
5) w szczególnie uzasadnionych przypadkach osoby posiadające poświadczenia bezpieczeństwa.

3. W toku postępowania bezpieczeństwa przemysłowego 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;
3) osób zatrudnionych w pionie ochrony;
4) administratora systemu teleinformatycznego;
5) pozostałych osób wskazanych w kwestionariuszu, które powinny mieć dostęp do informacji niejawnych.

4. W stosunku do osób, o których mowa w ust. 3 pkt 1 – 4, odpowiednie poświadczenie bezpieczeństwa oznacza poświadczenie upoważniające do dostępu do informacji niejawnych o klauzuli nie niższej niż wskazana we wniosku przedsiębiorcy o wydanie świadectwa.

Art. 58. 1. Sprawdzenie przedsiębiorcy i osób prowadzi 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 w szczególności:

1) dane identyfikujące podmiot podlegający sprawdzeniu, w tym jego status prawny;
2) dane o strukturze kapitału i powiązaniach kapitałowych przedsiębiorcy;
3) dane o źródłach pochodzenia środków finansowych i sytuacji finansowej przedsiębiorcy;
4) dane o strukturze organizacyjnej przedsiębiorcy;
5) dane dotyczące osób, o których mowa w art. 57 ust. 2 pkt 4;
6) dane o systemie ochrony informacji niejawnych przedsiębiorcy, w tym o stosowanych środkach bezpieczeństwa fizycznego;
7) wykaz pracowników posiadających poświadczenia bezpieczeństwa uprawniające do dostępu do informacji niejawnych;
8) wykaz pracowników, którzy powinni być poddani poszerzonemu postępowaniu sprawdzającemu;
9) wykaz osób, które ze strony przedsiębiorcy wykonują lub będą wykonywać funkcje związane z ochroną informacji niejawnych;
10) podpis osoby upoważnionej do składania oświadczeń woli w imieniu przedsiębiorcy.

Art. 59. Postępowanie bezpieczeństwa przemysłowego powinno być zakończone w terminie nie dłuższym niż 6 miesięcy od dnia przedłożenia wszystkich dokumentów niezbędnych do jego przeprowadzenia.

Art. 60. 1. W przypadku postępowania bezpieczeństwa przemysłowego prowadzonego w celu wydania świadectwa, o którym mowa w art. 55 ust. 1 pkt 3, zatrudnienie pełnomocnika ochrony oraz utworzenie pionu ochrony nie jest wymagane, z wyjątkiem ubiegania się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli będącej zagranicznym odpowiednikiem klauzuli „tajne” lub „poufne”, stosowanym przez organizacje międzynarodowe.

2. Pełnomocnik ochrony jednostki organizacyjnej zlecającej wykonanie umowy, z której wykonaniem łączy się dostęp do informacji niejawnych o klauzuli „poufne”,

może przeprowadzić zwykłe postępowanie sprawdzające oraz szkolenie w zakresie ochrony informacji niejawnych wobec osób określonych w art. 57 ust. 3 pkt 5 w przypadku postępowania bezpieczeństwa przemysłowego, o którym mowa w art. 55 ust. 1 pkt 3. Odpowiednie wnioski kierownik przedsiębiorcy składa do kierownika jednostki organizacyjnej, która zleca wykonanie umowy.

Art. 61. 1. Za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających wobec osób wymienionych w art. 57 ust. 3, z wyjątkiem postępowań sprawdzających, o których mowa w art. 32 ust. 4 i art. 33 ust. 1, ABW lub SKW przysługuje zwrot zryczałtowanych kosztów ponoszonych na przeprowadzenie czynności przy sprawdzeniach przedsiębiorcy oraz postępowań sprawdzających.

2. Prezes Rady Ministrów określi, w drodze rozporządzenia, wysokość zryczałtowanych kosztów, o których mowa w ust. 1, oraz tryb ich zwrotu, uwzględniając, że wysokość kosztów nie powinna przekroczyć 7-krotności kwoty przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłoszonego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 7 ust. 1 ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich.

Art. 62. ABW lub 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.

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

2. ABW lub 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) nieuregulowania w terminie zobowiązań publicznoprawnych;
4) uzależnienia wyniku oceny zdolności przedsiębiorcy do ochrony informacji niejawnych od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd.

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

Art. 64. 1. Postępowanie bezpieczeństwa przemysłowego kończy się wydaniem przez ABW lub SKW świadectwa zgodnie z wnioskiem przedsiębiorcy albo decyzją o odmowie wydania świadectwa lub decyzją o umorzeniu postępowania bezpieczeństwa przemysłowego.

2. ABW lub 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 i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy;
3) niezorganizowania, w terminie 6 miesięcy od daty wszczęcia postępowania, kompleksowego systemu ochrony informacji niejawnych w przypadku ubiegania się o świadectwo pierwszego lub drugiego stopnia;
4) zatajenia danych w kwestionariuszu lub podania w nim danych nieprawdziwych;
5) podania nieprawdziwych informacji o zmianach danych zawartych w kwestionariuszu.

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

1) ujawnienia, w wyniku sprawdzenia osób wymienionych w art. 57 ust. 2 pkt 4, w toku postępowania bezpieczeństwa przemysłowego niedających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1 – 3 lub 5 lub w art. 24 ust. 3;

2) niepowiadomienia w terminie 30 dni o zmianie danych zawartych w kwestionariuszu w trakcie postępowania bezpieczeństwa przemysłowego.

Art. 65. 1. ABW lub SKW, w okresie ważności świadectwa, może przeprowadzić z urzędu wybrane elementy sprawdzenia przedsiębiorcy, o których mowa w art. 57 ust. 2, w celu ustalenia, czy nie utracił on zdolności do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem.

2. W przypadku gdy świadectwo zostało wydane przez ABW, a przedsiębiorca realizuje umowę na rzecz jednostek organizacyjnych, o których mowa w art. 1 ust. 2 pkt 2, SKW – gdy w toku realizacji umowy ujawniła fakty wskazujące na możliwość utraty przez przedsiębiorcę zdolności do ochrony informacji niejawnych – może wystąpić do ABW o przeprowadzenie kontroli, o której mowa w art. 10 ust. 1 pkt 1, lub sprawdzenia określonego w art. 57 ust. 2.

3. W kontroli, o której mowa w art. 10 ust. 1 pkt 1, lub sprawdzeniu, o którym mowa w art. 57 ust. 2 pkt 3, mogą uczestniczyć funkcjonariusze lub żołnierze SKW. Przed kontrolą lub sprawdzeniem, o którym mowa w art. 57 ust. 2 pkt 3, upoważnieni żołnierze lub funkcjonariusze SKW mogą zapoznać się z aktami postępowania bezpieczeństwa przemysłowego w zakresie dotyczącym kontroli lub sprawdzenia.

4. W przypadku wydania świadectwa przez SKW i realizacji przez przedsiębiorcę umów na rzecz innych jednostek organizacyjnych niż wymienione w ust. 2 przepisy ust. 2 i 3 stosuje się odpowiednio w stosunku do ABW i jej funkcjonariuszy.

Art. 66. 1. Wyniki sprawdzenia przedsiębiorcy z urzędu lub ustalenia kontroli ochrony informacji niejawnych mogą stanowić podstawę wydania decyzji o cofnięciu świadectwa.

2. ABW lub SKW cofa świadectwo, stwierdzając utratę zdolności do ochrony informacji niejawnych, z powodu:

1) odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa osobie lub osobom, które zajmują stanowisko kierownika przedsiębiorcy;
2) braku możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy;

3) utraty funkcjonalności systemu ochrony informacji niejawnych;
4) podania nieprawdziwych danych lub ich zatajenia w ramach przekazywanych ABW lub SKW informacji o zmianach danych zawartych w kwestionariuszu.

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

1) ujawnienia, w wyniku sprawdzeń osób wymienionych w art. 57 ust. 2 pkt 4, w toku postępowania bezpieczeństwa przemysłowego niedających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1 – 3 lub 5 lub w art. 24 ust. 3;
2) niewykonania przez przedsiębiorcę obowiązku, o którym mowa w art. 70 ust. 1.

4. O cofnięciu świadectwa ABW lub SKW zawiadamia niezwłocznie jednostki organizacyjne, które zawarły umowy z przedsiębiorcą.

Art. 67. 1. Świadectwo, decyzja o odmowie wydania świadectwa oraz decyzja o cofnięciu świadectwa powinny zawierać:

1) oznaczenie organu, który wydał, odmówił wydania bądź cofnął świadectwo bezpieczeństwa przemysłowego;
2) miejsce i datę wystawienia;
3) nazwę podmiotu, adres jego siedziby, numer w Krajowym Rejestrze Sądowym i numer REGON;
4) podstawę prawną;
5) stwierdzenie wydania świadectwa bezpieczeństwa przemysłowego, odmowy wydania lub jego cofnięcia;
6) w przypadku wydania świadectwa bezpieczeństwa przemysłowego – jego stopień, klauzulę tajności oraz termin ważności;
7) imienną pieczęć i 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:

1) odwołania do Prezesa Rady Ministrów;
2) skargi do sądu administracyjnego.

3. Można odstąpić od uzasadnienia faktycznego decyzji lub je ograniczyć w zakresie, w jakim wiązałoby się to z udostępnieniem informacji niejawnych.

Art. 68. Rada Ministrów określi, w drodze rozporządzenia, wzory:

1) kwestionariusza bezpieczeństwa przemysłowego,
2) świadectwa bezpieczeństwa przemysłowego,
3) decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego,
4) decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego

– uwzględniając odpowiednio zakres danych, o których mowa w art. 58 ust. 2 i art. 67 ust. 1 i 2.

Art. 69. 1. Od decyzji o umorzeniu postępowania bezpieczeństwa przemysłowego, odmowie wydania oraz o cofnięciu świadectwa przedsiębiorcy przysługuje odwołanie do Prezesa Rady Ministrów, na którego decyzję lub postanowienie przysługuje skarga do sądu administracyjnego.

2. Do odwołania i skargi, o których mowa w ust. 1, stosuje się odpowiednio przepisy art. 35, 36 i 38.

3. W przypadku wydania orzeczenia o zakazie prowadzenia przez przedsiębiorcę działalności gospodarczej, przejęcia lub likwidacji przedsiębiorcy Prezes Rady Ministrów umarza postępowanie odwoławcze.

Art. 70. 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 bezpieczeństwa przemysłowego;
2) ogłoszeniu upadłości, likwidacji lub rozwiązaniu jednostki organizacyjnej albo innej formie zakończenia przez nią działalności;
3) potrzebie zawarcia lub zawarciu umowy z podwykonawcą, związanej z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej;
4) wypowiedzeniu umowy;

5) zakończeniu wykonania umowy;
6) zawarciu nowej umowy związanej z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej, ze szczególnym uwzględnieniem:
   a) nazwy i adresu jednostki organizacyjnej zawierającej umowę,
   b) przedmiotu umowy,
   c) najwyższej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonaniem umowy.

2. Przedsiębiorca, w czasie realizacji umowy, ma obowiązek niezwłocznego informowania osoby, o której mowa w art. 71 ust. 3, o:
1) zmianach w systemie ochrony informacji niejawnych;
2) zmianach osób wykonujących umowę;
3) potrzebie zawarcia z podwykonawcą umowy związanej z dostępem do informacji niejawnych.

3. W przypadkach gdy zawierającymi umowę są jednostki organizacyjne, o których mowa w art. 1 ust. 2 pkt 2, ABW po uzyskaniu od przedsiębiorcy informacji, o której mowa w ust. 1 pkt 6, przekazuje ją SKW.

4. W przypadku gdy zawierającą umowę jest inna jednostka organizacyjna niż wymieniona w ust. 3, SKW po uzyskaniu od przedsiębiorcy informacji, o której mowa w ust. 1 pkt 6, przekazuje ją ABW.

Art. 71. 1. Jednostka organizacyjna zawierająca umowę związaną 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 niniejszej ustawy, a także nieprzestrzegania wymagań określonych w instrukcji bezpieczeństwa przemysłowego.

2. Instrukcja bezpieczeństwa przemysłowego powinna określać w szczególności:

1) klauzule tajności poszczególnych materiałów lub rodzajów materiałów, które zostaną wytworzone przez przedsiębiorcę w związku z wykonaniem umowy;
2) sposób postępowania z materiałami niejawnymi, które zostaną przekazane przedsiębiorcy lub przez niego wytworzone w związku z wykonaniem umowy.

3. Kierownik jednostki organizacyjnej zawierający 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 wykonaniem umowy zostaną wytworzone informacje niejawne, odpowiednią klauzulę tajności nadaje osoba, o której mowa w art. 6 ust. 1, zgodnie ze wskazaniami zawartymi w instrukcji bezpieczeństwa przemysłowego, a w przypadku ich braku, po uzgodnieniu z osobą, o której mowa w ust. 3.

5. Jednostka organizacyjna, 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 przedsiębiorcy, z którym zawarto umowę,
   b) przedmiocie umowy,
   c) najwyższej koniecznej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonaniem umowy,
   d) naruszeniu przepisów o ochronie informacji niejawnych u przedsiębiorcy, z którym zawarto umowę,
   e) zakończeniu wykonania umowy;
2) niezwłocznego przekazania odpowiednio ABW lub SKW:
   a) kopii instrukcji bezpieczeństwa przemysłowego, o której mowa w ust. 1,
   b) kopii świadectwa przedsiębiorcy, z którym zawarto umowę.

6. W przypadkach gdy zawierającymi umowę są jednostki organizacyjne, o których mowa w art. 1 ust. 2 pkt 2, a świadectwo zostało wydane przez ABW, obowiązek, o którym mowa w ust. 5, jest także realizowany wobec SKW.

7. W przypadku gdy zawierającym umowę jest inna jednostka organizacyjna niż wymienione w ust. 6, a świadectwo zostało wydane przez SKW, obowiązek, o którym mowa w ust. 5, jest także realizowany wobec ABW.

Rozdział 10
Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego

Art. 72. 1. Akta postępowań sprawdzających lub kontrolnych postępowań sprawdzających przeprowadzonych przez służby i instytucje uprawnione do realizacji poszerzonych postępowań sprawdzających i akta postępowań bezpieczeństwa przemysłowego są udostępniane do wglądu bądź przekazywane wyłącznie na pisemne żądanie:

1) sądowi lub prokuratorowi dla celów postępowania karnego;
2) służbom i organom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających dla celów postępowania sprawdzającego wobec tej samej osoby;
3) właściwemu organowi w celu przeprowadzenia kontroli prawidłowości postępowania, z wyłączeniem postępowań, o których mowa w art. 23 ust. 5;
4) właściwemu organowi w celu rozpatrzenia odwołania lub zażalenia;
5) sądowi administracyjnemu w związku z rozpatrywaniem skargi.

2. Przepisu ust. 1 pkt 2 nie stosuje się w odniesieniu do akt postępowań sprawdzających lub kontrolnych postępowań sprawdzających przeprowadzonych przez AW, ABW, SKW lub SWW. Akta tych postępowań mogą być udostępnione do wglądu wyłącznie dla celów postępowania sprawdzającego prowadzonego przez tę samą służbę wobec tej samej osoby.

3. Akta zwykłych postępowań sprawdzających, w tym kontrolnych postępowań sprawdzających, mogą być udostępnione do wglądu i przekazane w przypadkach określonych w ust. 1 oraz dla celów postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego wobec tej samej osoby.

4. Akta zakończonych zwykłych postępowań sprawdzających, w tym kontrolnych postępowań sprawdzających, mogą być udostępnione do wglądu osobie sprawdzanej, z wyłączeniem danych dotyczących osób trzecich.

5. Po wykorzystaniu akta są niezwłocznie zwracane.

6. Po zakończeniu postępowania sprawdzającego, kontrolnego postępowania sprawdzającego lub postępowania bezpieczeństwa przemysłowego akta tych postępowań są przechowywane, z uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2006 r. Nr 97, poz. 673, z późn. zm.[14)]) oraz aktów wykonawczych wydanych na jej podstawie:

1) jako wyodrębniona część w archiwach służb i instytucji, które przeprowadziły te postępowania;
2) przez pełnomocnika ochrony lub w pionie ochrony – w przypadku akt zwykłych postępowań sprawdzających, w tym kontrolnych postępowań sprawdzających przeprowadzonych przez tego pełnomocnika.

7. W przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji jednostki organizacyjnej akta, o których mowa w ust. 6, przejmuje następca prawny, a w przypadku jego braku – ABW lub SKW.

Art. 73. 1. ABW i SKW prowadzą ewidencję osób uprawnionych na podstawie przepisów ustawy do dostępu do informacji niejawnych o klauzuli „poufne” i wyższej oraz ewidencję osób, którym odmówiono wydania poświadczenia bezpieczeństwa, a także osób, wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, z wyłączeniem osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w podmiotach, o których mowa w art. 23 ust. 5.

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

1) imię i nazwisko;
2) numer PESEL;
3) imię ojca;
4) datę i miejsce urodzenia;
5) adres miejsca zamieszkania lub pobytu;
6) nazwę jednostki organizacyjnej;
7) nazwę komórki organizacyjnej i zajmowanego stanowiska lub wykonywanych czynności zleconych;
8) określenie dokumentu kończącego procedurę, datę wydania oraz numer.

3. Dane z ewidencji, o których mowa w ust. 1, oraz wykazów, o których mowa w art. 15 ust. 1 pkt 8, są udostępniane na pisemne żądanie wyłącznie w przypadkach określonych w art. 72 ust. 1 pkt 1 i 3 – 5 oraz służbom i instytucjom uprawnionym do realizacji poszerzonych postępowań sprawdzających dla celów postępowania sprawdzającego oraz postępowania bezpieczeństwa przemysłowego.

Rozdział 11
Zmiany w przepisach obowiązujących

Art. 74. W ustawie z dnia 31 stycznia 1959 r. o cmentarzach i chowaniu zmarłych (Dz. U. z 2000 r. Nr 23, poz. 295, z późn. zm.[15)]) w art. 11 ust. 7 otrzymuje brzmienie:

„7. Lekarze stwierdzający zgon i jego przyczyny obowiązani są, dla celów statystycznych, udzielać na żądanie właściwych organów wyjaśnień odnoszących się do faktu zgonu i jego przyczyny. Jeżeli zmarły pozostawał podczas ostatniej choroby pod opieką lekarską, wyjaśnienia powinny również dotyczyć przebiegu tej choroby. Wyjaśnienia te stanowią tajemnicę prawnie chronioną i mogą być wykorzystywane tylko dla celów statystycznych oraz w postępowaniu sądowym.”.

Art. 75. W ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071, z późn. zm.[16)]) wprowadza się następujące zmiany:

1) w art. 74 § 1 otrzymuje brzmienie:

„§ 1. Przepisu art. 73 nie stosuje się do akt sprawy zawierających informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne”, a także do innych akt, które organ administracji publicznej wyłączy ze względu na ważny interes państwowy.”;

2) w art. 82 pkt 2 otrzymuje brzmienie:

„2) osoby obowiązane do zachowania w tajemnicy informacji niejawnych na okoliczności objęte tajemnicą, jeżeli nie

zostały w trybie określonym obowiązującymi przepisami zwolnione od obowiązku zachowania tej tajemnicy,”.

Art. 76. W ustawie z dnia 1 grudnia 1961 r. o izbach morskich (Dz. U. z 2009 r. Nr 69, poz. 599) w art. 21 ust. 4 otrzymuje brzmienie:

„4. Organy Marynarki Wojennej, Straży Granicznej, Policji i prokuratury wojskowej w sprawie toczącej się przed izbą morską nie są obowiązane do udzielania informacji, udostępniania dokumentów i innych danych, jeżeli może to doprowadzić do ujawnienia informacji niejawnych.”.

Art. 77. W ustawie z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296, z późn. zm.[17)]) wprowadza się następujące zmiany:

1) w art. 153 § 1 otrzymuje brzmienie:

„§ 1. Sąd z urzędu zarządza odbycie całego posiedzenia lub jego części przy drzwiach zamkniętych, jeżeli publiczne rozpoznanie sprawy zagraża porządkowi publicznemu lub moralności lub jeżeli mogą być ujawnione okoliczności objęte ochroną informacji niejawnych.”;

2) w art. 248 § 1 otrzymuje brzmienie:

„§ 1. Każdy obowiązany jest przedstawić na zarządzenie sądu w oznaczonym terminie i miejscu dokument znajdujący się w jego posiadaniu i stanowiący dowód faktu istotnego dla rozstrzygnięcia sprawy, chyba że dokument zawiera informacje niejawne.”;

3) w art. 259 pkt 2 otrzymuje brzmienie:

„2) wojskowi i urzędnicy niezwolnieni od zachowania w tajemnicy informacji niejawnych o klauzuli „zastrzeżone” lub „poufne”, jeżeli ich zeznanie miałoby być połączone z jej naruszeniem;”.

Art. 78. W ustawie z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2004 r. Nr 241, poz. 2416, z późn. zm.[18)]) 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 Agencja Bezpieczeństwa Wewnętrznego lub Służba Kontrwywiadu Wojskowego, zgodnie z właściwością określoną w przepisach o ochronie informacji niejawnych, na pisemny wniosek kierownika jednostki organizacyjnej przewidzianej do militaryzacji, do której nadano przydziały organizacyjno-mobilizacyjne.”.

Art. 79. W ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94, z późn. zm.[19)]) w art. 241^4 § 4 otrzymuje brzmienie:

„§ 4. Przepisy § 1 – 3 nie naruszają przepisów o ochronie informacji niejawnych.”.

Art. 80. W ustawie z dnia 26 marca 1982 r. o Trybunale Stanu (Dz. U. z 2002 r. Nr 101, poz. 925, z 2003 r. Nr 175, poz. 1692 oraz z 2004 r. Nr 25, poz. 219) wprowadza się następujące zmiany:

1) w art. 18 ust. 5 otrzymuje brzmienie:

„5. W postępowaniu przed Trybunałem Stanu oskarżeni, świadkowie i biegli zwolnieni są od obowiązku zachowania w tajemnicy informacji niejawnych.”;

2) art. 20b otrzymuje brzmienie:

„Art. 20b. Wykluczenie jawności rozprawy przed Trybunałem Stanu może uzasadnić wyłącznie wzgląd na bezpieczeństwo państwa lub ochronę informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne”.”.

Art. 81. W ustawie z dnia 6 lipca 1982 r. o zasadach prowadzenia na terytorium Polskiej Rzeczypospolitej Ludowej działalności gospodarczej w zakresie drobnej wytwórczości przez zagraniczne osoby prawne i fizyczne (Dz. U. z 1989 r. Nr 27, poz. 148, z późn. zm.[20)]) wprowadza się następujące zmiany:

1) w art. 5 w ust. 3 pkt 2 otrzymuje brzmienie:
„2) bezpieczeństwo państwa.”;
2) w art. 6 ust. 3 otrzymuje brzmienie:
„3. Organ administracji państwowej właściwy w sprawach zezwoleń może odmówić wpisania do zezwolenia nazwiska lub nazwy pełnomocnika ze względu na bezpieczeństwo państwa.”.

Art. 82. W ustawie z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz. U. z 2001 r. Nr 86, poz. 953, z późn. zm.[21)]) w art. 17 w ust. 2 pkt 5 otrzymuje brzmienie:

„5) dochowywać tajemnicy związanej z wykonywaniem obowiązków,”.

Art. 83. W ustawie z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy (Dz. U. Nr 35, poz. 163, z późn. zm.[22)]) w art. 8 ust. 3 otrzymuje brzmienie:

„3. Wykonywanie czynności, o których mowa w ust. 1 i 2, następuje z zachowaniem przepisów o ochronie informacji niejawnych.”.

Art. 84. W ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2006 r. Nr 97, poz. 673, z późn. zm.[23)]) wprowadza się następujące zmiany:

1) w art. 5 ust. 5 otrzymuje brzmienie:
„5. Zarządzenia dotyczące określenia sposobu kwalifikowania dokumentacji ze względu na okresy jej przechowywania w Agencji Bezpieczeństwa Wewnętrznego oraz w Agencji Wywiadu podlegają ochronie zgodnie z przepisami o ochronie informacji niejawnych.”;
2) w art. 17 w ust. 3 pkt 1 otrzymuje brzmienie:
„1) sposób postępowania z materiałami archiwalnymi zawierającymi informacje stanowiące tajemnice prawnie chronione, w szczególności informacje niejawne albo dane osobowe podlegające ochronie,”.

Art. 85. W ustawie z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24, z późn. zm.[24)]) w art. 14 ust. 5 otrzymuje brzmienie:

„5. Dziennikarz nie może opublikować informacji, jeżeli osoba udzielająca jej zastrzegła to ze względu na tajemnicę zawodową.”.

Art. 86. W ustawie z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (Dz. U. z 2006 r. Nr 122, poz. 851, z późn. zm.[25)]) art. 29a otrzymuje brzmienie:

„Art. 29a. Uzyskane przez organy Państwowej Inspekcji Sanitarnej w trakcie kontroli informacje, dokumenty i inne dane zawierające tajemnicę prawnie chronioną kontrolowanego nie mogą być przekazywane innym organom ani ujawniane, jeżeli nie jest to konieczne ze względu na ochronę życia lub zdrowia człowieka, z wyłączeniem żądania sądu lub prokuratora w związku z toczącym się postępowaniem.”.

Art. 87. W ustawie z dnia 18 kwietnia 1985 r. o rybactwie śródlądowym (Dz. U. z 1999 r. Nr 66, poz. 750 oraz z 2009 r. Nr 189, poz. 1471) w art. 23 w ust. 1 w pkt 8 lit. c otrzymuje brzmienie:

„c) na wały przeciwpowodziowe, śluzy, tamy, na teren elektrowni, młynów i tartaków wodnych, przepompowni oraz innych urządzeń piętrzących wodę, z wyjątkiem terenów i obiektów Sił Zbrojnych, Straży Granicznej i Policji oraz innych, których szczególne przeznaczenie stanowi informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne”,”.

Art. 88. W ustawie z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2008 r. Nr 7, poz. 39, z późn. zm.[26)]) wprowadza się następujące zmiany:

1) w art. 45 ust. 4 otrzymuje brzmienie:

„4. Przy powołaniu prokurator składa ślubowanie wobec Prokuratora Generalnego według następującej roty:

„Ślubuję uroczyście na powierzonym mi stanowisku prokuratora służyć wiernie Rzeczypospolitej Polskiej, stać na straży prawa i strzec praworządności, obowiązki mojego urzędu wypełniać sumiennie, dochować tajemnicy prawnie chronionej,

a w postępowaniu kierować się zasadami godności i uczciwości"; składający ślubowanie może dodać na końcu zwrot: „Tak mi dopomóż Bóg".";

2) w art. 49a ust. 5 otrzymuje brzmienie:

„5. Informacje zawarte w oświadczeniu o stanie majątkowym stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone" określonej w przepisach o ochronie informacji niejawnych, chyba że prokurator, który złożył oświadczenie, wyraził pisemną zgodę na ich ujawnienie. W szczególnie uzasadnionych przypadkach podmiot uprawniony, zgodnie z ust. 2 lub 3, do odebrania oświadczenia może je ujawnić mimo braku zgody składającego oświadczenie. Oświadczenie przechowuje się przez 6 lat.";

3) w art. 77 ust. 1a otrzymuje brzmienie:

„1a. W celu ograniczenia kręgu osób podejrzanych o popełnienie przewinienia zawierającego znamiona przestępstwa ujawnienia informacji z postępowania karnego stanowiących informacje niejawne o klauzuli tajności „tajne" lub „ściśle tajne" rzecznik dyscyplinarny, w trakcie wstępnego wyjaśniania okoliczności, o których mowa w ust. 1, może polecić biegłemu zastosowanie wobec prokuratora mającego dostęp do tych informacji, za jego zgodą, środków technicznych mających na celu kontrolę nieświadomych reakcji organizmu tej osoby.".

Art. 89. W ustawie z dnia 31 lipca 1985 r. o obowiązkach i prawach posłów i senatorów (Dz. U. z 1991 r. Nr 18, poz. 79 oraz z 1996 r. Nr 73, poz. 350) w art. 19 uchyla się ust. 2 i 3.

Art. 90. W ustawie z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2001 r. Nr 14, poz. 147 oraz z 2006 r. Nr 218, poz. 1592) art. 4 otrzymuje brzmienie:

„Art. 4. Przed przystąpieniem do wykonywania obowiązków Rzecznik składa przed Sejmem następujące ślubowanie:

„Ślubuję uroczyście, że przy wykonywaniu powierzonych mi obowiązków Rzecznika Praw Obywatelskich dochowam wierności Konstytucji Rzeczypospolitej Polskiej, będę strzec wolności i praw człowieka i obywatela, kierując się przepisami prawa oraz zasadami współżycia społecznego i sprawiedliwości.

Ślubuję, że powierzone mi obowiązki wypełniać będę bezstronnie, z najwyższą sumiennością i starannością, że będę strzec godności powierzonego mi stanowiska oraz dochowam tajemnicy prawnie chronionej."

Ślubowanie może być złożone z dodaniem zdania „Tak mi dopomóż Bóg".".

Art. 91. W ustawie z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne (Dz. U. z 2005 r. Nr 240, poz. 2027, z późn. zm.[27)]) w art. 7 ust. 2 otrzymuje brzmienie:

„2. Minister właściwy do spraw administracji publicznej w porozumieniu z Ministrem Obrony Narodowej określi, w drodze rozporządzenia, rodzaje materiałów geodezyjnych i kartograficznych, które podlegają ochronie zgodnie z przepisami o ochronie informacji niejawnych, uwzględniając przy tym potrzeby ochrony informacji niejawnych w działalności geodezyjnej i kartograficznej.".

Art. 92. W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277, z późn. zm.[28)]) wprowadza się następujące zmiany:

1) w art. 17 w ust. 1 pkt 8 otrzymuje brzmienie:

„8) w celu odparcia gwałtownego, bezpośredniego i bezprawnego zamachu na konwój ochraniający osoby, materiały zawierające informacje niejawne, pieniądze albo inne przedmioty wartościowe;";

2) w art. 27 ust. 1 otrzymuje brzmienie:

„1. Przed podjęciem służby policjant składa ślubowanie według następującej roty:

„Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków policjanta, ślubuję: służyć wiernie Narodowi, chronić ustanowiony Konstytucją Rzeczypospolitej Polskiej porządek prawny, strzec bezpieczeństwa Państwa i jego obywateli, nawet z narażeniem życia. Wykonując powierzone mi zadania, ślubuję pilnie przestrzegać prawa, dochować wierności konstytucyjnym organom Rzeczypospolitej Polskiej, przestrzegać dyscypliny służbowej oraz wykonywać rozkazy i polecenia przełożonych. Ślubuję strzec tajemnic związanych ze służbą, honoru, godności i dobrego imienia służby oraz przestrzegać zasad etyki zawodowej.”.”;

3) w art. 62 ust. 5 otrzymuje brzmienie:

„5. Informacje zawarte w oświadczeniu o stanie majątkowym stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone” określonej w przepisach o ochronie informacji niejawnych, chyba że policjant, który złożył oświadczenie, wyraził pisemną zgodę na ich ujawnienie, z zastrzeżeniem ust. 7.”;

4) w art. 132 w ust. 3 pkt 9 otrzymuje brzmienie:

„9) utrata materiału stanowiącego informacje niejawne.”.

Art. 93. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2005 r. Nr 234, poz. 1997, z późn. zm.[29)]) wprowadza się następujące zmiany:

1) art. 10d dodany w brzmieniu określonym w art. 3 pkt 2 ustawy z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. Nr 85, poz. 716) otrzymuje oznaczenie „Art. 10e.”;

2) w art. 24 w ust. 1 pkt 9 otrzymuje brzmienie:

„9) w celu odparcia gwałtownego, bezpośredniego i bezprawnego zamachu na konwój ochraniający osoby, materiały zawierające informacje niejawne, pieniądze albo inne przedmioty wartościowe;”;

3) w art. 33 ust. 1 otrzymuje brzmienie:

„1. Przed podjęciem służby funkcjonariusz Straży Granicznej składa ślubowanie według następującej roty:

„Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków funkcjonariusza Straży Granicznej – ślubuję służyć wiernie Narodowi Polskiemu, mając zawsze na względzie interes Państwa Polskiego.

Ślubuję stać nieugięcie na straży niepodległości i suwerenności oraz strzec nienaruszalności granicy państwowej Rzeczypospolitej Polskiej, nawet z narażeniem życia.

Ślubuję ściśle przestrzegać zasad Konstytucji Rzeczypospolitej Polskiej i obowiązującego porządku prawnego oraz ofiarnie i sumiennie wykonywać powierzone mi zadania, przestrzegać dyscypliny służbowej, wykonywać rozkazy i polecenia przełożonych, dochować tajemnic związanych ze służbą, strzec dobrego imienia służby, honoru i godności, a także przestrzegać zasad etyki funkcjonariusza Straży Granicznej.”.”;

4) w art. 91a ust. 5 otrzymuje brzmienie:

„5. Informacje zawarte w oświadczeniu o stanie majątkowym, z zastrzeżeniem ust. 6, stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone” określonej w przepisach o ochronie informacji niejawnych. Oświadczenie przechowuje się przez okres 10 lat.”.

Art. 94. W ustawie z dnia 14 lutego 1991 r. – Prawo o notariacie (Dz. U. z 2008 r. Nr 189, poz. 1158 oraz z 2009 r. Nr 37, poz. 286 i Nr 166, poz. 1317) w art. 15 § 1 otrzymuje brzmienie:

„§ 1. Przy powołaniu notariusz składa wobec Ministra Sprawiedliwości ślubowanie według następującej roty:

„Ślubuję uroczyście jako notariusz powierzone mi obowiązki wypełniać zgodnie z prawem i sumieniem, dochować tajemnicy zawodowej, w postępowaniu swym kierować się zasadami godności, honoru i uczciwości.”.”.

Art. 95. W ustawie z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska (Dz. U. z 2007 r. Nr 44, poz. 287, z późn. zm.[30)]) art. 10 otrzymuje brzmienie:

„Art. 10. Kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna, z zachowaniem przepisów o ochronie informacji niejawnych oraz o zakwaterowaniu sił zbrojnych, obowiązani są umożliwić inspektorowi przeprowadzenie kontroli, w szczególności umożliwić dokonanie czynności, o których mowa w art. 9 ust. 2.”.

Art. 96. W ustawie z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz. U. z 2000 r. Nr 14, poz. 176, z późn. zm.[31)]) art. 45a otrzymuje brzmienie:

„Art. 45a. Prezes Rady Ministrów określi, ze względu na ochronę informacji niejawnych, w drodze zarządzenia, odrębny tryb poboru podatku dochodowego, tryb składania informacji i zeznań podatkowych, a także dodatkowe zadania płatników związane z obowiązkiem rozliczania rocznego podatków, z uwzględnieniem wszystkich dodatkowych dochodów, wydatków, ulg, zwolnień i wyłączeń, mających wpływ na podstawę opodatkowania i wysokość podatku podatnika, innych niż określone w art. 6, 37, 38, 41, 42 i 45, ustalając jednocześnie dodatkowy zakres obowiązków płatnika, w szczególności prowadzenia postępowań i wydawania decyzji w sprawach podatkowych, w których właściwe są organy podatkowe.”.

Art. 97. W ustawie z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2009 r. Nr 12, poz. 68 i Nr 18, poz. 97) wprowadza się następujące zmiany:

1) w art. 30 ust. 1 otrzymuje brzmienie:

„1. Podejmując służbę w Państwowej Straży Pożarnej, strażak składa ślubowanie według następującej roty:

„Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków strażaka, uroczyście ślubuję być ofiarnym i mężnym w ratowaniu zagrożonego życia ludzkiego i wszelkiego mienia – nawet z narażeniem życia. Wykonując

powierzone mi zadania, ślubuję przestrzegać prawa, dyscypliny służbowej oraz wykonywać polecenia przełożonych. Ślubuję strzec tajemnic związanych ze służbą, a także honoru, godności i dobrego imienia służby oraz przestrzegać zasad etyki zawodowej.”.”;

2) w art. 57a ust. 9 otrzymuje brzmienie:

„9. Informacje zawarte w oświadczeniu o stanie majątkowym stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone” określonej w przepisach o ochronie informacji niejawnych, chyba że strażak, który złożył oświadczenie, wyraził pisemną zgodę na ich ujawnienie, z zastrzeżeniem ust. 11.”.

Art. 98. W ustawie z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65, z późn. zm.[32)]) wprowadza się następujące zmiany:

1) w art. 33 ust. 4 otrzymuje brzmienie:

„4. W żądaniu, o którym mowa w ust. 1 – 3, Generalny Inspektor Kontroli Skarbowej lub dyrektor urzędu kontroli skarbowej określa zakres informacji oraz termin ich przekazania; żądanie oznacza się klauzulą „Tajemnica skarbowa”, a jego przekazanie następuje w trybie przewidzianym dla dokumentów zawierających informacje niejawne o klauzuli „zastrzeżone” w rozumieniu przepisów o ochronie informacji niejawnych.”;

2) w art. 34a w ust. 1 pkt 7 otrzymuje brzmienie:

„7) Agencji Bezpieczeństwa Wewnętrznego, Służbie Kontrwywiadu Wojskowego, Agencji Wywiadu, Służbie Wywiadu Wojskowego, Centralnemu Biuru Antykorupcyjnemu, Policji, Żandarmerii Wojskowej, Straży Granicznej, Służbie Więziennej, Biuru Ochrony Rządu i ich upoważnionym pisemnie funkcjonariuszom lub żołnierzom w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych.”.

Art. 99. W ustawie z dnia 29 grudnia 1992 r. o radiofonii i telewizji (Dz. U. z 2004 r. Nr 253, poz. 2531, z późn. zm.[33)]) w art. 36 w ust. 2 pkt 1 otrzymuje brzmienie:

„1) zagrożenie interesów kultury narodowej, dobrych obyczajów i wychowania, bezpieczeństwa i obronności państwa oraz bezpieczeństwa informacji niejawnych;”.

Art. 100. W ustawie z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. Nr 111, poz. 535, z późn. zm.[34)]) w art. 50 w ust. 2 pkt 4 otrzymuje brzmienie:

„4) Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Policji, Żandarmerii Wojskowej, Straży Granicznej, Służby Więziennej, Biura Ochrony Rządu i ich upoważnionych pisemnie funkcjonariuszy lub żołnierzy w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych.”.

Art. 101. W ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.[35)]) wprowadza się następujące zmiany:

1) w art. 30 ust. 4 otrzymuje brzmienie:

„4. Kontrolę spraw lub dokumentów zakwalifikowanych jako „ściśle tajne” przeprowadza się na podstawie legitymacji służbowej i odrębnego upoważnienia wydanego przez Prezesa Najwyższej Izby Kontroli.”;

2) w art. 40 w ust. 2 pkt 1 otrzymuje brzmienie:

„1) tajemnicy prawnie chronionej, a kontroler nie posiada właściwego upoważnienia;”;

3) w art. 44 ust. 1 i 2 otrzymują brzmienie:

„1. Osoba obowiązana do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „zastrzeżone” lub „poufne” może być przesłuchana w charakterze świadka co do okoliczności, których dotyczy ten obowiązek.

2. Osoba obowiązana do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” może

być przesłuchana w charakterze świadka co do okoliczności, których dotyczy ten obowiązek, tylko po zwolnieniu od obowiązku zachowania tajemnicy, udzielonym na piśmie przez Prezesa Najwyższej Izby Kontroli.”.

Art. 102. W ustawie z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. z 2004 r. Nr 269, poz. 2681, z późn. zm.[36)]) w art. 22 ust. 3 otrzymuje brzmienie:

„3. Minister Finansów może, w drodze rozporządzenia, ze względu na ochronę informacji niejawnych, uregulować odrębnie tryb nadawania numerów identyfikacji podatkowej oraz warunki posługiwania się tymi numerami.”.

Art. 103. W ustawie z dnia 26 kwietnia 1996 r. o Służbie Więziennej (Dz. U. z 2002 r. Nr 207, poz. 1761, z późn. zm.[37)]) wprowadza się następujące zmiany:

1) w art. 20 pkt 6 otrzymuje brzmienie:

„6) w celu odparcia bezpośredniego zamachu na konwój ochraniający osoby, broń palną, amunicję, materiały zawierające informacje niejawne, pieniądze lub inne przedmioty wartościowe;”;

2) w art. 27 ust. 1 otrzymuje brzmienie:

„1. Przed podjęciem służby funkcjonariusz składa ślubowanie według następującej roty:

„Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków funkcjonariusza Służby Więziennej ślubuję uroczyście: dochować wierności konstytucyjnym organom Rzeczypospolitej Polskiej, przestrzegać prawa, kierować się zasadami humanizmu i poszanowania godności ludzkiej, stawiając siebie i swoje siły do dyspozycji służby, przyczyniać się do realizacji zadań Służby Więziennej.

Ślubuję: przestrzegać dyscypliny służbowej, tajemnicy prawnie chronionej, rzetelnie i sumiennie wykonywać powierzone mi

zadania i polecenia przełożonych, dbać o honor i dobre imię służby oraz przestrzegać zasad etyki zawodowej.”.”.

Art. 104. W ustawie z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora (Dz. U. z 2003 r. Nr 221, poz. 2199, z późn. zm.[38)]) art. 19 otrzymuje brzmienie:

„Art. 19. 1. W wykonywaniu mandatu poseł lub senator ma prawo, jeżeli nie narusza dóbr osobistych innych osób, do uzyskiwania informacji i materiałów oraz wglądu w działalność organów administracji rządowej i samorządu terytorialnego, a także spółek z udziałem Skarbu Państwa oraz zakładów i przedsiębiorstw państwowych i samorządowych, z zachowaniem przepisów o tajemnicy prawnie chronionej.

2. Zasady i tryb udostępniania posłom i senatorom informacji niejawnych określają przepisy o ochronie informacji niejawnych.”.

Art. 105. W ustawie z dnia 21 czerwca 1996 r. o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra (Dz. U. Nr 106, poz. 491, z późn. zm.[39)]) art. 9 otrzymuje brzmienie:

„Art. 9. 1. Minister właściwy do spraw wewnętrznych może zezwalać pracownikom, policjantom, strażakom, funkcjonariuszom Straży Granicznej lub funkcjonariuszom Biura Ochrony Rządu na udzielenie wiadomości stanowiącej informację niejawną określonej osobie lub instytucji. Zezwolenie to nie może jednak dotyczyć sytuacji, o której mowa w art. 21 ustawy wymienionej w art. 8 ust. 2 oraz art. 9a ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2005 r. Nr 234, poz. 1997 oraz z 2006 r. Nr 104, poz. 708 i 711 i Nr 170, poz. 1218), z wyjątkiem dokumentów i materiałów, które sąd okręgowy, prokurator Biura Lustracyjnego lub oddziałowego biura lustracyjnego Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni

przeciwko Narodowi Polskiemu uzna za niezbędne w związku z wykonywaniem ich zadań określonych w ustawie z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944 – 1990 oraz treści tych dokumentów oraz ustawie z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu.

2. W razie odmowy zwolnienia pracownika, policjanta, strażaka, funkcjonariusza Straży Granicznej lub funkcjonariusza Biura Ochrony Rządu, lub osoby udzielającej im pomocy w wykonywaniu czynności operacyjno–rozpoznawczych od obowiązku zachowania tajemnicy albo odmowy zezwolenia na udostępnienie dokumentów lub materiałów zawierających informacje niejawne o klauzuli tajności „tajne" lub „ściśle tajne" pomimo żądania prokuratora lub sądu, zgłoszonego w związku z postępowaniem karnym o przestępstwo wymienione w art. 109 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny lub o zbrodnię godzącą w życie ludzkie albo o występek przeciwko życiu i zdrowiu, gdy jego następstwem była śmierć człowieka, Minister Spraw Wewnętrznych i Administracji przedstawia żądane dokumenty i materiały oraz wyjaśnienia Pierwszemu Prezesowi Sądu Najwyższego. Jeżeli Pierwszy Prezes Sądu Najwyższego stwierdzi, że uwzględnienie żądania prokuratora lub sądu jest konieczne do prawidłowości postępowania karnego, Minister Spraw Wewnętrznych i Administracji jest obowiązany zwolnić od zachowania tajemnicy lub udostępnić dokumenty i materiały objęte tajemnicą.".

Art. 106. W ustawie z dnia 30 sierpnia 1996 r. o komercjalizacji i prywatyzacji (Dz. U. z 2002 r. Nr 171, poz. 1397, z późn. zm.[40)]) w art. 62 ust. 1 otrzymuje brzmienie:

„1. Informacje uzyskane przy opracowaniu analiz, o których mowa w art. 32 ust. 1 oraz w art. 42 ust. 1, stanowią tajemnicę podlegającą ochronie na zasadach określonych przepisami o ochronie informacji niejawnych.”.

Art. 107. W ustawie z dnia 6 czerwca 1997 r.– Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.[41)]) wprowadza się następujące zmiany:

1) w art. 265 § 1 otrzymuje brzmienie:

„§ 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „tajne” lub „ściśle tajne”, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.”;

2) w art. 266 § 2 otrzymuje brzmienie:

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

Art. 108. W ustawie z dnia 6 czerwca 1997 r.– Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.[42)]) wprowadza się następujące zmiany:

1) w art. 156 § 4 otrzymuje brzmienie:

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

2) w art. 179 § 1 otrzymuje brzmienie:

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

3) w art. 180 § 1 otrzymuje brzmienie:

„§ 1. Osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „zastrzeżone” lub „poufne” lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd lub prokurator zwolni te osoby od obowiązku zachowania tajemnicy, jeżeli ustawy szczególne nie stanowią inaczej.”;

4) w art. 181 § 2 otrzymuje brzmienie:

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

5) w art. 184:

a) § 1 otrzymuje brzmienie:

„§ 1. Jeżeli zachodzi uzasadniona obawa niebezpieczeństwa dla życia, zdrowia, wolności albo mienia w znacznych rozmiarach świadka lub osoby dla niego najbliższej, sąd, a w postępowaniu przygotowawczym prokurator, może wydać postanowienie o zachowaniu w tajemnicy okoliczności umożliwiających ujawnienie tożsamości świadka, w tym danych osobowych, jeżeli nie mają one znaczenia dla rozstrzygnięcia w sprawie. Postępowanie w tym zakresie toczy się bez udziału stron i objęte jest tajemnicą jako informacja niejawna o klauzuli tajności

„tajne” lub „ściśle tajne”. W postanowieniu pomija się okoliczności, o których mowa w zdaniu pierwszym.”,

b) § 5 otrzymuje brzmienie:

„§ 5. Na postanowienie w sprawie zachowania w tajemnicy okoliczności, o których mowa w § 1, świadkowi i oskarżonemu, a w postępowaniu przed sądem także prokuratorowi, przysługuje w terminie 3 dni zażalenie. Zażalenie na postanowienie prokuratora rozpoznaje sąd właściwy do rozpoznania sprawy. Postępowanie dotyczące zażalenia toczy się bez udziału stron i jest objęte tajemnicą jako informacja niejawna o klauzuli tajności „tajne” lub „ściśle tajne”.”;

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

„§ 1. Jeżeli kierownik instytucji państwowej lub samorządowej albo też osoba, u której dokonano zatrzymania rzeczy lub u której przeprowadza się przeszukanie, oświadczy, że wydane lub znalezione przy przeszukaniu pismo lub inny dokument zawiera informacje niejawne lub wiadomości objęte tajemnicą zawodową lub inną tajemnicą prawnie chronioną albo ma charakter osobisty, organ przeprowadzający czynność przekazuje niezwłocznie pismo lub inny dokument bez jego odczytania prokuratorowi lub sądowi w opieczętowanym opakowaniu.

§ 2. Tryb wskazany w § 1 nie obowiązuje w stosunku do pism lub innych dokumentów, które zawierają informacje niejawne o klauzuli „zastrzeżone” lub „poufne” albo dotyczą tajemnicy zawodowej lub innej tajemnicy prawnie chronionej, jeżeli ich posiadaczem jest osoba podejrzana o popełnienie przestępstwa, i do pism lub innych dokumentów o charakterze osobistym, których jest ona posiadaczem, autorem lub adresatem.”;

7) art. 226 otrzymuje brzmienie:

„Art. 226. W kwestii wykorzystania dokumentów zawierających informacje niejawne lub tajemnicę zawodową, jako dowodów w postępowaniu karnym, stosuje się

odpowiednio zakazy i ograniczenia określone w art. 178 – 181. Jednakże w postępowaniu przygotowawczym o wykorzystaniu, jako dowodów, dokumentów zawierających tajemnicę lekarską decyduje prokurator.”;

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

„10) szpiegostwa lub ujawnienia informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne”;”;

9) w art. 338 § 3 otrzymuje brzmienie:

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

10) w art. 361 § 2 otrzymuje brzmienie:

„§ 2. Przepisu § 1 nie stosuje się, jeżeli zachodzi obawa ujawnienia informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne”.”;

11) w art. 448 § 2 otrzymuje brzmienie:

„§ 2. W wypadku wniesienia apelacji przez prokuratora, obrońcę lub pełnomocnika dołącza się do zawiadomienia odpis apelacji strony przeciwnej, chyba że w sprawie była wyłączona jawność rozprawy ze względu na ochronę informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne”.”.

Art. 109. W ustawie z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. Nr 90, poz. 557, z późn. zm.[43)]) w art. 11 § 1 otrzymuje brzmienie:

„§ 1. Sąd, kierując orzeczenie do wykonania, przesyła jego odpis lub wyciąg, ze wzmianką o wykonalności, a w wypadku orzeczenia prawomocnego – z datą jego uprawomocnienia się, odpowiedniemu organowi powołanemu do wykonywania orzeczenia. Sąd przesyła dyrektorowi zakładu karnego lub aresztu

śledczego orzeczenie wraz z uzasadnieniem, jeżeli zostało sporządzone i nie zawiera informacji niejawnych o klauzuli tajności „tajne" lub „ściśle tajne", oraz dane zawierające imię, nazwisko i adres pokrzywdzonego.".

Art. 110. W ustawie z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2005 r. Nr 108, poz. 908, z późn. zm.[44)]) w art. 73 ust. 3a otrzymuje brzmienie:

„3a. Producent blankietów dowodów rejestracyjnych, pozwoleń czasowych, nalepek kontrolnych i innych dokumentów wymaganych do rejestracji pojazdów, a także starostowie przekazują odpłatnie wojewodzie mazowieckiemu odpowiednio: blankiety dowodów rejestracyjnych, pozwoleń czasowych, nalepek kontrolnych i innych dokumentów wymaganych do rejestracji pojazdów, a także zalegalizowane tablice rejestracyjne niezbędne do rejestracji, o której mowa w art. 76 ust. 4. Informacje dotyczące przekazanych blankietów dowodów rejestracyjnych, pozwoleń czasowych, nalepek kontrolnych i innych dokumentów wymaganych do rejestracji oraz tablic rejestracyjnych podlegają ochronie zgodnie z przepisami o ochronie informacji niejawnych o klauzuli tajności „tajne" lub „ściśle tajne".".

Art. 111. W ustawie z dnia 25 czerwca 1997 r. o świadku koronnym (Dz. U. z 2007 r. Nr 36, poz. 232) art. 23 otrzymuje brzmienie:

„Art. 23. Ochronie zgodnie z przepisami o ochronie informacji niejawnych podlegają:

1) przebieg i treść czynności, o których mowa w art. 3, 5 i 5a, do chwili uprawomocnienia się postanowienia sądu o dopuszczeniu dowodu z zeznań świadka koronnego;
2) okoliczności dotyczące ochrony lub pomocy, o których mowa w art. 14 – 20.".

Art. 112. W ustawie z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym (Dz. U. Nr 102, poz. 643, z późn. zm.[45)]) art. 23 otrzymuje brzmienie:

„Art. 23. 1. Rozprawy Trybunału są jawne, jeżeli przepis szczególny nie stanowi inaczej. Przewodniczący składu orzekającego może wyłączyć jawność ze względu na bezpieczeństwo państwa lub ochronę informacji niejawnych o klauzuli tajności „tajne" lub „ściśle tajne".

2. Sędziowie Trybunału są upoważnieni do dostępu do informacji niejawnych związanych z rozpoznawaną przez Trybunał sprawą.

3. Świadek lub biegły może być przesłuchany co do okoliczności stanowiących informację niejawną o klauzuli tajności „tajne" lub „ściśle tajne" po zwolnieniu przez uprawniony organ od obowiązku zachowania tajemnicy. Odmowa zgody może być uzasadniona jedynie ważnym interesem państwa.

4. Świadek lub biegły nie korzysta z prawa odmowy złożenia zeznań, o którym mowa w ust. 3, jeżeli Trybunał uzna taką odmowę za nieuzasadnioną.".

Art. 113. W ustawie z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych (Dz. U. z 2007 r. Nr 226, poz. 1676, z późn. zm.[46)]) w art. 28 § 5 otrzymuje brzmienie:

„§ 5. Informacje zawarte w oświadczeniu o stanie majątkowym stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone" określonej w przepisach o ochronie informacji niejawnych, chyba że sędzia, który złożył oświadczenie, wyraził pisemną zgodę na ich ujawnienie. W szczególnie uzasadnionych przypadkach podmiot uprawniony, zgodnie z § 2 lub 3, do odebrania oświadczenia może je ujawnić pomimo braku zgody składającego oświadczenie. Oświadczenie przechowuje się przez 6 lat.".

Art. 114. W ustawie z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2006 r. Nr 216, poz. 1584 oraz z 2008 r. Nr 223, poz. 1458) wprowadza się następujące zmiany:

1) w art. 8 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 o ochronie informacji niejawnych.";

2) w art. 10 ust. 3 otrzymuje brzmienie:

„3. Informacje zawarte w oświadczeniu o stanie majątkowym stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone" określonej w przepisach o ochronie informacji niejawnych, chyba że osoba, która złożyła oświadczenie, wyraziła pisemną zgodę na ich ujawnienie. W szczególnie uzasadnionych przypadkach osoba uprawniona, zgodnie z ust. 4, 5 lub 6, do odebrania oświadczenia może je ujawnić pomimo braku zgody składającego oświadczenie. Oświadczenie przechowuje się przez 6 lat.".

Art. 115. W ustawie z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych (Dz. U. z 2004 r. Nr 159, poz. 1667, z późn. zm.[47)]) w art. 41a ust. 5 otrzymuje brzmienie:

„5. Informacje zawarte w oświadczeniu o stanie majątkowym stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone" określonej w przepisach o ochronie informacji niejawnych, chyba że osoba, która złożyła oświadczenie, wyraziła pisemną zgodę na ich ujawnienie. Oświadczenie przechowuje się przez okres 6 lat.".

Art. 116. W ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. Nr 123, poz. 779, z późn. zm.[48)]) w art. 27 pkt 3 otrzymuje brzmienie:

„3) zachowanie tajemnicy prawnie chronionej,".

Art. 117. W ustawie z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji (Dz. U. z 2006 r. Nr 167, poz. 1191, z późn. zm.[49)]) wprowadza się następujące zmiany:

1) w art. 14 ust. 2 otrzymuje brzmienie:

„2. W terminie 14 dni od dnia otrzymania zawiadomienia, o którym mowa w ust. 1, prezes sądu apelacyjnego odbiera od komornika ślubowanie według następującej roty:

„Ślubuję uroczyście jako komornik powierzone mi obowiązki wypełniać zgodnie z prawem i sumieniem, dochować tajemnicy prawnie chronionej, w postępowaniu swym kierować się zasadami uczciwości, godności i honoru”.”;

2) w art. 16 ust. 6 otrzymuje brzmienie:

„6. Informacje zawarte w oświadczeniu o stanie majątkowym stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone” określonej w przepisach o ochronie informacji niejawnych, chyba że komornik, który złożył oświadczenie, wyraził pisemną zgodę na ich ujawnienie. W szczególnie uzasadnionych przypadkach podmiot uprawniony, zgodnie z ust. 3 lub 4, do odebrania oświadczenia może je ujawnić pomimo braku zgody składającego oświadczenie. Oświadczenie przechowuje się przez 6 lat.”.

Art. 118. W ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2005 r. Nr 8, poz. 60, z późn. zm.[50)]) wprowadza się następujące zmiany:

1) art. 13a otrzymuje brzmienie:

„Art. 13a. Rada Ministrów może, w drodze rozporządzenia, nadać uprawnienia organów podatkowych:

1) Szefowi Agencji Wywiadu,
2) Szefowi Agencji Bezpieczeństwa Wewnętrznego,
3) Szefowi Centralnego Biura Antykorupcyjnego,
4) Szefowi Służby Wywiadu Wojskowego,
5) Szefowi Służby Kontrwywiadu Wojskowego

– jeżeli jest to uzasadnione ochroną informacji niejawnych i wymogami bezpieczeństwa państwa.”;

2) w art. 82 § 4 otrzymuje brzmienie:

„§ 4. Żądanie, o którym mowa w § 3, oznacza się klauzulą: „Tajemnica skarbowa”, a jego przekazanie następuje w trybie przewidzianym dla dokumentów zawierających informacje niejawne o klauzuli „zastrzeżone”.”;

3) w art. 179 § 1 otrzymuje brzmienie:

„§ 1. Przepisów art. 178 nie stosuje się do znajdujących się w aktach sprawy dokumentów zawierających informacje niejawne, a także do innych dokumentów, które organ podatkowy wyłączy z akt sprawy ze względu na interes publiczny.”;

4) w art. 195 pkt 2 otrzymuje brzmienie:

„2) osoby obowiązane do zachowania w tajemnicy informacji niejawnych na okoliczności objęte tajemnicą, jeżeli nie zostały, w trybie określonym obowiązującymi przepisami, zwolnione od obowiązku zachowania tej tajemnicy;”;

5) w art. 196 § 4 otrzymuje brzmienie:

„§ 4. Minister właściwy do spraw finansów publicznych w porozumieniu z Ministrem Sprawiedliwości określi, w drodze rozporządzenia, sposób sporządzania oraz przechowywania protokołów zeznań obejmujących okoliczności, na które rozciąga się obowiązek ochrony informacji niejawnych lub dochowania tajemnicy zawodowej.”;

6) w art. 286 § 3 otrzymuje brzmienie:

„§ 3. Przeglądanie akt postępowania przygotowawczego i sądowego, akt spraw sądowych, a także dokumentów zawierających informacje niejawne lub stanowiące tajemnicę zawodową oraz sporządzanie z nich odpisów i notatek następuje z zachowaniem właściwych przepisów.”;

7) w art. 296 § 2 otrzymuje brzmienie:

„§ 2. Informacje, o których mowa w § 1, po ich wykorzystaniu są wyłączane z akt sprawy i przechowywane w kasach pancernych, szafach pancernych lub w urządzeniach służących

ochronie informacji niejawnych o klauzuli „poufne", którym na podstawie odrębnych przepisów przyznano certyfikaty lub świadectwa kwalifikacyjne. Adnotacji o wyłączeniu dokonuje się w aktach sprawy.";

8) w art. 297 w § 1 pkt 7 otrzymuje brzmienie:

„7) Agencji Bezpieczeństwa Wewnętrznego, Służbie Kontrwywiadu Wojskowego, Agencji Wywiadu, Służbie Wywiadu Wojskowego, Centralnemu Biuru Antykorupcyjnemu, Policji, Żandarmerii Wojskowej, Straży Granicznej, Służbie Więziennej, Biuru Ochrony Rządu i ich posiadającym pisemne upoważnienie funkcjonariuszom lub żołnierzom w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych;";

9) w art. 298 pkt 5a otrzymuje brzmienie:

„5a) Agencji Bezpieczeństwa Wewnętrznego, Służbie Kontrwywiadu Wojskowego, Agencji Wywiadu, Służbie Wywiadu Wojskowego, Centralnemu Biuru Antykorupcyjnemu, Policji, Żandarmerii Wojskowej, Straży Granicznej, Służbie Więziennej, Biuru Ochrony Rządu i ich posiadającym pisemne upoważnienie funkcjonariuszom lub żołnierzom w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych,".

Art. 119. W ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665, z późn. zm.[51)]) wprowadza się następujące zmiany:

1) w art. 105 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, Biura Ochrony Rządu i ich posiadających pisemne upoważnienie funkcjonariuszy lub żołnierzy w zakresie

niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych,”;

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, Biura Ochrony Rządu w związku z postępowaniami sprawdzającymi prowadzonymi na podstawie przepisów o ochronie informacji niejawnych;”.

Art. 120. W ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.[52)]) wprowadza się następujące zmiany:

1) w art. 30 pkt 1 otrzymuje brzmienie:

„1) ujawnienie wiadomości zawierających informacje niejawne,”;

2) w art. 32 w ust. 1 pkt 4 otrzymuje brzmienie:

„4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej,”;

3) w art. 43 w ust. 1 pkt 1 otrzymuje brzmienie:

„1) zawierających informacje niejawne,”.

Art. 121. W ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2007 r. Nr 11, poz. 74, z późn. zm.[53)]) art. 79 otrzymuje brzmienie:

„Art. 79. 1. Indywidualne dane zawarte na kontach ubezpieczonych i kontach płatników składek, a także w rejestrach prowadzonych przez Zakład oraz dane źródłowe będące podstawą zapisów na tych kontach i w rejestrach stanowią tajemnicę prawnie chronioną Zakładu. Do przestrzegania tej tajemnicy obowiązani są:

1) pracownicy Zakładu;

2) członkowie Rady Nadzorczej Zakładu.

2. Przepis ust. 1 stosuje się również do indywidualnych danych osób, przetwarzanych w Zakładzie w zakresie

przyznawania, ustalania i wypłaty świadczeń z ubezpieczeń społecznych, a także świadczeń finansowanych z budżetu państwa oraz o dokonanych wypłatach, w związku z realizacją zadań zleconych Zakładowi na podstawie odrębnych przepisów.”.

Art. 122. W ustawie z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (Dz. U. z 2007 r. Nr 63, poz. 424, późn. zm.[54)]) wprowadza się następujące zmiany:

1) w art. 11 ust. 2b otrzymuje brzmienie:

„2b. Na stanowisko Prezesa Instytutu Pamięci nie może być powołana również osoba, której działalność związana z dostępem do informacji niejawnych lub objęta ochroną jako informacja niejawna uniemożliwia szczegółowe przedstawienie informacji o przebiegu swojej służby, pracy lub współpracy.”;

2) w art. 22 ust. 1 otrzymuje brzmienie:

„1. Prezes Instytutu Pamięci może, w szczególnie uzasadnionych wypadkach, zezwolić na ujawnienie wiadomości stanowiącej informację niejawną oraz na udostępnienie dokumentów lub materiałów zawierających informacje niejawne określonej osobie lub instytucji, jeżeli zachowanie tajemnicy uniemożliwiałoby wykonanie wskazanych w ustawie zadań Instytutu Pamięci.”;

3) w art. 39 ust. 4 otrzymuje brzmienie:

„4. Zastrzeżenie podlega ochronie zgodnie z przepisami o ochronie informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne”.”.

Art. 123. W ustawie z dnia 18 grudnia 1998 r. o pracownikach sądów i prokuratury (Dz. U. Nr 162, poz. 1125, z późn. zm.[55)]) w art. 6 pkt 3 otrzymuje brzmienie:

„3) dochowywać tajemnicy prawnie chronionej;”.

Art. 124. W ustawie z dnia 21 stycznia 1999 r. o sejmowej komisji śledczej (Dz. U. z 2009 r. Nr 151, poz. 1218) wprowadza się następujące zmiany:

1) w art. 11e ust. 1 otrzymuje brzmienie:

„1. Osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” mogą być przesłuchane co do okoliczności, na które rozciąga się ten obowiązek, tylko po zwolnieniu ich od obowiązku zachowania tajemnicy przez właściwy organ.”;

2) art. 11f otrzymuje brzmienie:

„Art. 11f. Osoby obowiązane do zachowania tajemnicy prawnie chronionej innej niż informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne” mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że komisja zwolni je od obowiązku zachowania tajemnicy, z zastrzeżeniem przepisu art. 11g.”;

3) w art. 11h ust. 2 otrzymuje brzmienie:

„2. Wiadomości uzyskane w toku przesłuchań, o których mowa w art. 11f i art. 11g ust. 1, stanowią tajemnicę prawnie chronioną.”.

Art. 125. W ustawie z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka (Dz. U. Nr 6, poz. 69 oraz z 2008 r. Nr 214, poz. 1345) art. 5 otrzymuje brzmienie:

„Art. 5. Przed przystąpieniem do wykonywania obowiązków Rzecznik składa przed Sejmem następujące ślubowanie:

„Ślubuję uroczyście, że przy wykonywaniu powierzonych mi obowiązków Rzecznika Praw Dziecka dochowam wierności Konstytucji Rzeczypospolitej Polskiej, będę strzec praw dziecka, kierując się przepisami prawa, dobrem dziecka i dobrem rodziny. Ślubuję, że powierzone mi obowiązki będę wypełniać bezstronnie, z najwyższą sumiennością i starannością, że będę strzec godności powierzonego mi stanowiska oraz dochowam tajemnicy prawnie chronionej.”.

Ślubowanie może być złożone z dodaniem zdania „Tak mi dopomóż Bóg”.”.

Art. 126. W ustawie z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej (Dz. U. z 2003 r. Nr 119, poz. 1117, z późn. zm.[56)]) wprowadza się następujące zmiany:

1) w art. 57 ust. 1 otrzymuje brzmienie:

„1. Wynalazek tajny stanowi tajemnicę prawnie chronioną.”;

2) w art. 268 ust. 4 otrzymuje brzmienie:

„4. Przy powołaniu ekspert składa ślubowanie wobec Prezesa Urzędu Patentowego według następującej roty: „Ślubuję uroczyście na powierzonym mi stanowisku eksperta sumiennie wykonywać zadania, orzekać bezstronnie i zgodnie z przepisami prawa, dochować tajemnicy prawnie chronionej, a w postępowaniu kierować się zasadami godności i uczciwości.”.”;

3) w art. 270 w ust. 1 pkt 4 otrzymuje brzmienie:

„4) dochowywać tajemnicy prawnie chronionej;”.

Art. 127. W ustawie z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2005 r. Nr 121, poz. 1019, z późn. zm.[57)]) w art. 54 w ust. 1 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, Biura Ochrony Rządu i ich upoważnionych pisemnie funkcjonariuszy lub żołnierzy – w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych;”.

Art. 128. W ustawie z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2003 r. Nr 153, poz. 1505, z późn. zm.[58)]) wprowadza się następujące zmiany:

1) w art. 22 ust. 1 otrzymuje brzmienie:

„1. Na żądanie kontrolera instytucje obowiązane są zobowiązane do przedkładania wszelkich dokumentów i materiałów niezbędnych do przeprowadzenia kontroli, o której mowa w art. 21 ust. 1, z wyłączeniem dokumentów i materiałów zawierających informacje niejawne.”;

2) art. 29 otrzymuje brzmienie:

„Art. 29. Do ujawnienia Generalnemu Inspektorowi wszelkich informacji w trybie i zakresie przewidzianym ustawą nie stosuje się przepisów ograniczających udostępnianie danych objętych tajemnicą, z wyjątkiem informacji niejawnych.”.

Art. 129. W ustawie z dnia 15 grudnia 2000 r. o Inspekcji Handlowej (Dz. U. z 2009 r. Nr 151, poz. 1219) w art. 16 ust. 5 otrzymuje brzmienie:

„5. Uzyskane w trakcie kontroli informacje dotyczące stosowanej przez kontrolowanego technologii lub stanowiące tajemnicę handlową są prawnie chronione; nie dotyczy to informacji, których ujawnienie jest niezbędne ze względu na konieczność usunięcia zagrożeń związanych z produktem lub usługą.”.

Art. 130. W ustawie z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2006 r. Nr 123, poz. 857, z późn. zm.[59)]) art. 47b otrzymuje brzmienie:

„Art. 47b. Informacje, o których mowa w art. 47a ust. 2, podlegają ochronie zgodnie z przepisami o ochronie informacji niejawnych.”.

Art. 131. W ustawie z dnia 11 stycznia 2001 r. o substancjach i preparatach chemicznych (Dz. U. z 2009 r. Nr 152, poz. 1222) w art. 23 ust. 5 otrzymuje brzmienie:

„5. Inspektor może zażądać ujawnienia szczegółowego składu chemicznego preparatu. Informacja taka stanowi tajemnicę prawnie chronioną i może zostać wykorzystana wyłącznie w celach medycznych do zapobiegania i postępowania leczniczego.”.

Art. 132. W ustawie z dnia 16 marca 2001 r. o Biurze Ochrony Rządu (Dz. U. z 2004 r. Nr 163, poz. 1712, z późn. zm.[60)]) art. 22 otrzymuje brzmienie:

„Art. 22. Przed podjęciem służby funkcjonariusz składa ślubowanie według następującej roty:

„Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków funkcjonariusza Biura Ochrony

Rządu ślubuję służyć wiernie Narodowi Polskiemu, mając zawsze na względzie interes Państwa Polskiego, nawet z narażeniem własnego życia.

Ślubuję przestrzegać Konstytucji Rzeczypospolitej Polskiej i obowiązującego porządku prawnego oraz ofiarnie i sumiennie wykonywać powierzone mi obowiązki, przestrzegać dyscypliny służbowej, wykonywać polecenia przełożonych, dochować tajemnic związanych ze służbą, strzec dobrego imienia służby, honoru i godności.". Funkcjonariusz składający ślubowanie, po jego zakończeniu, może dodać wyrazy „Tak mi dopomóż Bóg".".

Art. 133. W ustawie z dnia 22 czerwca 2001 r. o wykonywaniu Konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów (Dz. U. Nr 76, poz. 812) art. 22 otrzymuje brzmienie:

„Art. 22. 1. Informacje uzyskane w związku z realizacją postanowień Konwencji, oznaczone klauzulą „OPCW restricted", podlegają ochronie i są udostępniane na zasadach określonych w przepisach o ochronie informacji niejawnych, dla informacji niejawnych o klauzuli tajności „zastrzeżone".

2. Informacje uzyskane w związku z realizacją postanowień Konwencji, oznaczone klauzulą „OPCW protected", podlegają ochronie i są udostępniane na zasadach określonych w przepisach, o których mowa w ust. 1, dla informacji niejawnych o klauzuli tajności „poufne".

3. Informacje uzyskane w związku z realizacją postanowień Konwencji, oznaczone klauzulą „OPCW highly protected", podlegają ochronie i są udostępniane na zasadach określonych w przepisach, o których mowa w ust. 1, dla informacji niejawnych o klauzuli tajności „tajne".

4. Informacje uzyskane od podmiotów i przedsiębiorców, o których mowa w art. 2, w związku z obowiązkiem ustanowionym w art. 14, oraz oznaczone odpowiednimi

klauzulami, podlegają ochronie i są udostępniane na zasadach określonych w przepisach, o których mowa w ust. 1, odpowiednio do przyznanej klauzuli tajności.”.

Art. 134. W ustawie z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (Dz. U. z 2006 r. Nr 216, poz. 1585, z późn. zm.[61)]) wprowadza się następujące zmiany:

1) w art. 6 pkt 4 otrzymuje brzmienie:

„4) zapewnienie bezpieczeństwa gromadzonym i przetwarzanym w Centrum informacjom kryminalnym, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz przepisami ustawy z dnia …… o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. Nr …., poz. ….);”;

2) w art. 16 ust. 1 otrzymuje brzmienie:

„1. Informacje kryminalne gromadzone, przetwarzane i przekazywane podlegają ochronie określonej w przepisach o ochronie informacji niejawnych.”;

3) w art. 40 ust. 2 otrzymuje brzmienie:

„2. Przekazanie informacji za granicę do kraju, który nie daje gwarancji, o których mowa w ust. 1, może nastąpić jedynie po zasięgnięciu opinii ministra właściwego do spraw zagranicznych oraz krajowej władzy bezpieczeństwa w rozumieniu przepisów o ochronie informacji niejawnych.”.

Art. 135. W ustawie z dnia 18 lipca 2001 r. – Prawo wodne (Dz. U. z 2005 r. Nr 239, poz. 2019, z późn. zm.[62)]) art. 158 otrzymuje brzmienie:

„Art. 158. Kontrolowany, z zachowaniem przepisów o ochronie informacji niejawnych oraz o zakwaterowaniu sił zbrojnych, jest obowiązany umożliwić inspektorowi przeprowadzenie kontroli, w szczególności umożliwić dokonanie czynności, o których mowa w art. 157 ust. 2.”.

Art. 136. W ustawie z dnia 27 lipca 2001 r. o kuratorach sądowych (Dz. U. Nr 98, poz. 1071, z późn. zm.[63)]) art. 74 otrzymuje brzmienie:

„Art. 74. Przed podjęciem obowiązków aplikant kuratorski składa ślubowanie wobec prezesa sądu okręgowego i kuratora okręgowego według następującej roty:

„Ślubuję uroczyście sumiennie wypełniać obowiązki aplikanta kuratorskiego, w postępowaniu kierować się zasadami godności i uczciwości oraz dochować tajemnicy prawnie chronionej.”.”.

Art. 137. W ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. Nr 98, poz. 1070, z późn. zm.[64)]) wprowadza się następujące zmiany:

1) art. 66 otrzymuje brzmienie:

„Art. 66. Przy powołaniu sędzia składa ślubowanie wobec Prezydenta Rzeczypospolitej Polskiej według następującej roty:

„Ślubuję uroczyście jako sędzia sądu powszechnego służyć wiernie Rzeczypospolitej Polskiej, stać na straży prawa, obowiązki sędziego wypełniać sumiennie, sprawiedliwość wymierzać zgodnie z przepisami prawa, bezstronnie według mego sumienia, dochować tajemnicy prawnie chronionej, a w postępowaniu kierować się zasadami godności i uczciwości.”; składający ślubowanie może dodać na końcu zwrot: „Tak mi dopomóż Bóg”.”;

2) w art. 87 § 6 otrzymuje brzmienie:

„§ 6. Informacje zawarte w oświadczeniu, o którym mowa w § 1, stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone” określonej w przepisach o ochronie informacji niejawnych, chyba że sędzia, który złożył oświadczenie, wyraził pisemną zgodę na ich ujawnienie. W szczególnie uzasadnionych przypadkach podmiot uprawniony, zgodnie z § 2 lub § 4, do odebrania oświadczenia może je ujawnić pomimo braku zgody składającego oświadczenie.”;

3) w art. 150 § 4 otrzymuje brzmienie:

„§ 4. Przed podjęciem pracy referendarz sądowy składa ślubowanie wobec prezesa sądu okręgowego według następującej roty: „Ślubuję uroczyście na powierzonym mi stanowisku referendarza służyć wiernie Rzeczypospolitej Polskiej, sumiennie i starannie wykonywać obowiązki urzędowe, przestrzegać prawa, kierować się zasadami godności i uczciwości oraz dochować tajemnicy prawnie chronionej.”; składający ślubowanie może dodać zwrot: „Tak mi dopomóż Bóg”.”.

Art. 138. W ustawie z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2008 r. Nr 133, poz. 848, z późn. zm.[65)]) wprowadza się następujące zmiany:

1) w art. 41 § 2 i 3 otrzymują brzmienie:

„§ 2. Osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” mogą być przesłuchane co do okoliczności, na które rozciąga się ten obowiązek, tylko po zwolnieniu tych osób od obowiązku zachowania tajemnicy przez uprawniony organ przełożony.

§ 3. Osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „zastrzeżone” lub „poufne” lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd zwolni te osoby od obowiązku zachowania tajemnicy, jeżeli ustawy szczególne nie stanowią inaczej. Na postanowienie sądu służy zażalenie.”;

2) w art. 70 § 3 otrzymuje brzmienie:

„§ 3. W razie wyłączenia jawności na rozprawie mogą być obecni, poza osobami biorącymi udział w postępowaniu, po jednej osobie wskazanej przez każdą ze stron, chyba że zachodzi obawa ujawnienia informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne”. Sąd może zezwolić poszczególnym

osobom na obecność na rozprawie prowadzonej z wyłączeniem jawności.”.

Art. 139. W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353, z późn. zm.[66)]) wprowadza się następujące zmiany:

1) w art. 31 w ust. 1 pkt 13 otrzymuje brzmienie:

„13) bezprawnego ujawnienia lub wykorzystania informacji niejawnych o klauzuli tajności „tajne” i „ściśle tajne”;”;

2) w art. 36 ust. 3 i 4 otrzymują brzmienie:

„3. W razie odmowy zwolnienia żołnierza Żandarmerii Wojskowej lub osoby udzielającej mu pomocy w wykonywaniu czynności operacyjno-rozpoznawczych od obowiązku zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” w związku z postępowaniem karnym albo odmowy zezwolenia na udostępnienie materiałów zawierających informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne”, pomimo żądania prokuratora lub sądu, zgłoszonego w związku z postępowaniem karnym w sprawie o przestępstwo przeciwko pokojowi lub ludzkości, przestępstwo wojenne, przestępstwo przeciwko Rzeczypospolitej Polskiej, przestępstwo zamachu terrorystycznego albo też przestępstwo zabójstwa lub spowodowania ciężkiego uszczerbku na zdrowiu, którego następstwem była śmierć człowieka, Minister Obrony Narodowej przedstawia żądane wyjaśnienia i materiały Pierwszemu Prezesowi Sądu Najwyższego. Jeżeli Pierwszy Prezes Sądu Najwyższego stwierdzi, że uwzględnienie żądania prokuratora lub sądu jest konieczne do zapewnienia prawidłowości postępowania karnego, Minister Obrony Narodowej jest zobowiązany zwolnić od obowiązku zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” żołnierza Żandarmerii Wojskowej albo udostępnić żądane wyjaśnienia i materiały

zawierające informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne”.

4. Dane o osobie, o której mowa w ust. 1, mogą być ujawnione na żądanie prokuratora również w razie uzasadnionego podejrzenia, że popełniła ona przestępstwo ścigane z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych. W takim przypadku Minister Obrony Narodowej przedstawia żądane wyjaśnienia i materiały Pierwszemu Prezesowi Sądu Najwyższego. Jeżeli Pierwszy Prezes Sądu Najwyższego stwierdzi, że uwzględnienie żądania prokuratora lub sądu jest konieczne do zapewnienia prawidłowości postępowania karnego, Minister Obrony Narodowej jest zobowiązany zwolnić od obowiązku zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” żołnierza Żandarmerii Wojskowej albo udostępnić żądane wyjaśnienia i materiały zawierające informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne”.”;

3) art. 39 otrzymuje brzmienie:

„Art. 39. Ujawnienie danych o osobie, co do której zachodzi uzasadnione podejrzenie, że popełniła przestępstwo ścigane z oskarżenia publicznego w związku z wykonywaniem przez tę osobę czynności operacyjno-rozpoznawczych, może nastąpić tylko na żądanie prokuratora lub sądu. W takim przypadku Minister Obrony Narodowej przedstawia żądane wyjaśnienia i materiały Pierwszemu Prezesowi Sądu Najwyższego. Jeżeli Pierwszy Prezes Sądu Najwyższego stwierdzi, że uwzględnienie żądania prokuratora lub sądu jest konieczne do zapewnienia prawidłowości postępowania karnego, Minister Obrony Narodowej jest obowiązany zwolnić od obowiązku zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” żołnierza Żandarmerii Wojskowej

i udostępnić żądane wyjaśnienia i materiały zawierające informacje niejawne o klauzuli tajności „tajne" lub „ściśle tajne".";

4) w art. 43 w ust. 1 pkt 8 otrzymuje brzmienie:

„8) w celu odparcia bezpośredniego i gwałtownego zamachu na konwój ochraniający osoby, materiały zawierające informacje niejawne albo środki pieniężne lub inne przedmioty wartościowe;".

Art. 140. W ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.[67)]) w art. 18 ust. 5 otrzymuje brzmienie:

„5. Agencja Bezpieczeństwa Wewnętrznego lub Służba Kontrwywiadu Wojskowego, zgodnie z właściwością określoną w przepisach o ochronie informacji niejawnych, dokonują oceny przydatności urządzeń, o których mowa w ust. 1 i 2, do ochrony informacji niejawnych i wydają stosowne certyfikaty bezpieczeństwa.".

Art. 141. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. Nr 74, poz. 676, z późn. zm.[68)]) wprowadza się następujące zmiany:

1) w art. 5 w ust. 1:

a) w pkt 2 lit. a otrzymuje brzmienie:

„a) szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa,",

b) pkt 3 otrzymuje brzmienie:

„3) realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych;";

2) w art. 9 ust. 4 otrzymuje brzmienie:

„4. Szefowie Agencji, każdy w zakresie swojej właściwości, określają, w drodze zarządzeń, stanowiące informacje niejawne

szczegółowe zasady tworzenia i gospodarowania funduszem operacyjnym.”;

3) w art. 12:
   a) w ust. 1 w pkt 11 lit. a i b otrzymują brzmienie:
      „a) zagrożeń o zasięgu ogólnokrajowym w zakresie ochrony informacji niejawnych,
      b) sposobów postępowania w sytuacji zagrożenia o zasięgu ogólnokrajowym, powstałej wskutek ujawnienia informacji niejawnych, oraz dokonywanie oceny skutków ujawnienia takich informacji,”,
   b) ust. 4 otrzymuje brzmienie:
      „4. Prezydent Rzeczypospolitej Polskiej może delegować swojego przedstawiciela do udziału w posiedzeniach Kolegium, spełniającego wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności „ściśle tajne”.”,
   c) ust. 6 otrzymuje brzmienie:
      „6. Sekretarza Kolegium powołuje, spośród osób spełniających wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności „ściśle tajne”, i odwołuje Prezes Rady Ministrów.”;
4) w art. 15 pkt 5 otrzymuje brzmienie:
   „5) spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności „ściśle tajne”;”;
5) w art. 26 w ust. 1 pkt 8 otrzymuje brzmienie:
   „8) w celu odparcia gwałtownego, bezpośredniego i bezprawnego zamachu na konwój ochraniający osoby, materiały zawierające informacje niejawne, pieniądze albo inne przedmioty wartościowe;”;
6) w art. 35 ust. 7 – 9 otrzymują brzmienie:
   „7. Prezes Rady Ministrów określi, w drodze zarządzenia, sposób współdziałania właściwych organów, służb i instytucji

państwowych z Szefem ABW przy prowadzeniu rejestru, o którym mowa w ust. 4, z uwzględnieniem wymogów dotyczących ochrony informacji niejawnych.

8. Szefowie Agencji, każdy w zakresie swojego działania, określą, w drodze zarządzeń, szczegółowy tryb wydawania i posługiwania się, a także przechowywania dokumentów, o których mowa w ust. 2 i 3, z uwzględnieniem wymogów dotyczących ochrony informacji niejawnych.

9. Szef ABW określi, w drodze zarządzenia, sposób prowadzenia rejestru, o którym mowa w ust. 4, z zachowaniem wymogów dotyczących ochrony informacji niejawnych.";

7) w art. 39 ust. 6 otrzymuje brzmienie:

„6. W razie odmowy zwolnienia funkcjonariusza, pracownika lub osoby udzielającej im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych od obowiązku zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne" lub „ściśle tajne" albo odmowy zezwolenia na udostępnienie materiałów stanowiących informacje niejawne o klauzuli tajności „tajne" lub „ściśle tajne" pomimo żądania prokuratora lub sądu, zgłoszonego w związku z postępowaniem karnym o przestępstwo określone w art. 105 § 1 Kodeksu karnego lub o zbrodnię godzącą w życie ludzkie albo o występek przeciwko życiu lub zdrowiu, gdy jego następstwem była śmierć człowieka, Szef ABW albo Szef AW przedstawia żądane materiały oraz wyjaśnienie Pierwszemu Prezesowi Sądu Najwyższego. Jeżeli Pierwszy Prezes Sądu Najwyższego stwierdzi, że uwzględnienie żądania prokuratora lub sądu jest konieczne do prawidłowości postępowania karnego, Szef ABW albo Szef AW jest obowiązany zwolnić od zachowania tajemnicy lub udostępnić materiały objęte tajemnicą.";

8) w art. 40 ust. 3 otrzymuje brzmienie:

„3. Prezes Rady Ministrów określi, w drodze zarządzenia, sposób współdziałania służb specjalnych z Szefem ABW w zakresie prowadzenia ewidencji, o której mowa w ust. 2,

z uwzględnieniem wymogów dotyczących ochrony informacji niejawnych.”;

9) w art. 47 ust. 1 otrzymuje brzmienie:

„1. Przed podjęciem służby funkcjonariusz ABW albo AW składa ślubowanie według następującej roty:

„Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego (Agencji Wywiadu), ślubuję: służyć wiernie Narodowi, chronić ustanowiony Konstytucją Rzeczypospolitej Polskiej porządek prawny, strzec bezpieczeństwa Państwa i jego obywateli, nawet z narażeniem życia. Wykonując powierzone mi zadania, ślubuję pilnie przestrzegać prawa, dochować wierności konstytucyjnym organom Rzeczypospolitej Polskiej, przestrzegać dyscypliny służbowej oraz wykonywać rozkazy i polecenia przełożonych. Ślubuję strzec tajemnicy prawnie chronionej, honoru, godności i dobrego imienia służby oraz przestrzegać zasad etyki zawodowej.”.”;

10) w art. 85a ust. 2 otrzymuje brzmienie:

„2. Szefowie Agencji, każdy w zakresie swojej właściwości, określą, w drodze zarządzeń, państwa, na których terytoriach występują warunki wymienione w ust. 1, z zachowaniem wymogów dotyczących ochrony informacji niejawnych.”;

11) w art. 116 ust. 3 otrzymuje brzmienie:

„3. Szefowie Agencji, każdy w zakresie swojego działania, określą, w drodze zarządzeń, stanowiące informacje niejawne stanowiska służbowe i stopnie etatowe, zaszeregowanie tych stanowisk do grup uposażenia i przypisanych im stopni etatowych.”.

Art. 142. W ustawie z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. Nr 153, poz. 1270, z późn. zm.[69)]) w art. 96 § 1 otrzymuje brzmienie:

„§ 1. Sąd z urzędu zarządza odbycie całego posiedzenia lub części przy drzwiach zamkniętych, jeżeli publiczne rozpoznanie sprawy zagraża moralności, bezpieczeństwu państwa lub porządkowi publicznemu, a także gdy mogą być ujawnione okoliczności stanowiące informacje niejawne.”.

Art. 143. W ustawie z dnia 23 listopada 2002 r. o Sądzie Najwyższym (Dz. U. Nr 240, poz. 2052, z późn. zm.[70)]) w art. 27 § 1 otrzymuje brzmienie:

„§ 1. Przy powołaniu sędzia Sądu Najwyższego składa ślubowanie wobec Prezydenta Rzeczypospolitej Polskiej według następującej roty:

„Ślubuję uroczyście jako sędzia Sądu Najwyższego służyć wiernie Rzeczypospolitej Polskiej, stać na straży prawa, obowiązki sędziego wypełniać sumiennie, sprawiedliwość wymierzać zgodnie z przepisami prawa, bezstronnie według mego sumienia, dochować tajemnicy prawnie chronionej, a w postępowaniu kierować się zasadami godności i uczciwości”; składający ślubowanie może dodać na końcu zwrot: „Tak mi dopomóż Bóg”.”.

Art. 144. W ustawie z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. Nr 65, poz. 595 oraz z 2005 r. Nr 164, poz. 1365) w art. 17 ust. 5 otrzymuje brzmienie:

„5. Obowiązek publikacji nie dotyczy rozprawy habilitacyjnej zawierającej informacje niejawne.”.

Art. 145. W ustawie z dnia 27 czerwca 2003 r. o rencie socjalnej (Dz. U. Nr 135, poz. 1268, z późn. zm.[71)]) w art. 13 wprowadza się następujące zmiany:

1) uchyla się ust. 2;
2) ust. 3 otrzymuje brzmienie:

„3. Przepis ust. 1 stosuje się odpowiednio do organu emerytalno-rentowego.”.

Art. 146. W ustawie z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (Dz. U. z 2008 r. Nr 141, poz. 892, z późn. zm.[72)]) wprowadza się następujące zmiany:

1) w art. 58 ust. 4 otrzymuje brzmienie:

„4. 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 o ochronie informacji niejawnych, chyba że żołnierz zawodowy, który złożył oświadczenie, wyraził pisemną zgodę na ich ujawnienie. W szczególnie uzasadnionych przypadkach Minister Obrony Narodowej może je ujawnić pomimo braku zgody składającego oświadczenie.";

2) w art. 107 ust. 3 otrzymuje brzmienie:

„3. Zezwolenie, o którym mowa w ust. 2, może być przez Ministra Obrony Narodowej zawieszone lub cofnięte, jeżeli wymagają tego względy ochrony informacji niejawnych oraz potrzeby Sił Zbrojnych.".

Art. 147. W ustawie z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2007 r. Nr 223, poz. 1655, z późn. zm.[73)]) w art. 4 pkt 5 otrzymuje brzmienie:

„5) zamówień zawierających informacje niejawne, jeżeli wymaga tego istotny interes publiczny lub istotny interes państwa;".

Art. 148. W ustawie z dnia 20 kwietnia 2004 r. o wyrobach medycznych (Dz. U. Nr 93, poz. 896, z późn. zm.[74)]) w art. 47 ust. 1 otrzymuje brzmienie:

„1. Wszelkie dane dotyczące uczestnika badania zebrane w czasie badania klinicznego stanowią tajemnicę prawnie chronioną.".

Art. 149. W ustawie z dnia 27 maja 2004 r. o funduszach inwestycyjnych (Dz. U. Nr 146, poz. 1546, z późn. zm.[75)]) w art. 281 w ust. 1 pkt 8 otrzymuje brzmienie:

„8) Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Policji, Żandarmerii

Wojskowej, Straży Granicznej, Służby Więziennej, Biura Ochrony Rządu i ich upoważnionych pisemnie funkcjonariuszy lub żołnierzy w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych;".

Art. 150. W ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2007 r. Nr 155, poz. 1095, z późn. zm.[76)]) wprowadza się następujące zmiany:

1) w art. 91 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) działalność przedsiębiorcy zagranicznego zagraża bezpieczeństwu i obronności państwa, bezpieczeństwu informacji niejawnych o klauzuli tajności „poufne" lub wyższej lub innemu ważnemu interesowi publicznemu.";

2) w art. 99 w ust. 1 pkt 1 otrzymuje brzmienie:

„1) utworzenie przedstawicielstwa zagrażałoby bezpieczeństwu i obronności państwa lub bezpieczeństwu informacji niejawnych o klauzuli tajności „poufne" lub wyższej lub innemu ważnemu interesowi publicznemu;";

3) w art. 101 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) działalność przedsiębiorcy zagranicznego zagraża bezpieczeństwu i obronności państwa, bezpieczeństwu informacji niejawnych o klauzuli tajności „poufne" lub wyższej lub innemu ważnemu interesowi publicznemu.".

Art. 151. W ustawie z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2008 r. Nr 164, poz. 1027, z późn. zm.[77)]) w art. 188 ust. 6 otrzymuje brzmienie:

„6. Rada Ministrów może określić, w drodze rozporządzenia, osoby spośród wymienionych w art. 66 ust. 1 pkt 2 – 9, wobec których, z uwagi na konieczność zapewnienia bezpieczeństwa form i metod realizacji zadań podlegających ochronie zgodnie z przepisami o ochronie informacji niejawnych, stosuje się odrębny tryb przetwarzania danych, o których mowa w ust. 4. Rozporządzenie powinno w szczególności określać dane osobowe, które będą

przetwarzane, sposób ich przetwarzania oraz podmiot uprawniony do ich gromadzenia i przetwarzania.”.

Art. 152. W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[78)]) wprowadza się następujące zmiany:

1) w art. 123 ust. 9 otrzymuje brzmienie:

„9. Jeżeli uzasadnienie opinii lub wniosku organów, o których mowa w ust. 8, wskazujące na okoliczności prowadzące do zagrożenia obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego zawiera informacje niejawne, zamiast uzasadnienia doręcza się zawiadomienie, że uzasadnienie takie zostało sporządzone.”;

2) w art. 201 ust. 6 otrzymuje brzmienie:

„6. Przed wydaniem decyzji, o której mowa w ust. 5, Prezes UKE zasięga opinii Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu, w zakresie ich właściwości. Jeżeli uzasadnienie do opinii tych organów zawiera informacje niejawne, zamiast uzasadnienia doręcza się zawiadomienie, że uzasadnienie zostało sporządzone.”;

3) w art. 202 ust. 4 otrzymuje brzmienie:

„4. Działania, o których mowa w ust. 1, Prezes UKE może także podejmować na wniosek organów właściwych w sprawach obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Jeżeli uzasadnienia do wniosku tych organów zawierają informacje niejawne, zamiast uzasadnień doręcza się informację, że uzasadnienia takie zostały sporządzone.”.

Art. 153. W ustawie z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego (Dz. U. Nr 273, poz. 2702 oraz z 2006 r. Nr 107, poz. 722) w art. 7 ust. 1 otrzymuje brzmienie:

„1. Tłumacz przysięgły składa wobec Ministra Sprawiedliwości ślubowanie według następującej roty:

„Mając świadomość znaczenia moich słów i odpowiedzialności przed prawem, przyrzekam uroczyście, że powierzone mi zadania tłumacza przysięgłego będę wykonywać sumiennie i bezstronnie, dochowując tajemnicy prawnie chronionej oraz kierując się w swoim postępowaniu uczciwością i etyką zawodową.”.”.

Art. 154. W ustawie z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz. U. z 2005 r. Nr 14, poz. 114, z późn. zm.[79)]) wprowadza się następujące zmiany:

1) w art. 91 ust. 5 otrzymuje brzmienie:

„5. Świadek może odmówić udzielenia odpowiedzi na pytania co do okoliczności stanowiących informacje niejawne, chyba że zostanie zwolniony z obowiązku zachowania tajemnicy w trybie i na zasadach określonych w odrębnych przepisach. Zwolnienia można odmówić tylko wtedy, gdyby złożenie wyjaśnień lub udzielenie odpowiedzi mogło wyrządzić poważną szkodę państwu.”;

2) w art. 96 ust. 3 otrzymuje brzmienie:

„3. Dokumenty, opinie lub inne informacje, zawierające informacje niejawne, przekazuje się rzecznikowi dyscypliny w trybie i na zasadach określonych w przepisach o ochronie informacji niejawnych tylko w przypadku zwolnienia z obowiązku zachowania tajemnicy, o którym mowa w art. 91 ust. 5.”;

3) w art. 119 w ust. 2 pkt 1 otrzymuje brzmienie:

„1) ze względu na bezpieczeństwo państwa lub ochronę informacji niejawnych;”.

Art. 155. W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.[80)]) wprowadza się następujące zmiany:

1) w art. 25 ust. 2 otrzymuje brzmienie:

„2. Kontrola, o której mowa w ust. 1, nie może dotyczyć informacji niejawnych lub informacji i danych stanowiących inną tajemnicę prawnie chronioną, zawartych w kontrolowanych systemach teleinformatycznych oraz rejestrach publicznych, jak również prowadzić do ich ujawnienia ani narażać na ujawnienie, z zastrzeżeniem art. 26 ust. 3 pkt 4.”;

2) w art. 26 w ust. 3 pkt 4 otrzymuje brzmienie:

„4) aktualnego poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych – w przypadku gdy kontrola ma dotyczyć systemów teleinformatycznych lub rejestrów publicznych zawierających informacje i dane stanowiące informacje niejawne o klauzuli tajności „poufne” lub wyższej.”.

Art. 156. W ustawie z dnia 30 czerwca 2005 r. o finansach publicznych (Dz. U. Nr 249, poz. 2104, z późn. zm.[81)]) w art. 22:

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

„18) z opłat za przeprowadzenie procesów certyfikacji, o których mowa w art. 50 ust. 1 – 3 ustawy z dnia ……..... o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. Nr …, poz. …).”;

2) w ust. 6 pkt 1 otrzymuje brzmienie:

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

Art. 157. W ustawie z dnia 8 lipca 2005 r. o Prokuratorii Generalnej Skarbu Państwa (Dz. U. Nr 169, poz. 1417, z późn. zm.[82)]) art. 33 otrzymuje brzmienie:

„Art. 33. Przed wręczeniem aktu mianowania radca Prokuratorii Generalnej i starszy radca Prokuratorii Generalnej, o którym mowa w art. 30 pkt 2 – 5, składa wobec Prezesa Prokuratorii Generalnej ślubowanie według następującej roty: „Ślubuję uroczyście na powierzonym mi stanowisku służyć wiernie

Rzeczypospolitej Polskiej, stać na straży prawa oraz strzec praw i interesów Skarbu Państwa, obowiązki swoje wypełniać sumiennie, dochować tajemnicy prawnie chronionej, a w postępowaniu kierować się zasadami godności i uczciwości". Składający ślubowanie może dodać na końcu zwrot: „Tak mi dopomóż Bóg".".

Art. 158. W ustawie z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. Nr 183, poz. 1538, z późn. zm.[83)]) w art. 149 pkt 7 otrzymuje brzmienie:

„7) Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Policji, Żandarmerii Wojskowej, Straży Granicznej, Służby Więziennej, Biura Ochrony Rządu i ich upoważnionych pisemnie funkcjonariuszy lub żołnierzy – w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych;".

Art. 159. W ustawie z dnia 29 sierpnia 2005 r. o zwrocie osobom fizycznym niektórych wydatków związanych z budownictwem mieszkaniowym (Dz. U. Nr 177, poz. 1468 oraz z 2007 r. Nr 23, poz. 138 i Nr 192, poz. 1382) art. 6a otrzymuje brzmienie:

„Art. 6a. Jeżeli jest to uzasadnione ochroną informacji niejawnych i wymogami bezpieczeństwa państwa, do przyjmowania wniosków, o których mowa w art. 5 ust. 1, wydawania decyzji określających kwotę zwrotu oraz do dokonywania zwrotu, o którym mowa w art. 3 ust. 1, uprawnione są organy wymienione w art. 13a ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2005 r. Nr 8, poz. 60, z późn. zm.).".

Art. 160. W ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708, z późn. zm.[84)]) wprowadza się następujące zmiany:

1) w art. 4 ust. 3 otrzymuje brzmienie:

„3. Szef Centralnego Biura Antykorupcyjnego określi, w drodze zarządzenia, stanowiący informacje niejawne sposób tworzenia i gospodarowania funduszem operacyjnym, o którym mowa w ust. 2.”;

2) w art. 7 w ust. 1 pkt 5 otrzymuje brzmienie:

„5) spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności „ściśle tajne”;”;

3) w art. 16 w ust. 1 pkt 8 otrzymuje brzmienie:

„8) w celu odparcia gwałtownego, bezpośredniego i bezprawnego zamachu na konwój ochraniający osoby, materiały zawierające informacje niejawne, pieniądze albo inne przedmioty wartościowe;”;

4) w art. 24 ust. 5 otrzymuje brzmienie:

„5. Prezes Rady Ministrów określi, w drodze zarządzenia, szczegółowy tryb wydawania i posługiwania się, a także przechowywania dokumentów, o których mowa w ust. 2 i 3, z uwzględnieniem wymogów dotyczących ochrony informacji niejawnych.”;

5) w art. 28 ust. 5 otrzymuje brzmienie:

„5. W przypadku odmowy zwolnienia funkcjonariusza, pracownika lub osoby udzielającej im pomocy w wykonywaniu czynności operacyjno–rozpoznawczych od obowiązku zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” albo odmowy zezwolenia na udostępnienie materiałów stanowiących informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne” pomimo żądania prokuratora lub sądu, zgłoszonego w związku z postępowaniem karnym o zbrodnie przeciwko pokojowi, ludzkości i przestępstw wojennych oraz godzących w życie ludzkie albo o występek przeciwko życiu lub zdrowiu, gdy jego następstwem była śmierć człowieka, Szef CBA przedstawia żądane materiały oraz wyjaśnienie Pierwszemu Prezesowi Sądu Najwyższego. Jeżeli Pierwszy Prezes Sądu Najwyższego stwierdzi, że

uwzględnienie żądania prokuratora lub sądu jest konieczne do prawidłowości postępowania karnego, Szef CBA jest obowiązany zwolnić od zachowania tajemnicy lub udostępnić materiały objęte tajemnicą.”;

6) w art. 29 ust. 3 otrzymuje brzmienie:

3. Prezes Rady Ministrów określi, w drodze zarządzenia, warunki, zakres i tryb:

1) współdziałania w zakresie, o którym mowa w ust. 1,

2) koordynacji, o której mowa w ust. 2

– mając na uwadze zapewnienie sprawności i skuteczności postępowań, a także uwzględniając wymogi dotyczące ochrony informacji niejawnych.”;

7) w art. 107 w ust. 2 pkt 9 otrzymuje brzmienie:

„9) utrata materiału zawierającego informacje niejawne;”.

Art. 161. W ustawie z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 i Nr 218, poz. 1592 oraz z 2009 r. Nr 85, poz. 716) wprowadza się następujące zmiany:

1) art. 1 otrzymuje brzmienie:

„Art. 1. Tworzy się Służbę Kontrwywiadu Wojskowego, zwaną dalej „SKW”, jako służbę specjalną, właściwą w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej, zwanych dalej „SZRP”, oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej.”;

2) w art. 5 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) realizowanie, w granicach swojej właściwości, zadań określonych w przepisach o ochronie informacji niejawnych;”;

3) w art. 11 ust. 3 otrzymuje brzmienie:

„3. Szefowie SKW i SWW, każdy w zakresie swojej właściwości, po zatwierdzeniu przez Ministra Obrony Narodowej, określają, w drodze zarządzeń, stanowiące informacje niejawne

szczegółowe zasady tworzenia i gospodarowania funduszem operacyjnym, o którym mowa w ust. 2.”;

4) w art. 16 pkt 5 otrzymuje brzmienie:

„5) spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności „ściśle tajne”;”;

5) w art. 30 w ust. 1 pkt 6 otrzymuje brzmienie:

„6) w celu odparcia gwałtownego, bezpośredniego i bezprawnego zamachu na konwój ochraniający osoby, materiały zawierające informacje niejawne, pieniądze albo inne przedmioty wartościowe.”;

6) w art. 39 ust. 7 otrzymuje brzmienie:

„7. Szefowie SKW i SWW, każdy w zakresie swojego działania, określą, w drodze zarządzeń, szczegółowy tryb wydawania i posługiwania się, a także przechowywania dokumentów, o których mowa w ust. 2 i 3, z uwzględnieniem wymogów dotyczących ochrony informacji niejawnych.”;

7) w art. 43 ust. 6 otrzymuje brzmienie:

„6. W razie odmowy zwolnienia funkcjonariusza, pracownika lub osoby udzielającej im pomocy w wykonywaniu czynności operacyjno–rozpoznawczych od obowiązku zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” albo odmowy zezwolenia na udostępnienie materiałów stanowiących informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne” pomimo żądania prokuratora lub sądu, zgłoszonego w związku z postępowaniem karnym o przestępstwo określone w art. 105 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny lub o zbrodnię godzącą w życie ludzkie albo o występek przeciwko życiu lub zdrowiu, gdy jego następstwem była śmierć człowieka, Szef SKW albo Szef SWW przedstawia żądane materiały oraz wyjaśnienie Pierwszemu Prezesowi Sądu Najwyższego. Jeżeli Pierwszy Prezes Sądu Najwyższego stwierdzi, że uwzględnienie żądania prokuratora lub sądu jest konieczne do prawidłowości

postępowania karnego, Szef SKW albo Szef SWW jest obowiązany zwolnić od zachowania tajemnicy lub udostępnić materiały objęte tajemnicą.”.

Art. 162. W ustawie z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (Dz. U. Nr 104, poz. 710 oraz z 2009 r. Nr 114, poz. 957) wprowadza się następujące zmiany:

1) w art. 76 ust. 4 otrzymuje brzmienie:

„4. Szef SKW i Szef SWW, każdy w zakresie swojego działania, określą, w drodze zarządzeń, stanowiące informacje niejawne stanowiska służbowe i stopnie etatowe, zaszeregowanie tych stanowisk do grup uposażenia i przypisanych im stopni etatowych.”;

2) w art. 106 w ust. 2 pkt 7 otrzymuje brzmienie:

„7) utrata służbowej broni palnej, amunicji lub legitymacji służbowej, a także materiału zawierającego informacje niejawne.”.

Art. 163. W ustawie z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia (Dz. U. Nr 171, poz. 1225, z późn. zm.[85)]) w art. 76 ust. 2 otrzymuje brzmienie:

„2. Uzyskane przez organy urzędowej kontroli żywności, w trakcie kontroli, informacje, dokumenty i inne dane stanowiące tajemnicę przedsiębiorcy nie mogą być przekazywane innym organom ani ujawniane, jeżeli nie jest to konieczne ze względu na ochronę życia lub zdrowia człowieka, z wyłączeniem żądania sądu lub prokuratury w związku z toczącym się postępowaniem.”.

Art. 164. W ustawie 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 2007 r. Nr 63, poz. 425, z późn. zm.[86)]) wprowadza się następujące zmiany:

1) art. 9 otrzymuje brzmienie:

„Art. 9. Osoby składające oświadczenie lustracyjne, w zakresie jego treści, są zwolnione z mocy prawa z obowiązku zachowania w tajemnicy informacji niejawnych.”;

2) w art. 18 ust. 2a otrzymuje brzmienie:

„2a. Sąd może wyłączyć jawność całości albo części rozprawy również na żądanie prokuratora Biura Lustracyjnego lub prokuratora oddziałowego biura lustracyjnego Instytutu Pamięci Narodowej, jeżeli zachodzi obawa ujawnienia informacji niejawnych.”.

Art. 165. W ustawie z dnia 17 listopada 2006 r. o systemie oceny zgodności wyrobów przeznaczonych na potrzeby obronności i bezpieczeństwa państwa (Dz. U. Nr 235, poz. 1700) w art. 14 ust. 2 otrzymuje brzmienie:

„2. Spełnienie wymogu, o którym mowa w ust. 1 pkt 5, ocenia ABW lub SKW, zgodnie z właściwością wskazaną w przepisach o ochronie informacji niejawnych, przez wystawienie opinii w tej sprawie.”.

Art. 166. W ustawie z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy (Dz. U. Nr 89, poz. 589, z późn. zm.[87)]) wprowadza się następujące zmiany:

1) w art. 23:

a) ust. 4 otrzymuje brzmienie:

„4. Na postanowienie w sprawie zachowania w tajemnicy danych osobowych, o których mowa w ust. 2, pracodawcy przysługuje zażalenie w terminie 3 dni od dnia doręczenia postanowienia. Zażalenie na postanowienie inspektora pracy rozpoznaje właściwy okręgowy inspektor pracy. Postępowanie dotyczące zażalenia toczy się bez udziału pracodawcy i z wyłączeniem jawności.”,

b) ust. 6 otrzymuje brzmienie:

„6. Główny Inspektor Pracy określi zasady postępowania z protokołami przesłuchań i innymi dokumentami, o których mowa w ust. 2 – 5.”;

2) w art. 44 ust. 1 otrzymuje brzmienie:

„1. Pracownicy wykonujący czynności kontrolne są odpowiedzialni za sumienne wykonywanie swoich obowiązków, w szczególności za rzetelne i obiektywne ujmowanie i dokumentowanie wyników kontroli oraz za przestrzeganie przepisów o ochronie informacji niejawnych.”.

Art. 167. W ustawie z dnia 15 czerwca 2007 r. o licencji syndyka (Dz. U. Nr 123, poz. 850) w art. 15 ust. 1 otrzymuje brzmienie:

„1. Osoba, której przyznano licencję syndyka, składa wobec Ministra Sprawiedliwości, przed wpisem na listę osób posiadających licencję syndyka, o której mowa w art. 17 ust. 1, ślubowanie według następującej roty: „Mając świadomość znaczenia moich słów i odpowiedzialności przed prawem, ślubuję uroczyście, że powierzone mi obowiązki w postępowaniu upadłościowym lub naprawczym będę wypełniać sumiennie i bezstronnie, dochowując tajemnic prawnie chronionych oraz kierując się w swym postępowaniu zasadami godności, uczciwości i etyki.”.”.

Art. 168. W ustawie z dnia 9 stycznia 2009 r. o koncesji na roboty budowlane lub usługi (Dz. U. Nr 19, poz. 101 oraz z 2009 r. Nr 157, poz. 1241) w art. 4 w ust. 1 pkt 1 otrzymuje brzmienie:

„1) której wykonanie jest związane z dostępem do informacji niejawnych o klauzuli tajności „poufne” lub wyższej albo jeżeli jej wykonaniu muszą towarzyszyć szczególne środki bezpieczeństwa, albo jeżeli wymaga tego ochrona podstawowych interesów państwa;”.

Art. 169. W ustawie z dnia 23 stycznia 2009 r. o Krajowej Szkole Sądownictwa i Prokuratury (Dz. U. Nr 26, poz. 157, Nr 56, poz. 459 i Nr 178, poz. 1375) wprowadza się następujące zmiany:

1) art. 24 otrzymuje brzmienie:

„Art. 24. Przed objęciem obowiązków aplikant aplikacji ogólnej składa ślubowanie wobec Dyrektora Krajowej Szkoły według następującej roty: „Ślubuję uroczyście sumiennie

wypełniać obowiązki aplikanta Krajowej Szkoły Sądownictwa i Prokuratury, w postępowaniu kierować się zasadami godności i uczciwości, dbać o dobre imię Krajowej Szkoły Sądownictwa i Prokuratury oraz dochować tajemnicy prawnie chronionej"; składający ślubowanie może dodać zwrot: „Tak mi dopomóż Bóg"."];

2) art. 30 otrzymuje brzmienie:

„Art. 30. Przed objęciem obowiązków aplikant aplikacji sędziowskiej albo prokuratorskiej składa ślubowanie wobec Dyrektora Krajowej Szkoły według następującej roty: „Ślubuję uroczyście sumiennie wypełniać obowiązki aplikanta Krajowej Szkoły Sądownictwa i Prokuratury, w postępowaniu kierować się zasadami godności i uczciwości, dbać o dobre imię Krajowej Szkoły Sądownictwa i Prokuratury oraz dochować tajemnicy prawnie chronionej"; składający ślubowanie może dodać zwrot: „Tak mi dopomóż Bóg".".

Art. 170. W ustawie z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. Nr 168, poz. 1323 i Nr 201, poz. 1540) wprowadza się następujące zmiany:

1) w art. 8 ust. 8 otrzymuje brzmienie:

„8. Przepisów o tajemnicy celnej nie stosuje się do informacji podlegających ochronie na podstawie przepisów o ochronie informacji niejawnych.";

2) w art. 123 ust. 2 otrzymuje brzmienie:

„2. Treść oświadczenia o stanie majątkowym stanowi tajemnicę prawnie chronioną i podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone" określonej w przepisach o ochronie informacji niejawnych.".

Rozdział 12
Przepisy przejściowe i końcowe

Art. 171. 1. Materiały zawierające informacje niejawne w dniu wejścia w życie ustawy podlegają ochronie zgodnie z przepisami niniejszej ustawy.

2. Kierownicy jednostek organizacyjnych przeprowadzą, w terminie 36 miesięcy od dnia wejścia w życie ustawy, przegląd wytworzonych w podległych im jednostkach organizacyjnych materiałów, o których mowa w ust. 1, w celu ustalenia, czy spełniają ustawowe przesłanki ochrony na podstawie ustawy, i dokonają w razie potrzeby zmiany lub zniesienia klauzuli tajności.

3. Obowiązek, o którym mowa w ust. 2, nie dotyczy zbiorów materiałów spraw zakończonych oraz kartotek ewidencyjnych, w szczególności stanowiących materiał archiwalny przekazany do właściwych archiwów na podstawie odrębnych przepisów.

4. Kierownik właściwego archiwum, w uzasadnionych przypadkach, może zwrócić się do kierownika jednostki organizacyjnej, która przekazała materiał archiwalny, o którym mowa w ust. 3, o przeprowadzenie przeglądu tego materiału w celu ustalenia, czy spełnia ustawowe przesłanki ochrony i dokonanie, w razie potrzeby, zmiany lub zniesienia klauzuli tajności.

Art. 172. Poświadczenia bezpieczeństwa wydane na podstawie przepisów dotychczasowych zachowują ważność przez okres wskazany w tych przepisach.

Art. 173. Przepis art. 14 ust. 3 pkt 2 stosuje się do pełnomocników ochrony i zastępców pełnomocników ochrony zatrudnionych po dniu wejścia w życie ustawy.

Art. 174. Kierownicy jednostek organizacyjnych, w których w dniu wejścia w życie ustawy funkcjonują kancelarie tajne, informują o nich w terminie do trzech miesięcy od tej daty odpowiednio ABW lub SKW, z określeniem klauzuli tajności przetwarzanych informacji niejawnych.

Art. 175. 1. Akredytacje systemów teleinformatycznych udzielone przed dniem wejścia w życie ustawy zachowują ważność do czasu dokonania w systemie teleinformatycznym zmian, które mogą mieć istotny wpływ na bezpieczeństwo teleinformatyczne, nie dłużej jednak niż przez okres 5 lat od dnia wejścia w życie ustawy.

2. Ponowna akredytacja systemu teleinformatycznego przeprowadzana jest w trybie art. 48. ABW lub SKW, przeprowadzając ponowną akredytację, może odstąpić od przeprowadzenia audytu bezpieczeństwa systemu teleinformatycznego, niezależnie od klauzuli informacji niejawnych przetwarzanych w systemie teleinformatycznym.

3. Środki techniczne dopuszczone do eksploatacji na podstawie art. 60 ust. 8 ustawy, o której mowa w art. 179, mogą być użytkowane do czasu uzyskania wymaganej w przepisach niniejszej ustawy akredytacji bezpieczeństwa teleinformatycznego, jednak nie dłużej niż przez okres 12 miesięcy, z zastrzeżeniem art. 51.

Art. 176. 1. Świadectwa bezpieczeństwa przemysłowego wydane na podstawie przepisów dotychczasowych, ważne w dniu wejścia w życie ustawy, potwierdzające zdolność do ochrony informacji niejawnych:

1) o klauzuli „ściśle tajne" – potwierdzają także zdolność do ochrony informacji niejawnych o klauzuli „tajne" i „poufne" w okresie wskazanym w niniejszej ustawie;
2) o klauzuli „tajne" – potwierdzają także zdolność do ochrony informacji niejawnych o klauzuli „poufne" w okresie wskazanym w niniejszej ustawie.

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

Art. 177. Do postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego wszczętych i niezakończonych przed dniem wejścia w życie ustawy stosuje się przepisy dotychczasowe.

Art. 178. 1. Dotychczasowe przepisy wykonawcze wydane na podstawie ustawy, o której mowa w art. 179, zachowują moc do czasu wejścia przepisów wykonawczych wydanych na podstawie niniejszej ustawy, nie dłużej jednak niż przez okres 12 miesięcy od dnia jej wejścia w życie.

2. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 7 ust. 2 ustawy, o której mowa w art. 91, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na postawie art. 7 ust. 2 tej ustawy w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż przez okres 12 miesięcy od dnia jej wejścia w życie.

Art. 179. Traci moc ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm. [88)]).

Art. 180. Ustawa wchodzi w życie po upływie 3 miesięcy od dnia ogłoszenia.

[1)] Niniejszą ustawą zmienia się ustawy: ustawę z dnia 31 stycznia 1959 r. o cmentarzach i chowaniu zmarłych, ustawę z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, ustawę z dnia 1 grudnia 1961 r. o izbach morskich, ustawę z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, ustawę z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, ustawę z dnia 26 czerwca 1974 r. – Kodeks pracy, ustawę z dnia 26 marca 1982 r. o Trybunale Stanu, ustawę z dnia 6 lipca 1982 r. o zasadach prowadzenia na terytorium Polskiej Rzeczypospolitej Ludowej działalności gospodarczej w zakresie drobnej wytwórczości przez zagraniczne osoby prawne i fizyczne, ustawę z dnia 16 września 1982 r. o pracownikach urzędów państwowych, ustawę z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy, ustawę z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, ustawę z dnia 26 stycznia 1984 r. – Prawo prasowe, ustawę z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej, ustawę z dnia 18 kwietnia 1985 r. o rybactwie śródlądowym, ustawę z dnia 20 czerwca 1985 r. o prokuraturze, ustawę z dnia 31 lipca 1985 r. o obowiązkach i prawach posłów i senatorów, ustawę z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich, ustawę z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne, ustawę z dnia 6 kwietnia 1990 r. o Policji, ustawę z dnia 12 października 1990 r. o Straży Granicznej, ustawę z dnia 14 lutego 1991 r. – Prawo o notariacie, ustawę z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska, ustawę z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych, ustawę z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej, ustawę z dnia 28 września 1991 r. o kontroli skarbowej, ustawę z dnia 29 grudnia 1992 r. o radiofonii i telewizji, ustawę z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego, ustawę z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli, ustawę z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników, ustawę z dnia 26 kwietnia 1996 r. o Służbie Więziennej, ustawę z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora, ustawę z dnia 21 czerwca 1996 r. o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra, ustawę z dnia 30 sierpnia 1996 r. o komercjalizacji i prywatyzacji, ustawę z dnia 6 czerwca 1997 r.– Kodeks karny, ustawę z dnia 6 czerwca 1997 r.– Kodeks postępowania karnego, ustawę z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy, ustawę z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym, ustawę z dnia 25 czerwca 1997 r. o świadku koronnym, ustawę z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym, ustawę z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych, ustawę z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, ustawę z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych, ustawę z dnia 29 sierpnia 1997 r. o strażach gminnych, ustawę z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji, ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 29 sierpnia 1997 r. – Prawo bankowe, ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ustawę z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, ustawę z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, ustawę z dnia 18 grudnia 1998 r. o pracownikach sądów i prokuratury, ustawę z dnia 21 stycznia 1999 r. o sejmowej komisji śledczej, ustawę z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka, ustawę z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej, ustawę z dnia 26 października 2000 r. o giełdach towarowych, ustawę z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ustawę z dnia 15 grudnia 2000 r. o Inspekcji Handlowej, ustawę z dnia 21 grudnia 2000 r. o żegludze śródlądowej, ustawę z dnia 11 stycznia 2001 r. o substancjach i preparatach chemicznych, ustawę z dnia 16 marca 2001 r. o Biurze Ochrony Rządu, ustawę z dnia 22 czerwca 2001 r. o wykonywaniu Konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów, ustawę z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych, ustawę z dnia 18 lipca 2001 r. – Prawo wodne, ustawę z dnia 27 lipca 2001 r. o kuratorach sądowych, ustawę z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, ustawę z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia, ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawę z dnia 18 września 2001 r. o podpisie elektronicznym, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed

sądami administracyjnymi, ustawę z dnia 23 listopada 2002 r. o Sądzie Najwyższym, ustawę z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki, ustawę z dnia 27 czerwca 2003 r. o rencie socjalnej, ustawę z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych, ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, ustawę z dnia 20 kwietnia 2004 r. o wyrobach medycznych, ustawę z dnia 27 maja 2004 r. o funduszach inwestycyjnych, ustawę z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, ustawę z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, ustawę z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego, ustawę z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych, ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawę z dnia 30 czerwca 2005 r. o finansach publicznych, ustawę z dnia 8 lipca 2005 r. o Prokuratorii Generalnej Skarbu Państwa, ustawę z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, ustawę z dnia 29 sierpnia 2005 r. o zwrocie osobom fizycznym niektórych wydatków związanych z budownictwem mieszkaniowym, ustawę z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, ustawę z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, ustawę z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego, ustawę z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia, ustawę z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944 – 1990 oraz treści tych dokumentów, ustawę z dnia 17 listopada 2006 r. o systemie oceny zgodności wyrobów przeznaczonych na potrzeby obronności i bezpieczeństwa państwa, ustawę z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy, ustawę z dnia 15 czerwca 2007 r. o licencji syndyka, ustawę z dnia 9 stycznia 2009 r. o koncesji na roboty budowlane lub usługi, ustawę z dnia 23 stycznia 2009 r. o Krajowej Szkole Sądownictwa i Prokuratury oraz ustawę z dnia 27 sierpnia 2009 r. o Służbie Celnej.

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 96, poz. 959 i Nr 173, poz. 1808, z 2007 r. Nr 50, poz. 331, z 2008 r. Nr 171, poz. 1056 i Nr 216, poz. 1371 oraz z 2009 r. Nr 201, poz. 1540.

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 180, poz. 1280, z 2008 r. Nr 70, poz. 416, Nr 116, poz. 732, Nr 141, poz. 888, Nr 171, poz. 1056 i Nr 216, poz. 1367 oraz z 2009 r. Nr 3, poz. 11, Nr 18, poz. 97, Nr 168, poz. 1323 i Nr 201, poz. 1540.

[4)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 49, poz. 509, z 2002 r. Nr 113, poz. 984, Nr 153, poz. 1271 i Nr 169, poz. 1387, z 2003 r. Nr 130, poz. 1188 i Nr 170, poz. 1660, z 2004 r. Nr 162, poz. 1692, z 2005 r. Nr 64, poz. 565, Nr 78, poz. 682 i Nr 181, poz. 1524, z 2008 r. Nr 229, poz. 1539 oraz z 2009 r. Nr 195, poz. 1501.

[5)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1999 r. Nr 83, poz. 931, z 2000 r. Nr 50, poz. 580, Nr 62, poz. 717, Nr 73, poz. 852 i Nr 93, poz. 1027, z 2001 r. Nr 98, poz. 1071 i Nr 106, poz. 1149, z 2002 r. Nr 74, poz. 676, z 2003 r. Nr 17, poz. 155, Nr 111, poz. 1061 i Nr 130, poz. 1188, z 2004 r. Nr 51, poz. 514, Nr 69, poz. 626, Nr 93, poz. 889, Nr 240, poz. 2405 i Nr 264, poz. 2641, z 2005 r. Nr 10, poz. 70, Nr 48, poz. 461, Nr 77, poz. 680, Nr 96, poz. 821, Nr 141, poz. 1181, Nr 143, poz. 1203, Nr 163, poz. 1363, Nr 169, poz. 1416 i Nr 178, poz. 1479, z 2006 r. Nr 15, poz. 118, Nr 66, poz. 467, Nr 95, poz. 659, Nr 104, poz. 708 i 711, Nr 141, poz. 1009 i 1013, Nr 167, poz. 1192 i Nr 226, poz. 1647 i 1648, z 2007 r. Nr 20, poz. 116, Nr 64, poz. 432, Nr 80, poz. 539, Nr 89, poz. 589, Nr 99, poz. 664, Nr 112, poz. 766, Nr 123, poz. 849 i Nr 128, poz. 903, z 2008 r. Nr 27, poz. 162, Nr 100, poz. 648, Nr 107, poz. 686, Nr 123, poz. 802, Nr 182, poz. 1133, Nr 208, poz. 1308, Nr 214, poz. 903, Nr 225, poz. 1485, Nr 234, poz. 1571 i Nr 237, poz. 1651 oraz z 2009 r. Nr 8, poz. 39, Nr 20, poz. 104, Nr 28, poz. 171, Nr 68, poz. 585, Nr 85, poz. 716, Nr 127, poz. 1051, Nr 144, poz. 1178, Nr 168, poz. 1323, Nr 190, poz. 1474 i Nr 206, poz. 1586.

[6)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 64, poz. 432, Nr 83, poz. 561, Nr 85, poz. 571 i Nr 140, poz. 983.

[7)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 83, poz. 561, Nr 85, poz. 571, Nr 115, poz. 789, Nr 165, poz. 1171 i Nr 176, poz. 1242 oraz z 2009 r. Nr 178, poz. 1375.

[8)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 209, poz. 1315, Nr 225, poz. 1502 i Nr 227, poz. 1505.

[9)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2000 r. Nr 48, poz. 550, z 2004 r. Nr 146, poz. 1546 i Nr 152, poz. 1598 oraz z 2005 r. Nr 23, poz. 187 i Nr 164, poz. 1365.

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

poz. 1546 oraz z 2009 r. Nr 18, poz. 97, Nr 42, poz. 341, Nr 65, poz. 545, Nr 71, poz. 609, Nr 127, poz. 1045, Nr 144, poz. 1176, Nr 165, poz. 1316, Nr 166, poz. 1317, Nr 168, poz. 1323 i Nr 201, poz. 1540.

11) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 85, poz. 727, Nr 86, poz. 732 i Nr 143, poz. 1199, z 2006 r. Nr 57, poz. 609 i 610, Nr 66, poz. 470, Nr 104, poz. 708, Nr 217, poz. 1590 i Nr 225, poz. 1635, z 2007 r. Nr 105, poz. 721, Nr 112, poz. 769, Nr 120, poz. 818, Nr 192, poz. 1378, Nr 195, poz. 1414 i Nr 225, poz. 1671, z 2008 r. Nr 118, poz. 745, Nr 141, poz. 888, Nr 180, poz. 1109, Nr 209, poz. 1316, 1318 i 1320 oraz z 2009 r. Nr 18, poz. 97, Nr 44, poz. 362, Nr 57, poz. 466, Nr 166, poz. 1317 i Nr 168, poz. 1323.

12) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 64, poz. 594, Nr 91, poz. 868, Nr 171, poz. 1800 i Nr 173, poz. 1808, z 2005 r. Nr 132, poz. 1110 i Nr 183, poz. 1537, z 2006 r. Nr 66, poz. 470, Nr 104, poz. 708 i 711, Nr 157, poz. 1119, Nr 191, poz. 1413 i Nr 217, poz. 1590, z 2007 r. Nr 171, poz. 1207, z 2008 r. Nr 110, poz. 707, Nr 209, poz. 1318 i Nr 227, poz. 1505 oraz z 2009 r. Nr 18, poz. 97, Nr 85, poz. 716, Nr 166, poz. 1317 i Nr 201, poz. 1540.

13) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556, z 2008 r. Nr 17, poz. 101 i Nr 227, poz. 1505 oraz z 2009 r. Nr 11, poz. 59, Nr 18, poz. 97 i Nr 85, poz. 716.

14) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708, Nr 170, poz. 1217 i Nr 220, poz. 1600, z 2007 r. Nr 64, poz. 426, z 2008 r. Nr 227, poz. 1505 oraz z 2009 r. Nr 39, poz. 307 i Nr 166, poz. 1317.

15) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2000 r. Nr 120, poz. 1268, z 2002 r. Nr 112, poz. 984, z 2003 r. Nr 80, poz. 717 i Nr 162, poz. 1568, z 2006 r. Nr 220, poz. 1600, z 2008 r. Nr 216, poz. 1367 oraz z 2009 r. Nr 98, poz. 817.

16) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 49, poz. 509, z 2002 r. Nr 113, poz. 984, Nr 153, poz. 1271 i Nr 169, poz. 1387, z 2003 r. Nr 130, poz. 1188 i Nr 170, poz. 1660, z 2004 r. Nr 162, poz. 1692, z 2005 r. Nr 64, poz. 565, Nr 78, poz. 682 i Nr 181, poz. 1524, z 2008 r. Nr 229, poz. 1539 oraz z 2009 r. Nr 195, poz. 1501.

17) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1965 r. Nr 15, poz. 113, z 1974 r. Nr 27, poz. 157 i Nr 39, poz. 231, z 1975 r. Nr 45, poz. 234, z 1982 r. Nr 11, poz. 82 i Nr 30, poz. 210, z 1983 r. Nr 5, poz. 33, z 1984 r. Nr 45, poz. 241 i 242, z 1985 r. Nr 20, poz. 86, z 1987 r. Nr 21, poz. 123, z 1988 r. Nr 41, poz. 324, z 1989 r. Nr 4, poz. 21 i Nr 33, poz. 175, z 1990 r. Nr 14, poz. 88, Nr 34, poz. 198, Nr 53, poz. 306, Nr 55, poz. 318 i Nr 79, poz. 464, z 1991 r. Nr 7, poz. 24, Nr 22, poz. 92 i Nr 115, poz. 496, z 1993 r. Nr 12, poz. 53, z 1994 r. Nr 105, poz. 509, z 1995 r. Nr 83, poz. 417 i Nr 141, poz. 692, z 1996 r. Nr 24, poz. 110, Nr 43, poz. 189, Nr 73, poz. 350 i Nr 149, poz. 703, z 1997 r. Nr 43, poz. 240, Nr 54, poz. 348, Nr 75, poz. 471, Nr 102, poz. 643, Nr 117, poz. 752, Nr 121, poz. 769 i 770, Nr 133, poz. 882, Nr 139, poz. 934, Nr 140, poz. 940 i Nr 141, poz. 944, z 1998 r. Nr 106, poz. 668 i Nr 117, poz. 757, z 1999 r. Nr 52, poz. 532, z 2000 r. Nr 22, poz. 269 i 271, Nr 48, poz. 552 i 554, Nr 55, poz. 665, Nr 73, poz. 852, Nr 94, poz. 1037, Nr 114, poz. 1191, Nr 122, poz. 1314, 1319 i 1322, z 2001 r. Nr 4, poz. 27, Nr 49, poz. 508, Nr 63, poz. 635, Nr 98, poz. 1069, 1070 i 1071, Nr 123, poz. 1353, Nr 125, poz. 1368 i Nr 138, poz. 1546, z 2002 r. Nr 25, poz. 253, Nr 26, poz. 265, Nr 74, poz. 676, Nr 84, poz. 764, Nr 126, poz. 1069 i 1070, Nr 129, poz. 1102, Nr 153, poz. 1271, Nr 219, poz. 1849 i Nr 240, poz. 2058, z 2003 r. Nr 41, poz. 360, Nr 42, poz. 363, Nr 60, poz. 535, Nr 109, poz. 1035, Nr 119, poz. 1121, Nr 130, poz. 1188, Nr 139, poz. 1323, Nr 199, poz. 1939 i Nr 228, poz. 2255, z 2004 r. Nr 9, poz. 75, Nr 11, poz. 101, Nr 68, poz. 623, Nr 91, poz. 871, Nr 93, poz. 891, Nr 121, poz. 1264, Nr 162, poz. 1691, Nr 169, poz. 1783, Nr 172, poz. 1804, Nr 204, poz. 2091, Nr 210, poz. 2135, Nr 236, poz. 2356 i Nr 237, poz. 2384, z 2005 r. Nr 13, poz. 98, Nr 22, poz. 185, Nr 86, poz. 732, Nr 122, poz. 1024, Nr 150, poz. 1239, Nr 143, poz. 1199, Nr 167, poz. 1398, Nr 169, poz. 1413 i 1417, Nr 172, poz. 1438, Nr 178, poz. 1478, Nr 183, poz. 1538 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 66, poz. 466, Nr 104, poz. 708 i 711, Nr 186, poz. 1379, Nr 208, poz. 1537 i 1540, Nr 226, poz. 1656 i Nr 235, poz. 1699, z 2007 r. Nr 7, poz. 58, Nr 47, poz. 319, Nr 50, poz. 331, Nr 61, poz. 418, Nr 99, poz. 662, Nr 106, poz. 731, Nr 112, poz. 766 i 769, Nr 115, poz. 794, Nr 121, poz. 831, Nr 123, poz. 849, Nr 176, poz. 1243, Nr 181, poz. 1287, Nr 192, poz. 1378 i Nr 247, poz. 1845, z 2008 r. Nr 59, poz. 367, Nr 96, poz. 609 i 619, Nr 110, poz. 706, Nr 116, poz. 731, Nr 119, poz. 772, Nr 120, poz. 779, Nr 122, poz. 796, Nr 171, poz. 1056, Nr 220, poz. 1431, Nr 228, poz. 1507, Nr 231, poz. 1547 i Nr 234, poz. 1571 oraz z 2009 r. Nr 26, poz. 156, Nr 67, poz. 571, Nr 69, poz. 592 i 593, Nr 131, poz. 1075 i Nr 179, poz. 1395.

18) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 277, poz. 2742, z 2005 r. Nr 180, poz. 1496, z 2006 r. Nr 104, poz. 708, Nr 104, poz. 711 i Nr 220, poz. 1600, z 2007 r. Nr 107, poz. 732, Nr 176, poz. 1242, z 2008 r. Nr 171, poz. 1056, Nr 180, poz. 1109, Nr 206, poz. 1288, Nr 208, poz. 1308, Nr 223, poz. 1458 oraz z 2009 r. Nr 22, poz. 120, Nr 97, poz. 801, Nr 161, poz. 1278 i Nr 190, poz. 1474.

[19] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 1998 r. Nr 106, poz. 668 i Nr 113, poz. 717, z 1999 r. Nr 99, poz. 1152, z 2000 r. Nr 19, poz. 239, Nr 43, poz. 489, Nr 107, poz. 1127 i Nr 120, poz. 1268, z 2001 r. Nr 11, poz. 84, Nr 28, poz. 301, Nr 52, poz. 538, Nr 99, poz. 1075, Nr 111, poz. 1194, Nr 123, poz. 1354, Nr 128, poz. 1405 i Nr 154, poz. 1805, z 2002 r. Nr 74, poz. 676, Nr 135, poz. 1146, Nr 196, poz. 1660, Nr 199, poz. 1673 i Nr 200, poz. 1679, z 2003 r. Nr 166, poz. 1608 i Nr 213, poz. 2081, z 2004 r. Nr 96, poz. 959, Nr 99, poz. 1001, Nr 120, poz. 1252 i Nr 240, poz. 2407, z 2005 r. Nr 10, poz. 71, Nr 68, poz. 610, Nr 86, poz. 732 i Nr 167, poz. 1398, z 2006 r. Nr 104, poz. 708 i 711, Nr 133, poz. 935, Nr 217, poz. 1587 i Nr 221, poz. 1615, z 2007 r. Nr 64, poz. 426, Nr 89, poz. 589, Nr 176, poz. 1239, Nr 181, poz. 1288 i Nr 225, poz. 1672, z 2008 r. Nr 93, poz. 586, Nr 116, poz. 740, Nr 223, poz. 1460 i Nr 237, poz. 1654 oraz z 2009 r. Nr 6, poz. 33, Nr 56, poz. 458, Nr 58, poz. 485, Nr 98, poz. 817, Nr 99, poz. 825, Nr 115, poz. 958 i Nr 157, poz. 1241.

[20] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 1989 r. Nr 74, poz. 442, z 1991 r. Nr 60, poz. 253 i Nr 111, poz. 480, z 1994 r. Nr 121, poz. 591, z 1995 r. Nr 141, poz. 692, z 1997 r. Nr 121, poz. 770 i Nr 121, poz. 769, z 1998 r. Nr 106, poz. 668, z 2002 r. Nr 153, poz. 1271 oraz z 2004 r. Nr 173, poz.1808.

[21] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 98, poz. 1071, Nr 123, poz. 1353 i Nr 128, poz. 1403, z 2002 r. Nr 153, poz. 1271 i Nr 240, poz. 2052, z 2005 r. Nr 10, poz. 71 i Nr 169, poz. 1417, z 2006 r. Nr 45, poz. 319, Nr 170, poz. 1218, Nr 218, poz. 1592 i Nr 220, poz. 1600, z 2007 r. Nr 89, poz. 589 oraz z 2008 r. Nr 157, poz. 976 i Nr 227, poz. 1505.

[22] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1985 r. Nr 35, poz. 162, z 1996 r. Nr 24, poz. 110, z 1998 r. Nr 113, poz. 717 oraz z 2001 r. Nr 128, poz. 1405.

[23] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708, Nr 170, poz. 1217 i Nr 220, poz. 1600, z 2007 r. Nr 64, poz. 426, z 2008 r. Nr 227, poz. 1505 oraz z 2009 r. Nr 39, poz. 307 i Nr 166, poz. 1317.

[24] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1988 r. Nr 41, poz. 324, z 1989 r. Nr 34, poz. 187, z 1990 r. Nr 29, poz. 173, z 1991 r. Nr 100, poz. 442, z 1996 r. Nr 114, poz. 542, z 1997 r. Nr 88, poz. 554 i Nr 121, poz. 770, z 1999 r. Nr 90, poz. 999, z 2001 r. Nr 112, poz. 1198, z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 111, poz. 1181, z 2005 r. Nr 39, poz. 377 oraz z 2007 r. Nr 89, poz. 590.

[25] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 143, poz. 1032, Nr 170, poz. 1214, Nr 171, poz. 1225 i Nr 220, poz. 1600, z 2007 r. Nr 176, poz. 1238, z 2008 r. Nr 227, poz. 1505 i Nr 234, poz. 1570 oraz z 2009 r. Nr 18, poz. 97, Nr 20, poz. 106, Nr 92, poz. 753 i Nr 157, poz. 1241.

[26] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2009 r. Nr 1, poz. 4, Nr 26, poz. 156, Nr 26, poz. 157, Nr 56, poz. 459, Nr 178, poz. 1375 i Nr 190, poz. 1474.

[27] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 170, poz. 1217, z 2007 r. Nr 21, poz. 125, z 2008 r. Nr 201, poz. 1237 i Nr 227, poz. 1505 oraz z 2009 r. Nr 31, poz. 206, Nr 42, poz. 334, Nr 98, poz. 817 i Nr 157, poz. 1241.

[28] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 57, poz. 390, Nr 120, poz. 818, Nr 140, poz. 981 i Nr 165, poz. 1170, z 2008 r. Nr 86, poz. 521, Nr 171, poz. 1065 i Nr 237, poz. 1651 oraz z 2009 r. Nr 22, poz. 120, Nr 62, poz. 504, Nr 85, poz. 716, Nr 97, poz. 803, Nr 98, poz. 817, Nr 115, poz. 959, Nr 168, poz. 1323, Nr 195, poz. 1502, Nr 201, poz. 1540, Nr 206, poz. 1589 i Nr 157, poz. 1241.

[29] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708 i 711 i Nr 170, poz. 1218, z 2007 r. Nr 57, poz. 390 i Nr 82, poz. 558, z 2008 r. Nr 86, poz. 521, Nr 195, poz. 1199, Nr 216, poz. 1367 i Nr 227, poz. 1505 oraz z 2009 r. Nr 22, poz. 120, Nr 85, poz. 716, Nr 98, poz. 817, Nr 168, poz. 1323, Nr 201, poz. 1540 i Nr 157, poz. 1241.

[30] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 75, poz. 493, Nr 88, poz. 587 i Nr 124, poz. 859, z 2008 r. Nr 138, poz. 865, Nr 199, poz. 1227 i Nr 227, poz. 1505 oraz z 2009 r. Nr 18, poz. 97, Nr 31, poz. 206, Nr 79, poz. 666 i Nr 130, poz. 1070.

[31] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2000 r. Nr 22, poz. 270, Nr 60, poz. 703, Nr 70, poz. 816, Nr 101, poz. 1090, Nr 104, poz. 1104, Nr 117, poz. 1228 i Nr 122, poz. 1324, z 2001 r. Nr 4, poz. 27, Nr 8, poz. 64, Nr 52, poz. 539, Nr 73, poz. 764, Nr 74, poz. 784, Nr 88, poz. 961, Nr 89, poz. 968, Nr 102, poz. 1117, Nr 106, poz. 1150, Nr 110, poz. 1190, Nr 125, poz. 1363 i Nr 134, poz. 1509, z 2002 r. Nr 25, poz. 253, Nr 74, poz. 676, Nr 89, poz. 804, Nr 135, poz. 1146, Nr 141, poz. 1182, Nr 169, poz. 1384, Nr 181, poz. 1515, Nr 200, poz. 1679 i 1691 i Nr 240, poz. 2058, z 2003 r. Nr 7, poz. 79, Nr 45, poz. 391, Nr 65, poz. 595, Nr 84, poz. 774, Nr 90, poz. 844, Nr 96, poz. 874, Nr 122, poz. 1143, Nr 135, poz. 1268, Nr 137, poz. 1302, Nr 166, poz. 1608, Nr 202, poz. 1956, Nr 223, poz. 2217 i Nr 228, poz. 2255, z 2004 r. Nr 29, poz. 257, Nr 54, poz. 535, Nr 93, poz. 894, Nr 99, poz. 1001, Nr 109, poz. 1163, Nr 116, poz. 1203 i 1205, Nr 116, poz. 1207, Nr 120, poz. 1252, Nr 123, poz. 1291, Nr 162, poz. 1691,

Nr 210, poz. 2135, Nr 263, poz. 2619 i Nr 281, poz. 2779 i 2781, z 2005 r. Nr 25, poz. 202, Nr 85, poz. 725, Nr 86, poz. 732, Nr 90, poz. 757, Nr 102, poz. 852, Nr 143, poz. 1199 i 1202, Nr 155, poz. 1298, Nr 164, poz. 1365 i 1366, Nr 169, poz. 1418 i 1420, Nr 177, poz. 1468, Nr 179, poz. 1484, Nr 180, poz. 1495 i Nr 183, poz. 1538, z 2006 r. Nr 46, poz. 328, Nr 104, poz. 708 i 711, Nr 107, poz. 723, Nr 157, poz. 1119, Nr 183, poz. 1353 i 1354, Nr 217, poz. 1588, Nr 226, poz. 1657 i Nr 249, poz. 1824, z 2007 r. Nr 35, poz. 219, Nr 99, poz. 658, Nr 115, poz. 791 i 793, Nr 176, poz. 1243, Nr 181, poz. 1288, Nr 191, poz. 1361 i 1367, Nr 192, poz. 1378, Nr 211, poz. 1549 i Nr 225, poz. 1673, z 2008 r. Nr 97, poz. 623, Nr 141, poz. 888, Nr 143, poz. 894, Nr 209, poz. 1316, Nr 217, poz. 1588, Nr 220, poz. 1431 i 1432, Nr 223, poz. 1459 i Nr 228, poz. 1507 oraz z 2009 r. Nr 3, poz. 11, Nr 6, poz. 33, Nr 19, poz. 100, Nr 69, poz. 587, Nr 79, poz. 666, Nr 91, poz. 741, Nr 97, poz. 800, Nr 115, poz. 964, Nr 125, poz. 1035 i 1037, Nr 127, poz. 1052, Nr 157, poz. 1241, Nr 161, poz. 1278, Nr 168, poz. 1323, Nr 201, poz. 1540 i 1541.

[32] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 64, poz. 594, Nr 91, poz. 868, Nr 171, poz. 1800 i Nr 173, poz. 1808, z 2005 r. Nr 132, poz. 1110 i Nr 183, poz. 1537, z 2006 r. Nr 66, poz. 470, Nr 104, poz. 708 i 711, Nr 157, poz. 1119, Nr 191, poz. 1413 i Nr 217, poz. 1590, z 2007 r. Nr 171, poz. 1207, z 2008 r. Nr 110, poz. 707, Nr 209, poz. 1318 i Nr 227, poz. 1505 oraz z 2009 r. Nr 18, poz. 97, Nr 85, poz. 716, Nr 166, poz. 1317 i Nr 201, poz. 1540.

[33] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 17, poz. 141, Nr 85, poz. 728 i Nr 267, poz. 2258, z 2006 r. Nr 83, poz. 574, Nr 133, poz. 935 i Nr 218, poz. 1592, z 2007 r. Nr 61, poz. 411 oraz z 2009 r. Nr 18, poz. 97, Nr 115, poz. 965 i Nr 201, poz. 1540.

[34] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1997 r. Nr 113, poz. 731 i Nr 88, poz. 554, z 1998 r. Nr 106, poz. 668, z 1999 r. Nr 11, poz. 95, z 2000 r. Nr 120, poz. 1268, z 2005 r. Nr 141, poz. 1183, Nr 167, poz. 1398 i Nr 175, poz. 1462, z 2007 r. Nr 112, poz. 766 i Nr 121, poz. 831, z 2008 r. Nr 180, poz. 1108 oraz z 2009 r. Nr 76, poz. 641 i Nr 98, poz. 817.

[35] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 209, poz. 1315, Nr 225, poz. 1502 i Nr 227, poz. 1505.

[36] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 14, poz. 113, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 112, poz. 769, z 2008 r. Nr 209, poz. 1318, z 2009 r. Nr 3, poz. 11, Nr 18, poz. 97 i Nr 166, poz. 1317.

[37] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2003 r. Nr 90, poz. 844, Nr 142, poz. 1380, Nr 166, poz. 1609 i Nr 210, poz. 2036, z 2004 r. Nr 273, poz. 2703 oraz z 2006 r. Nr 104, poz. 708 i 711.

[38] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 116, poz. 1202 i Nr 210, poz. 2135, z 2005 r. Nr 48, poz. 446 i Nr 169, poz. 1414, z 2006 r. Nr 104, poz. 708 oraz z 2009 r. Nr 144, poz. 1177.

[39] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1997 r. Nr 70, poz. 443 i Nr 141, poz. 943, z 1998 r. Nr 131, poz. 860 oraz z 2006 r. Nr 218, poz. 1592.

[40] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 240, poz. 2055, z 2003 r. Nr 60, poz. 535 i Nr 90, poz. 844, z 2004 r. Nr 6, poz. 39, Nr 116, poz. 1207, Nr 123, poz. 1291 i Nr 273, poz. 2703 i 2722, z 2005 r. Nr 167, poz. 1400, Nr 169, poz. 1418, Nr 178, poz. 1479 i Nr 184, poz. 1539, z 2006 r. Nr 107, poz. 721 i Nr 208, poz. 1532, z 2008 r. Nr 180, poz. 1109 oraz z 2009 r. Nr 13, poz. 70.

[41] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1997 r. Nr 128, poz. 840, z 1999 r. Nr 64, poz. 729 i Nr 83, poz. 931, z 2000 r. Nr 48, poz. 548, Nr 93, poz. 1027 i Nr 116, poz. 1216, z 2001 r. Nr 98, poz. 1071, z 2003 r. Nr 111, poz. 1061, Nr 179, poz. 1750 i Nr 228, poz. 2255, z 2004 r. Nr 25, poz. 219, Nr 69, poz. 626, Nr 93, poz. 889 i Nr 243, poz. 2426, z 2005 r. Nr 86, poz. 732, Nr 90, poz. 757, Nr 132, poz. 1109, Nr 163, poz. 1363, Nr 178, poz. 1479 i Nr 180, poz. 1493, z 2006 r. Nr 190, poz. 1409, Nr 218, poz. 1592 i Nr 226, poz. 1648, z 2007 r. Nr 89, poz. 589, Nr 123, poz. 850, Nr 124, poz. 859 i Nr 192, poz. 1378, z 2008 r. Nr 90, poz. 560, Nr 122, poz. 782, Nr 171, poz. 1056, Nr 173, poz. 1080 i Nr 214, poz. 1344 oraz z 2009 r. Nr 62, poz. 504, Nr 166, poz. 1317, Nr 168, poz. 1323, Nr 190, poz. 1474, Nr 201, poz. 1540 i Nr 206, poz. 1589.

[42] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1999 r. Nr 83, poz. 931, z 2000 r. Nr 50, poz. 580, Nr 62, poz. 717, Nr 73, poz. 852 i Nr 93, poz. 1027, z 2001 r. Nr 98, poz. 1071 i Nr 106, poz. 1149, z 2002 r. Nr 74, poz. 676, z 2003 r. Nr 17, poz. 155, Nr 111, poz. 1061 i Nr 130, poz. 1188, z 2004 r. Nr 51, poz. 514, Nr 69, poz. 626, Nr 93, poz. 889, Nr 240, poz. 2405 i Nr 264, poz. 2641, z 2005 r. Nr 10, poz. 70, Nr 48, poz. 461, Nr 77, poz. 680, Nr 96, poz. 821, Nr 141, poz. 1181, Nr 143, poz. 1203, Nr 163, poz. 1363, Nr 169, poz. 1416 i Nr 178, poz. 1479, z 2006 r. Nr 15, poz. 118, Nr 66, poz. 467, Nr 95, poz. 659, Nr 104, poz. 708 i 711, Nr 141, poz. 1009 i 1013, Nr 167, poz. 1192 i Nr 226, poz. 1647 i 1648, z 2007 r. Nr 20, poz. 116, Nr 64, poz. 432, Nr 80, poz. 539, Nr 89, poz. 589, Nr 99, poz. 664, Nr 112, poz. 766, Nr 123, poz. 849 i Nr 128, poz. 903, z 2008 r. Nr 27, poz. 162, Nr 100, poz. 648, Nr 107, poz. 686, Nr 123, poz. 802, Nr 182, poz. 1133, Nr 208, poz. 1308, Nr 214, poz. 903, Nr 225, poz. 1485, Nr 234, poz. 1571 i Nr 237, poz. 1651

oraz z 2009 r. Nr 8, poz. 39, Nr 20, poz. 104, Nr 28, poz. 171, Nr 68, poz. 585, Nr 85, poz. 716, Nr 127, poz. 1051, Nr 144, poz. 1178, Nr 168, poz. 1323, Nr 190, poz. 1474 i Nr 206, poz. 1586.

43) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1997 r. Nr 160, poz. 1083, z 1999 r. Nr 83, poz. 931, z 2000 r. Nr 60, poz. 701 i Nr 120, poz. 1268, z 2001 r. Nr 98, poz. 1071 i Nr 111, poz. 1194, z 2002 r. Nr 74, poz. 676 i Nr 200, poz. 1679, z 2003 r. Nr 111, poz. 1061, Nr 142, poz. 1380 i Nr 179, poz. 1750, z 2004 r. Nr 93, poz. 889, Nr 210, poz. 2135, Nr 240, poz. 2405, Nr 243, poz. 2426 i Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1363 i Nr 178, poz. 1479, z 2006 r. Nr 104, poz. 708 i Nr 226, poz. 1648, z 2007 r. Nr 123, poz. 849, z 2008 r. Nr 214, poz. 1344 oraz z 2009 r. Nr 8, poz. 39, Nr 22, poz. 119, Nr 62, poz. 504, Nr 96, poz. 620, Nr 98, poz. 817, Nr 108, poz. 911, Nr 115, poz. 963, Nr 190, poz. 1475 i Nr 201, poz. 1540.

44) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 109, poz. 925, Nr 175, poz. 1462, Nr 179, poz. 1486, Nr 180, poz. 1494 i Nr 180, poz. 1497, z 2006 r. Nr 17, poz. 141, Nr 104, poz. 708 i 711, Nr 190, poz. 1400, Nr 191, poz. 1410 i Nr 235, poz. 1701, z 2007 r. Nr 52, poz. 343, Nr 57, poz. 381, Nr 99, poz. 661, Nr 123, poz. 845 i Nr 176, poz. 1238, z 2008 r. Nr 37, poz. 214, Nr 100, poz. 649, Nr 163, poz. 1015, Nr 209, poz. 1320, Nr 220, poz. 1411 i 1426, Nr 223, poz. 1461 i 1462, Nr 234, poz. 1573 i 1574 oraz z 2009 r. Nr 3, poz. 11, Nr 18, poz. 97, Nr 79, poz. 663, Nr 91, poz. 739, Nr 92, poz. 753, Nr 97, poz. 802 i 803, Nr 98, poz. 817 i Nr 168, poz. 1323.

45) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2000 r. Nr 48, poz. 552 i Nr 53, poz. 638, z 2001 r. Nr 98, poz. 1070, z 2005 r. Nr 169, poz. 1417 oraz z 2009 r. Nr 56, poz. 459.

46) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 237, poz. 1651 oraz z 2009 r. Nr 26, poz. 157, Nr 56, poz. 459 i Nr 157, poz. 1241.

47) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 143, poz. 1202 i Nr 183, poz. 1538, z 2006 r. Nr 104, poz. 708 i 711 i Nr 157, poz. 1119, z 2007 r. Nr 17, poz. 95, z 2008 r. Nr 180, poz. 1109 i Nr 228, poz. 1507 oraz z 2009 r. Nr 18, poz. 97, Nr 86, poz. 720, Nr 127, poz. 1048 i Nr 165, poz. 1316.

48) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 113, poz. 984, z 2003 r. Nr 130, poz. 1190, z 2008 r. Nr 223, poz. 1458, oraz z 2009 r. Nr 97, poz. 803.

49) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 218, poz. 1592, z 2007 r. Nr 44, poz. 228, Nr 85, poz. 571 i Nr 112, poz. 769 oraz z 2009 r. Nr 26, poz. 156, Nr 81, poz. 687 i Nr 105, poz. 879.

50) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 85, poz. 727, Nr 86, poz. 732 i Nr 143, poz. 1199, z 2006 r. Nr 57, poz. 609 i 610, Nr 66, poz. 470, Nr 104, poz. 708, Nr 217, poz. 1590 i Nr 225, poz. 1635, z 2007 r. Nr 105, poz. 721, Nr 112, poz. 769, Nr 120, poz. 818, Nr 192, poz. 1378, Nr 195, poz. 1414 i Nr 225, poz. 1671, z 2008 r. Nr 118, poz. 745, Nr 141, poz. 888, Nr 180, poz. 1109 i Nr 209, poz. 1316, 1318 i 1320 oraz z 2009 r. Nr 18, poz. 97, Nr 44, poz. 362, Nr 57, poz. 466, Nr 166, poz. 1317 i Nr 168, poz. 1323.

51) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 126, poz. 1070, Nr 141, poz. 1178, Nr 144, poz. 1208, Nr 153, poz. 1271, Nr 169, poz. 1385 i 1387 i Nr 241, poz. 2074, z 2003 r. Nr 50, poz. 424, Nr 60, poz. 535, Nr 65, poz. 594, Nr 228, poz. 2260 i Nr 229, poz. 2276, z 2004 r. Nr 64, poz. 594, Nr 68, poz. 623, Nr 91, poz. 870, Nr 96, poz. 959, Nr 121, poz. 1264, Nr 146, poz. 1546 i Nr 173, poz. 1808, z 2005 r. Nr 83, poz. 719, Nr 85, poz. 727, Nr 167, poz. 1398 i Nr 183, poz. 1538, z 2006 r. Nr 104, poz. 708, Nr 157, poz. 1119, Nr 190, poz. 1401 i Nr 245, poz. 1775, z 2007 r. Nr 42, poz. 272 i Nr 112, poz. 769, z 2008 r. Nr 171, poz. 1056, Nr 192, poz. 1179, Nr 209, poz. 1315 i Nr 231, poz. 1546 oraz z 2009 r. Nr 18, poz. 97, Nr 42, poz. 341, Nr 65, poz. 545, Nr 71, poz. 609, Nr 127, poz. 1045, Nr 144, poz. 1176, Nr 165, poz. 1316, Nr 166, poz. 1317, Nr 168, poz. 1323 i Nr 201, poz. 1540.

52) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711 oraz z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238.

53) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 237, poz. 1654 i Nr 237, poz. 1656 oraz z 2009 r. Nr 71, poz. 609, Nr 131, poz. 1075, Nr 157, poz. 1241 i Nr 161, poz. 1278.

54) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 64, poz. 432, Nr 83, poz. 561, Nr 85, poz. 571 i Nr 140, poz. 983.

55) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 98, poz. 1070, z 2003 r. Nr 228, poz. 2256, z 2005 r. Nr 10, poz. 71, z 2007 r. Nr 64, poz. 432, Nr 64, poz. 433, Nr 102, poz. 690 i Nr 136, poz. 959 oraz z 2009 r. Nr 26, poz. 157 i Nr 178, poz. 1375.

56) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 33, poz. 286, z 2005 r. Nr 10, poz. 68, Nr 163, poz. 1362 i Nr 167, poz. 1398, z 2006 r. Nr 170, poz. 1217 i 1218 i Nr 208, poz. 1539, z 2007 r. Nr 99, poz. 662 i Nr 136, poz. 958 oraz z 2008 r. Nr 180, poz. 1113, Nr 216, poz. 1368 i Nr 227, poz. 1505.

[57] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 183, poz. 1537 i 1538, z 2006 r. Nr 157, poz. 1119, z 2007 r. Nr 112, poz. 769, z 2008 r. Nr 171, poz. 1056 oraz z 2009 r. Nr 165, poz. 1316, Nr 168, poz. 1323 i Nr 201, poz. 1540.

[58] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 62, poz. 577, Nr 96, poz. 959 i Nr 116, poz. 1203, z 2005 r. Nr 183, poz. 1538, z 2006 r. Nr 104, poz. 708 i 711 i Nr 157, poz. 1119, z 2008 r. Nr 171, poz. 1056 i Nr 180, poz. 1109 oraz z 2009 r. Nr 42, poz. 341, Nr 165, poz. 1316, Nr 166, poz. 1317, Nr 168, poz. 1323 i Nr 201, poz. 1540.

[59] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 123, poz. 846 i Nr 176, poz. 1238, z 2008 r. Nr 171, poz. 1057 oraz z 2009 r. Nr 98, poz. 818.

[60] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 210, poz. 2135, z 2006 r. Nr 104, poz. 708 i 711, z 2008 r. Nr 66, poz. 402 oraz z 2009 r. Nr 22, poz. 120 i Nr 85, poz. 716.

[61] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 220, poz. 1600, z 2007 r. Nr 120, poz. 818 i Nr 165, poz. 1170, z 2008 r. Nr 157, poz. 976 oraz z 2009 r. Nr 69, poz. 595 i Nr 201, poz. 1540.

[62] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 267, poz. 2255, z 2006 r. Nr 170, poz. 1217 i Nr 227, poz. 1658, z 2007 r. Nr 21, poz. 125, Nr 64, poz. 427, Nr 75, poz. 493, Nr 88, poz. 587, Nr 147, poz. 1033, Nr 176, poz. 1238, Nr 181, poz. 1286 i Nr 231, poz. 1704, z 2008 r. Nr 199, poz. 1227 i Nr 227, poz. 1505 oraz z 2009 r. Nr 168, poz. 1323.

[63] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 154, poz. 1787, z 2002 r. Nr 153, poz. 1271 i Nr 213, poz. 1802, z 2003 r. Nr 228, poz. 2256 oraz z 2005 r. Nr 169, poz. 1410.

[64] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 154, poz. 1787, z 2002 r. Nr 153, poz. 1271, Nr 213, poz. 1802 i Nr 240, poz. 2052, z 2003 r. Nr 188, poz. 1838 i Nr 228, poz. 2256, z 2004 r. Nr 34, poz. 304, Nr 130, poz. 1376, Nr 185, poz. 1907, Nr 273, poz. 2702 i 2703, z 2005 r. Nr 13, poz. 98, Nr 131, poz. 1102, Nr 167, poz. 1398, Nr 169, poz. 1410, 1413 i 1417, Nr 178, poz. 1479 i Nr 249, poz. 2104, z 2006 r. Nr 144, poz. 1044 i Nr 218, poz. 1592, z 2007 r. Nr 64, poz. 433, Nr 73, poz. 484, Nr 99, poz. 664, Nr 112, poz. 766, Nr 136, poz. 959, Nr 138, poz. 976, Nr 204, poz. 1482 i Nr 230, poz. 1698, z 2008 r. Nr 41, poz. 251, Nr 223, poz. 1457, Nr 228, poz. 1507 i Nr 234, poz. 1571 oraz z 2009 r. Nr 1, poz. 4, Nr 9, poz. 57, Nr 26, poz. 156 i 157, Nr 56, poz. 459, Nr 157, poz. 1241 i Nr 178, poz. 1375.

[65] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 214, poz. 1344 i Nr 237, poz. 1651 oraz z 2009 r. Nr 178, poz. 1375, Nr 190, poz. 1474 i Nr 206, poz. 1589.

[66] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. 2001 r. Nr 154, poz. 1800, z 2002 r. Nr 74, poz. 676 i Nr 89, poz. 804, z 2003 r. Nr 113, poz. 1070 i Nr 139, poz. 1326, z 2004 r. Nr 116, poz. 1203, Nr 171, poz. 1800 i Nr 273, poz. 2703, z 2006 r. Nr 104, poz. 711, z 2007 r. Nr 176, poz. 1242 oraz z 2009 r. Nr 85, poz. 716, Nr 157, poz. 1241 i Nr 190, poz. 1474.

[67] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. 2002 r. Nr 153, poz. 1271, z 2003 r. Nr 124, poz. 1152 i Nr 217, poz. 2125, z 2004 r. Nr 96, poz. 959, z 2005 r. Nr 64, poz. 565, z 2006 r. Nr 145, poz. 1050 oraz z 2009 r. Nr 18, poz. 97.

[68] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2003 r. Nr 90, poz. 844, Nr 113, poz. 1070, Nr 130, poz. 1188 i Nr 166, poz. 1609, z 2004 r. Nr 109, poz. 1159, Nr 171, poz. 1800, Nr 267, poz. 2647 i Nr 273, poz. 2703, z 2006 r. Nr 104, poz. 708 i 711 i Nr 218, poz. 1592, z 2008 r. Nr 11, poz. 59 i Nr 220, poz. 1428 oraz z 2009 r. Nr 85, poz. 716, Nr 98, poz. 817 i Nr 157, poz. 1241.

[69] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 162, poz. 1692, z 2005 r. Nr 94, poz. 788, Nr 169, poz. 1417 i Nr 250, poz. 2118, z 2006 r. Nr 38, poz. 268, Nr 208, poz. 1536 i Nr 217, poz. 1590, z 2007 r. Nr 120, poz. 818, Nr 121, poz. 831 i Nr 221, poz. 1650, z 2008 r. Nr 190, poz. 1171 i Nr 216, poz. 1367 oraz z 2009 r. Nr 53, poz. 433, Nr 144, poz. 1179 i Nr 178, poz. 1375.

[70] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 25, poz. 219, z 2006 r. Nr 157, poz. 1119, z 2008 r. Nr 234, poz. 1571 oraz z 2009 r. Nr 56, poz. 459, Nr 157, poz. 1241 i Nr 178, poz. 1375.

[71] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 96, poz. 959 i Nr 120, poz. 1252, z 2005 r. Nr 94, poz. 788, z 2006 r. Nr 144, poz. 1043, z 2007 r. Nr 120, poz. 818 i Nr 176, poz. 1241, z 2008 r. Nr 70, poz. 416 oraz z 2009 r. Nr 97, poz. 800.

[72] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 206, poz. 1288 i Nr 208, poz. 1308 oraz z 2009 r. Nr 26, poz. 157 i Nr 79, poz. 669.

[73] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 171, poz. 1058, Nr 220, poz. 1420 i Nr 227, poz. 1505 oraz z 2009 r. Nr 19, poz. 101, Nr 65, poz. 545, Nr 91, poz. 742, Nr 157, poz. 1241 i Nr 206, poz. 1591.

[74] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 64, poz. 565, z 2007 r. Nr 176, poz. 1238 oraz z 2008 r. Nr 157, poz. 976.

[75)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. 2005 r. Nr 83, poz. 719, Nr 183, poz. 1537 i 1538 i Nr 184, poz. 1539, z 2006 r. Nr 157, poz. 1119, z 2007 r. Nr 112, poz. 769, z 2008 r. Nr 231, poz. 1546 oraz z 2009 r. Nr 18, poz. 97, Nr 42, poz. 341, Nr 168, poz. 1323 i Nr 201, poz. 1540.

[76)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 96, poz. 959 i Nr 173, poz. 1808, z 2007 r. Nr 50, poz. 331, z 2008 r. Nr 171, poz. 1056 i Nr 216, poz. 1371 oraz z 2009 r. Nr 201, poz. 1540.

[77)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 216, poz. 1367, Nr 225, poz. 1486, Nr 227, poz. 1505, Nr 234, poz. 1570 i Nr 237, poz. 1654 oraz z 2009 r. Nr 6, poz. 33, Nr 22, poz. 120, Nr 26, poz. 157, Nr 38, poz. 299, Nr 92, poz. 753, Nr 97, poz. 800, Nr 98, poz. 817, Nr 111, poz. 918, Nr 118, poz. 989, Nr 157, poz. 1241, Nr 161, poz. 1278 i Nr 178, poz. 1374.

[78)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556, z 2008 r. Nr 17, poz. 101 i Nr 227, poz. 1505 oraz z 2009 r. Nr 11, poz. 59, Nr 18, poz. 97 i Nr 85, poz. 716.

[79)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 249, poz. 2104, z 2006 r. Nr 79, poz. 551 oraz z 2009 r. Nr 19, poz. 101 i Nr 157, poz. 1241.

[80)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501, z 2008 r. Nr 127, poz. 817 oraz z 2009 r. Nr 157, poz. 1241.

[81)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 169, poz. 1420, z 2006 r. Nr 45, poz. 319, Nr 104, poz. 708, Nr 170, poz. 1217 i 1218, Nr 187, poz. 1381 i Nr 249, poz. 1832, z 2007 r. Nr 82, poz. 560, Nr 88, poz. 587, Nr 115, poz. 791 i Nr 140, poz. 984, z 2008 r. Nr 180, poz. 1112, Nr 209, poz. 1317, Nr 216, poz. 1370 i Nr 227, poz. 1505 oraz z 2009 r. Nr 19, poz. 100, Nr 62, poz. 504, Nr 72, poz. 619, Nr 79, poz. 666, Nr 157, poz. 1241 i Nr 161, poz. 1277.

[82)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 264, poz. 2205, z 2006 r. Nr 170, poz. 1217 i Nr 218, poz. 1592, z 2008 r. Nr 227, poz. 1505 oraz z 2009 r. Nr 26, poz. 156 i Nr 79, poz. 660.

[83)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708 i Nr 157, poz. 1119, z 2008 r. Nr 171, poz. 1056 oraz z 2009 r. Nr 13, poz. 69, Nr 42, poz. 341, Nr 77, poz. 649, Nr 78, poz. 659, Nr 165, poz. 1316, Nr 166, poz. 1317, Nr 168, poz. 1323 i Nr 201, poz. 1540.

[84)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 158, poz. 1122 i Nr 218, poz. 1592, z 2008 r. Nr 171, poz. 1056 oraz z 2009 r. Nr 18, poz. 97, Nr 85, poz. 716, Nr 105, poz. 880 i Nr 157, poz. 1241.

[85)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 214, poz. 1346, Nr 223, poz. 1463 i Nr 234, poz. 1570 oraz z 2009 r. Nr 98, poz. 817.

[86)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 83, poz. 561, Nr 85, poz. 571, Nr 115, poz. 789, Nr 165, poz. 1171 i Nr 176, poz. 1242 oraz z 2009 r. Nr 178, poz. 1375.

[87)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 237, poz. 1656 oraz z 2009 r. Nr 6, poz. 33 i Nr 20, poz. 106.

[88)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708 i 711, Nr 149, poz. 1078, Nr 218, poz. 1592 i Nr 220, poz. 1600, z 2008 r. Nr 171, poz. 1056 oraz z 2009 r. Nr 178, poz. 1375.

Załącznik
do ustawy
z dnia

ANKIETA BEZPIECZEŃSTWA OSOBOWEGO

Szanowna Pani, Szanowny Panie,

Rząd Rzeczypospolitej Polskiej, kierując się troską o bezpieczeństwo narodowe i mając na uwadze powinność jego ochrony, przedstawia tę ankietę w przekonaniu, iż zostanie ona wypełniona zgodnie z Pani (Pana) najlepszą wiedzą i wolą. Dziękując za współpracę, podkreślamy, że celem tej ankiety jest wyłącznie ochrona bezpieczeństwa narodowego przed zagrożeniami ze strony obcych służb specjalnych oraz ugrupowań terrorystycznych lub grup przestępczych. Prosimy uważnie przeczytać poniższą instrukcję, a w razie wątpliwości zwrócić się do pełnomocnika ochrony w Pani (Pana) jednostce organizacyjnej albo do Agencji Bezpieczeństwa Wewnętrznego bądź Służby Kontrwywiadu Wojskowego o pomoc w wypełnieniu ankiety.

Ankieta bezpieczeństwa osobowego, po wypełnieniu, stanowi tajemnicę prawnie chronioną i podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „poufne" w przypadku poszerzonego postępowania sprawdzającego lub „zastrzeżone" w przypadku zwykłego postępowania sprawdzającego. Jednocześnie informujemy Państwa, że informacje zawarte w niniejszej ankiecie są chronione ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) i mogą być wykorzystane jedynie do celów postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego, prowadzonego na podstawie przepisów ustawy z dnia o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. Nr , poz.). Akta zakończonego postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego mogą zostać udostępnione wyłącznie na żądanie sądu lub prokuratora w celu ścigania karnego lub podmiotom uprawnionym do prowadzenia postępowań sprawdzających, a także właściwemu organowi w celu rozpatrzenia odwołania lub dokonania sprawdzenia prawidłowości przeprowadzenia postępowania sprawdzającego oraz sądowi administracyjnemu w związku z rozpatrywaniem skargi.

Instrukcja

1. Przed wypełnieniem ankiety proszę się z nią dokładnie zapoznać.
2. Proszę wypełniać ankietę osobiście. Cudzoziemcy, niewładający językiem polskim, składają osobiście wypełnione ankiety w językach ojczystych, dołączając do nich tłumaczenie ich treści, wykonane przez tłumacza przysięgłego.
3. Jeśli ankieta zawiera zbyt mało miejsca na wpisanie danych, proszę je podać na osobnej karcie formatu A4, którą należy dołączyć do ankiety.
4. W przypadku udzielenia odpowiedzi twierdzącej na pytanie zasadnicze, proszę wypełnić wszystkie pozostałe rubryki odnoszące się do tego pytania.
5. W przypadku udzielenia odpowiedzi przeczącej na pytanie zasadnicze, proszę nie wypełniać pozostałych rubryk odnoszących się do tego pytania.
6. W razie braku wiedzy umożliwiającej podanie danych, proszę wpisać sformułowanie: „nie wiem” i podać przyczynę.
7. Informacje o partnerce (partnerze), o której (którym) mowa w części II B, należy podać tylko i wyłącznie wtedy, gdy związek z partnerką (partnerem) ma charakter trwałego i faktycznego pożycia.
8. Jeżeli dane w kolejnych punktach ankiety są identyczne z danymi podanymi w poprzednich punktach, można w kolejnych punktach wpisywać sformułowanie: „jak w pkt ...”.
9. Jeżeli któryś z członków rodziny zmarł, proszę ograniczać wypełnianie takiego fragmentu ankiety wyłącznie do podania jego imienia, nazwiska, daty i miejsca urodzenia oraz sformułowania: „nie żyje”.
10. Osoby objęte zwykłym postępowaniem sprawdzającym nie wypełniają części V, VI i VII ankiety.
11. Osoby objęte poszerzonym postępowaniem sprawdzającym, z wyjątkiem osób ubiegających się o wydanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne” lub stanowiącą jej odpowiednik klauzulą tajności organizacji międzynarodowej, nie wypełniają części VII ankiety.
12. Przy kolejnym postępowaniu sprawdzającym część III należy wypełnić wyłącznie z odniesieniem się do okresu, począwszy od daty wypełnienia poprzedniej ankiety do dnia wypełnienia następnej ankiety. Jeżeli dane odnoszące się do wyżej wymienionych punktów nie uległy zmianie, należy przy nich pisać sformułowanie: „bez zmian”.
13. Osoby objęte poszerzonym postępowaniem sprawdzającym mogą włożyć ankietę do koperty i zakleić.

CZĘŚĆ I: DANE OSOBOWE

KOLOROWE ZDJĘCIE
OSOBY SPRAWDZANEJ
(WYS. 5 cm × SZER. 4 cm)

1. NAZWISKO

2. PIERWSZE IMIĘ

3. DRUGIE IMIĘ

4. NAZWISKO RODOWE

5. INNE POPRZEDNIE NAZWISKA

6. DATA URODZENIA (DD-MM-RRRR)
– –

7. MIEJSCE URODZENIA (MIEJSCOWOŚĆ, PAŃSTWO)

8. POSIADANE OBYWATELSTWA (OD KIEDY?)

9. WCZEŚNIEJ POSIADANE OBYWATELSTWA (OD KIEDY – DO KIEDY?)

10. NR PESEL

11. NIP

12.1. NR DOWODU OSOBISTEGO

12.2. DATA WAŻNOŚCI DOWODU OSOBISTEGO

12.3. NAZWA ORGANU, KTÓRY WYDAŁ DOWÓD OSOBISTY

13. CZY POSIADA PANI (PAN) PASZPORT?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 13.1. – 13.4.)

TAK ☐ NIE ☐

13.1. NR PASZPORTU

13.2. DATA WAŻNOŚCI PASZPORTU

13.3. NAZWA ORGANU, KTÓRY WYDAŁ PASZPORT

13.4. CZY POSIADA PANI (PAN) INNY PASZPORT, NIŻ WSKAZANY W PKT 13.1. – 13.3.?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 13.1. – 13.4.)

TAK ☐ NIE ☐

14. CZY JEST LUB BYŁA PANI (BYŁ PAN) OBJĘTY POWSZECHNYM OBOWIĄZKIEM OBRONY?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 14.1. – 14.3.)

TAK ☐ NIE ☐

14.1. STOPIEŃ WOJSKOWY	14.2. NR WOJSKOWEGO DOKUMENTU TOŻSAMOŚCI
14.3. NAZWA ORGANU, KTÓRY WYDAŁ WOJSKOWY DOKUMENT TOŻSAMOŚCI	
15. NR TELEFONU KONTAKTOWEGO	
16. ADRES ZAMELDOWANIA (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)	
17. ADRES ZAMIESZKANIA (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)	
18. CZY JEST PANI (PAN) ZATRUDNIONA (ZATRUDNIONY) LUB PROWADZI DZIAŁALNOŚĆ GOSPODARCZĄ? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 18.1. – 18.4.) TAK ☐ NIE ☐	
18.1. NAZWA MIEJSCA ZATRUDNIENIA LUB PROWADZONEJ FIRMY	
18.2. ADRES MIEJSCA ZATRUDNIENIA LUB PROWADZONEJ FIRMY (ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)	
18.3. ZAJMOWANE STANOWISKO	
18.4. CZY POSIADA PANI (PAN) INNE MIEJSCE ZATRUDNIENIA, NIŻ WSKAZANE W PKT 18.1. – 18.3.? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 18.1. – 18.4.) TAK ☐ NIE ☐	

CZĘŚĆ II: DANE OSOBOWE CZŁONKÓW RODZINY

A. WSPÓŁMAŁŻONEK OSOBY SPRAWDZANEJ

1. CZY POZOSTAJE PANI (PAN) W ZWIĄZKU MAŁŻEŃSKIM? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 2. – 25.4.) TAK ☐ NIE ☐	
2. OD KIEDY? (DD-MM-RRRR) – –	3. MIEJSCE ZAWARCIA MAŁŻEŃSTWA (MIEJSCOWOŚĆ, PAŃSTWO)
4. NAZWISKO WSPÓŁMAŁŻONKA	
5. PIERWSZE IMIĘ WSPÓŁMAŁŻONKA	6. DRUGIE IMIĘ WSPÓŁMAŁŻONKA
7. NAZWISKO RODOWE WSPÓŁMAŁŻONKA	8. INNE POPRZEDNIE NAZWISKA WSPÓŁMAŁŻONKA
9. IMIĘ OJCA WSPÓŁMAŁŻONKA	10. NAZWISKO OJCA WSPÓŁMAŁŻONKA
11. NAZWISKO RODOWE OJCA WSPÓŁMAŁŻONKA	12. IMIĘ MATKI WSPÓŁMAŁŻONKA

13. NAZWISKO MATKI WSPÓŁMAŁŻONKA

14. NAZWISKO RODOWE MATKI WSPÓŁMAŁŻONKA

15. DATA URODZENIA (DD-MM-RRRR) WSPÓŁMAŁŻONKA

– –

16. MIEJSCE URODZENIA WSPÓŁMAŁŻONKA
(MIEJSCOWOŚĆ, PAŃSTWO)

17. OBYWATELSTWA POSIADANE PRZEZ WSPÓŁMAŁŻONKA (OD KIEDY?)

18. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ WSPÓŁMAŁŻONKA (OD KIEDY – DO KIEDY?)

19. NR PESEL WSPÓŁMAŁŻONKA

20. NIP WSPÓŁMAŁŻONKA

21.1. NR DOWODU OSOBISTEGO WSPÓŁMAŁŻONKA

21.2. DATA WAŻNOŚCI DOWODU OSOBISTEGO WSPÓŁMAŁŻONKA

21.3. NAZWA ORGANU, KTÓRY WYDAŁ DOWÓD OSOBISTY WSPÓŁMAŁŻONKA

22.1. NR PASZPORTU WSPÓŁMAŁŻONKA

22.2. DATA WAŻNOŚCI PASZPORTU WSPÓŁMAŁŻONKA

22.3. NAZWA ORGANU, KTÓRY WYDAŁ PASZPORT WSPÓŁMAŁŻONKA

22.4. CZY PANI (PANA) WSPÓŁMAŁŻONEK POSIADA INNY PASZPORT, NIŻ WSKAZANY W PKT 22.1. – 22.3.?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 22.1. – 22.4.)

TAK ☐ NIE ☐

23. ADRES ZAMELDOWANIA WSPÓŁMAŁŻONKA
(ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

24. ADRES ZAMIESZKANIA WSPÓŁMAŁŻONKA
(ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

25. CZY PANI (PANA) WSPÓŁMAŁŻONEK JEST ZATRUDNIONY LUB PROWADZI DZIAŁALNOŚĆ GOSPODARCZĄ?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 25.1. – 25.4.)

TAK ☐ NIE ☐

25.1. NAZWA MIEJSCA ZATRUDNIENIA WSPÓŁMAŁŻONKA

25.2. ADRES MIEJSCA ZATRUDNIENIA WSPÓŁMAŁŻONKA
(ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

25.3. STANOWISKO ZAJMOWANE PRZEZ WSPÓŁMAŁŻONKA

25.4. CZY PANI (PANA) WSPÓŁMAŁŻONEK POSIADA INNE MIEJSCE ZATRUDNIENIA, NIŻ WSKAZANE W PKT 25.1. – 25.3.?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK"
proszę wypełnić odpowiedni załącznik według schematu z pkt 25.1. – 25.4.)

TAK ☐ NIE ☐

B. PARTNER ŻYCIOWY (PARTNERKA ŻYCIOWA) OSOBY SPRAWDZANEJ
NALEŻY WPISAĆ DANE OSOBY, KTÓRA POZOSTAJE W FAKTYCZNYM – NIEBĘDĄCYM MAŁŻEŃSTWEM – ZWIĄZKU Z OSOBĄ SPRAWDZANĄ

1. CZY POSIADA PANI (PAN) PARTNERA ŻYCIOWEGO (PARTNERKĘ ŻYCIOWĄ), Z KTÓRYM (KTÓRĄ) NIE POZOSTAJE PANI (PAN) W ZWIĄZKU MAŁŻEŃSKIM?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 2. – 22.4.)

TAK ☐ NIE ☐

2. OD KIEDY? (ROK)

3. CZY PANI (PAN) PARTNER (PARTNERKA) POZOSTAJE W ZWIĄZKU MAŁŻEŃSKIM Z INNĄ OSOBĄ?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU)

TAK ☐ NIE ☐

4. NAZWISKO PARTNERA (PARTNERKI)

5. PIERWSZE IMIĘ PARTNERA (PARTNERKI)

6. DRUGIE IMIĘ PARTNERA (PARTNERKI)

7. NAZWISKO RODOWE PARTNERA (PARTNERKI)

8. INNE POPRZEDNIE NAZWISKA PARTNERA (PARTNERKI)

9. IMIĘ OJCA PARTNERA (PARTNERKI)

10. NAZWISKO OJCA PARTNERA (PARTNERKI)

11. NAZWISKO RODOWE OJCA PARTNERA (PARTNERKI)

12. IMIĘ MATKI PARTNERA (PARTNERKI)

13. NAZWISKO MATKI PARTNERA (PARTNERKI)

14. NAZWISKO RODOWE MATKI PARTNERA (PARTNERKI)

15. DATA URODZENIA (DD-MM-RRRR) PARTNERA (PARTNERKI)
– –

16. MIEJSCE URODZENIA PARTNERA (PARTNERKI)
(MIEJSCOWOŚĆ, PAŃSTWO)

17. OBYWATELSTWA POSIADANE PRZEZ PARTNERA (PARNERKĘ) (OD KIEDY?)

18. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ PARTNERA (PARTNERKĘ) (OD KIEDY – DO KIEDY?)

19. NR PESEL PARTNERA (PARTNERKI)

20. NIP PARTNERA (PARTNERKI)

21.1. NR DOWODU OSOBISTEGO PARTNERA (PARTNERKI)

21.2. DATA WAŻNOŚCI DOWODU OSOBISTEGO PARTNERA (PARTNERKI)

21.3. NAZWA ORGANU, KTÓRY WYDAŁ DOWÓD OSOBISTY PARTNERA (PARTNERKI)

22.1. NR PASZPORTU PARTNERA (PARTNERKI)

22.2. DATA WAŻNOŚCI PASZPORTU PARTNERA (PARTNERKI)

22.3. NAZWA ORGANU, KTÓRY WYDAŁ PASZPORT PARTNERA (PARTNERKI)

22.4. CZY PANI (PANA) PARTNER (PARTNERKA) POSIADA INNY PASZPORT, NIŻ WSKAZANY W PKT 22.1. – 22.3.?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK"
proszę wypełnić odpowiedni załącznik według schematu z pkt 22.1 – 22.4.)

TAK ☐ NIE ☐

23. ADRES ZAMELDOWANIA PARTNERA (PARTNERKI) (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

24. ADRES ZAMIESZKANIA PARTNERA (PARTNERKI) (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

25.1. NAZWA MIEJSCA ZATRUDNIENIA PARTNERA (PARTNERKI)

25.2. ADRES MIEJSCA ZATRUDNIENIA PARTNERA (PARTNERKI) (ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

25.3. STANOWISKO ZAJMOWANE PRZEZ PARTNERA (PARTNERKĘ)

25.4. CZY PANI (PANA) PARTNER (PARTNERKA) POSIADA INNE MIEJSCE ZATRUDNIENIA, NIŻ WSKAZANE W PKT 25.1. – 25.3.?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK”
proszę wypełnić odpowiedni załącznik według schematu z pkt 25.1 – 25.4.)

TAK ☐ NIE ☐

C. OJCIEC OSOBY SPRAWDZANEJ

1. NAZWISKO OJCA

2. PIERWSZE IMIĘ OJCA

3. DRUGIE IMIĘ OJCA

4. NAZWISKO RODOWE OJCA

5. DATA URODZENIA (DD-MM-RRRR) OJCA
– –

6. MIEJSCE URODZENIA OJCA (MIEJSCOWOŚĆ, PAŃSTWO)

7. OBYWATELSTWA POSIADANE PRZEZ OJCA (OD KIEDY?)

8. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ OJCA (OD KIEDY – DO KIEDY?)

9. NR PESEL OJCA

10. ADRES ZAMIESZKANIA OJCA (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

11. NAZWA MIEJSCA ZATRUDNIENIA OJCA

12. ADRES MIEJSCA ZATRUDNIENIA OJCA (ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

13. STANOWISKO ZAJMOWANE PRZEZ OJCA

D. MATKA OSOBY SPRAWDZANEJ

1. NAZWISKO MATKI

2. PIERWSZE IMIĘ MATKI

3. DRUGIE IMIĘ MATKI

4. NAZWISKO RODOWE MATKI

5. DATA URODZENIA (DD-MM-RRRR) MATKI
– –

6. MIEJSCE URODZENIA MATKI (MIEJSCOWOŚĆ, PAŃSTWO)

7. OBYWATELSTWA POSIADANE PRZEZ MATKĘ (OD KIEDY?)

8. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ MATKĘ (OD KIEDY – DO KIEDY?)

9. NR PESEL MATKI

10. ADRES ZAMIESZKANIA MATKI (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

11. NAZWA MIEJSCA ZATRUDNIENIA MATKI

12. ADRES MIEJSCA ZATRUDNIENIA MATKI (ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

13. STANOWISKO ZAJMOWANE PRZEZ MATKĘ

E. RODZEŃSTWO OSOBY SPRAWDZANEJ

E. 1.

1. CZY POSIADA PANI (PAN) RODZEŃSTWO MAJĄCE UKOŃCZONE 15 LAT?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 2. – 15.)

TAK ☐ NIE ☐

2. NAZWISKO SIOSTRY (BRATA)* (*niewłaściwe skreślić)

3. PIERWSZE IMIĘ SIOSTRY (BRATA)*

4. DRUGIE IMIĘ SIOSTRY (BRATA)*

5. NAZWISKO RODOWE SIOSTRY (BRATA)*

6. DATA URODZENIA (DD-MM-RRRR) SIOSTRY (BRATA)*
– –

7. MIEJSCE URODZENIA SIOSTRY (BRATA)*
(MIEJSCOWOŚĆ, PAŃSTWO)

8. OBYWATELSTWA POSIADANE PRZEZ SIOSTRĘ (BRATA)* (OD KIEDY?)

9. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ SIOSTRĘ (BRATA)* (OD KIEDY – DO KIEDY?)

10. NR PESEL SIOSTRY (BRATA)*

11. ADRES ZAMIESZKANIA SIOSTRY (BRATA)*
(ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

12. NAZWA MIEJSCA ZATRUDNIENIA SIOSTRY (BRATA)*

13. ADRES MIEJSCA ZATRUDNIENIA SIOSTRY (BRATA)*
(ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

14. STANOWISKO ZAJMOWANE PRZEZ SIOSTRĘ (BRATA)*

15. CZY POSIADA PANI/PAN INNE RODZEŃSTWO MAJĄCE UKOŃCZONE 15 LAT?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt E. 2.)

TAK ☐ NIE ☐

E. RODZEŃSTWO OSOBY SPRAWDZANEJ

E. 2.

1. NAZWISKO SIOSTRY (BRATA)* (*niewłaściwe skreślić)	2. PIERWSZE IMIĘ SIOSTRY (BRATA)*
3. DRUGIE IMIĘ SIOSTRY (BRATA)*	4. NAZWISKO RODOWE SIOSTRY (BRATA)*
5. DATA URODZENIA (DD-MM-RRRR) SIOSTRY (BRATA)* – –	6. MIEJSCE URODZENIA SIOSTRY (BRATA)* (MIEJSCOWOŚĆ, PAŃSTWO)
7. OBYWATELSTWA POSIADANE PRZEZ SIOSTRĘ (BRATA)* (OD KIEDY?)	
8. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ SIOSTRĘ (BRATA)* (OD KIEDY – DO KIEDY?)	
9. NR PESEL SIOSTRY (BRATA)*	
10. ADRES ZAMIESZKANIA SIOSTRY (BRATA)* (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)	
11. NAZWA MIEJSCA ZATRUDNIENIA SIOSTRY (BRATA)*	
12. ADRES MIEJSCA ZATRUDNIENIA SIOSTRY (BRATA)* (ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)	
13. STANOWISKO ZAJMOWANE PRZEZ SIOSTRĘ (BRATA)*	
14. CZY POSIADA PANI (PAN) INNE RODZEŃSTWO MAJĄCE UKOŃCZONE 15 LAT? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt E. 2.) TAK ☐ NIE ☐	

F. DZIECI OSOBY SPRAWDZANEJ

F. 1.

1. CZY POSIADA PANI (PAN) DZIECI MAJĄCE UKOŃCZONE 15 LAT? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 2. – 15.) TAK ☐ NIE ☐	
2. NAZWISKO CÓRKI (SYNA)* (*niewłaściwe skreślić)	3. PIERWSZE IMIĘ CÓRKI (SYNA)*
4. DRUGIE IMIĘ CÓRKI (SYNA)*	5. NAZWISKO RODOWE CÓRKI (SYNA)*
6. DATA URODZENIA (DD-MM-RRRR) CÓRKI (SYNA)* – –	7. MIEJSCE URODZENIA CÓRKI (SYNA)* (MIEJSCOWOŚĆ, PAŃSTWO)
8. OBYWATELSTWA POSIADANE PRZEZ CÓRKĘ (SYNA) * (OD KIEDY?)	
9. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ CÓRKĘ (SYNA) * (OD KIEDY – DO KIEDY?)	
10. NR PESEL CÓRKI (SYNA)*	

11. ADRES ZAMIESZKANIA CÓRKI (SYNA)*
(ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

12. NAZWA MIEJSCA ZATRUDNIENIA CÓRKI (SYNA)*

13. ADRES MIEJSCA ZATRUDNIENIA CÓRKI (SYNA)*
(ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

14. STANOWISKO ZAJMOWANE PRZEZ CÓRKĘ (SYNA) *

15. CZY POSIADA PANI/PAN INNE DZIECI MAJĄCE UKOŃCZONE 15 LAT?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt F. 2.)

TAK ☐ NIE ☐

F. DZIECI OSOBY SPRAWDZANEJ

F. 2.

1. NAZWISKO CÓRKI (SYNA)* (*niewłaściwe skreślić)

2. PIERWSZE IMIĘ CÓRKI (SYNA) *

3. DRUGIE IMIĘ CÓRKI (SYNA)*

4. NAZWISKO RODOWE CÓRKI (SYNA)*

5. DATA URODZENIA (DD-MM-RRRR) CÓRKI (SYNA)*
– –

6. MIEJSCE URODZENIA CÓRKI (SYNA)*
(MIEJSCOWOŚĆ, PAŃSTWO)

7. OBYWATELSTWA POSIADANE PRZEZ CÓRKĘ (SYNA) * (OD KIEDY?)

8. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ CÓRKĘ (SYNA)* (OD KIEDY – DO KIEDY?)

9. NR PESEL CÓRKI (SYNA)*

10. ADRES ZAMIESZKANIA CÓRKI (SYNA)*
(ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

11. NAZWA MIEJSCA ZATRUDNIENIA CÓRKI (SYNA)*

12. ADRES MIEJSCA ZATRUDNIENIA CÓRKI (SYNA)*
(ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

13. STANOWISKO ZAJMOWANE PRZEZ CÓRKĘ (SYNA)*

14. CZY POSIADA PANI/PAN INNE DZIECI MAJĄCE UKOŃCZONE 15 LAT?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt F. 2.)

TAK ☐ NIE ☐

G. WSPÓŁMIESZKAŃCY OSOBY SPRAWDZANEJ

G. 1.

1. CZY ZAMIESZKUJE PAN Z OSOBAMI MAJĄCYMI UKOŃCZONE 15 LAT, INNYMI NIŻ WSKAZANE W PKT A. – F. TEJ CZĘŚCI ANKIETY?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 2. – 20.)

TAK ☐ NIE ☐

2. OKREŚLENIE POKREWIEŃSTWA LUB POWINOWACTWA WSPÓŁMIESZKAŃCA Z OSOBĄ SPRAWDZANĄ

3. NAZWISKO WSPÓŁMIESZKAŃCA

4. PIERWSZE IMIĘ WSPÓŁMIESZKAŃCA

5. DRUGIE IMIĘ WSPÓŁMIESZKAŃCA

6. NAZWISKO RODOWE WSPÓŁMIESZKAŃCA

7. IMIĘ OJCA WSPÓŁMIESZKAŃCA

8. NAZWISKO OJCA WSPÓŁMIESZKAŃCA

9. NAZWISKO RODOWE OJCA WSPÓŁMIESZKAŃCA

10. IMIĘ MATKI WSPÓŁMIESZKAŃCA

11. NAZWISKO MATKI WSPÓŁMIESZKAŃCA

12. NAZWISKO RODOWE MATKI WSPÓŁMIESZKAŃCA

13. DATA URODZENIA (DD-MM-RRRR) WSPÓŁMIESZKAŃCA

– –

14. MIEJSCE URODZENIA WSPÓŁMIESZKAŃCA
(MIEJSCOWOŚĆ, PAŃSTWO)

15. OBYWATELSTWA POSIADANE PRZEZ WSPÓŁMIESZKAŃCA (OD KIEDY?)

16. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ WSPÓŁMIESZKAŃCA (OD KIEDY – DO KIEDY?)

17. NR PESEL WSPÓŁMIESZKAŃCA

18. NAZWA MIEJSCA ZATRUDNIENIA WSPÓŁMIESZKAŃCA

19. ADRES MIEJSCA ZATRUDNIENIA WSPÓŁMIESZKAŃCA
(ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

20. STANOWISKO ZAJMOWANE PRZEZ WSPÓŁMIESZKAŃCA

21. CZY ZAMIESZKUJE PAN Z OSOBAMI MAJĄCYMI UKOŃCZONE 15 LAT, INNYMI NIŻ WSKAZANE W PKT A. – G.1. TEJ CZĘŚCI ANKIETY?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt G.2.)

TAK ☐ NIE ☐

G. WSPÓŁMIESZKAŃCY OSOBY SPRAWDZANEJ

G.2.

1. OKREŚLENIE POKREWIEŃSTWA WSPÓŁMIESZKAŃCA Z OSOBĄ SPRAWDZANĄ

2. NAZWISKO WSPÓŁMIESZKAŃCA

3. PIERWSZE IMIĘ WSPÓŁMIESZKAŃCA

4. DRUGIE IMIĘ WSPÓŁMIESZKAŃCA

5. NAZWISKO RODOWE WSPÓŁMIESZKAŃCA

6. IMIĘ OJCA WSPÓŁMIESZKAŃCA

7. NAZWISKO OJCA WSPÓŁMIESZKAŃCA

8. NAZWISKO RODOWE OJCA WSPÓŁMIESZKAŃCA

9. IMIĘ MATKI WSPÓŁMIESZKAŃCA

10. NAZWISKO MATKI WSPÓŁMIESZKAŃCA

11. NAZWISKO RODOWE MATKI WSPÓŁMIESZKAŃCA

12. DATA URODZENIA (DD-MM-RRRR) WSPÓŁMIESZKAŃCA

_ _

13. MIEJSCE URODZENIA WSPÓŁMIESZKAŃCA
(MIEJSCOWOŚĆ, PAŃSTWO)

14. OBYWATELSTWA POSIADANE PRZEZ WSPÓŁMIESZKAŃCA (OD KIEDY?)

15. OBYWATELSTWA POSIADANE WCZEŚNIEJ PRZEZ WSPÓŁMIESZKAŃCA (OD KIEDY – DO KIEDY?)

16. NR PESEL WSPÓŁMIESZKAŃCA

17. NAZWA MIEJSCA ZATRUDNIENIA WSPÓŁMIESZKAŃCA

18. ADRES MIEJSCA ZATRUDNIENIA WSPÓŁMIESZKAŃCA
(ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

19. STANOWISKO ZAJMOWANE PRZEZ WSPÓŁMIESZKAŃCA

20. CZY ZAMIESZKUJE PANI (PAN) Z OSOBAMI MAJĄCYMI UKOŃCZONE 15 LAT, INNYMI NIŻ WSKAZANE W PKT A. – G.2. TEJ CZĘŚCI ANKIETY?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt G.2.)

TAK ☐ NIE ☐

CZĘŚĆ III: DANE DOTYCZĄCE HISTORII ŻYCIA ZAWODOWEGO I OSOBISTEGO

1. CZY JEST PANI ZATRUDNIONA (PAN ZATRUDNIONY) ALBO PROWADZI PANI (PAN) DZIAŁALNOŚĆ GOSPODARCZĄ?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „tak" proszę wypełnić tabelę)

TAK ☐ NIE ☐

od kiedy	nazwa miejsca zatrudnienia (firmy)	zajmowane stanowiska

2. CZY POSIADAŁA PANI (POSIADAŁ PAN) LUB POSIADA PANI (PAN) DOSTĘP DO INFORMACJI NIEJAWNYCH?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „tak" proszę wypełnić tabelę)

TAK ☐ NIE ☐

daty dostępu do informacji niejawnych (od – do)	nazwa miejsca zatrudnienia (jednostki i komórki organizacyjnej), w której posiadała Pani (posiadał Pan) lub posiada Pani (Pan) dostęp do informacji niejawnych	nazwa i nr dokumentu upoważniającego do dostępu do informacji niejawnych, nazwa organu, który wydał ten dokument, data wydania dokumentu	klauzula tajności, do jakiej miała Pani (miał Pan) w przeszłości lub ma Pani (Pan) obecnie dostęp

3.1. WYKSZTAŁCENIE	3.2. TYTUŁ NAUKOWY (TYTUŁY NAUKOWE)

3.3. PROSZĘ PODAĆ NAZWY SZKÓŁ I KURSÓW ZAGRANICZNYCH, KTÓRE UKOŃCZYŁA PANI (UKOŃCZYŁ PAN) BĘDĄC OSOBĄ DOROSŁĄ (LUB GDY OSTATNIĄ SZKOŁĘ UKOŃCZYŁA PANI (UKOŃCZYŁ PAN) PRZED UPŁYWEM 18 ROKU ŻYCIA – PROSZĘ PODAĆ NAZWĘ OSTATNIEJ UKOŃCZONEJ PRZEZ PANIĄ (PANA) SZKOŁY) ORAZ NAZWY SZKÓŁ I KURSÓW ZAGRANICZNYCH, GDZIE UCZY SIĘ PANI (PAN) OBECNIE

daty nauki (od – do)	nazwa i adres szkoły	uzyskane dokumenty

4. CZY BYŁA PANI (BYŁ PAN) W PRZESZŁOŚCI – BĘDĄC OSOBĄ DOROSŁĄ – LUB JEST PANI (PAN) OBECNIE CZŁONKIEM PARTII POLITYCZNYCH, STOWARZYSZEŃ, INNYCH ORGANIZACJI SPOŁECZNYCH ALBO WŁADZ FUNDACJI?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „tak" proszę wypełnić tabelę)

TAK ☐ NIE ☐

daty członkostwa (od – do)	nazwa i adres organizacji	pełniona funkcja

5. PROSZĘ PODAĆ ADRESY, POD KTÓRYMI ZAMIESZKIWAŁA PANI (ZAMIESZKIWAŁ PAN) PO UKOŃCZENIU 18 ROKU ŻYCIA PRZEZ OKRES DŁUŻSZY NIŻ 30 DNI

daty zamieszkania (od – do)	adres

CZĘŚĆ IV: DANE DOTYCZĄCE BEZPIECZEŃSTWA

1. CZY W LATACH 1944 – 1990 BYŁA PANI (BYŁ PAN) PRACOWNIKIEM LUB TAJNYM WSPÓŁPRACOWNIKIEM ORGANÓW BEZPIECZEŃSTWA PAŃSTWA W ROZUMIENIU 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 DNIA 30 LISTOPADA 2006 R. NR 218, POZ. 1592, Z PÓŹN. ZM.)?
(**UDZIELENIE ODPOWIEDZI NA TO PYTANIE – PRZEZ ANALOGIĘ DO ART. 9 CYT. USTAWY – JEST Z MOCY PRAWA ZWOLNIONE Z ZACIĄGNIĘTYCH WCZEŚNIEJ ZOBOWIĄZAŃ DO ZACHOWANIA TAJEMNICY)**
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU)

TAK ☐ NIE ☐

2. CZY BYŁA PANI KARANA (BYŁ PAN KARANY) ZA POPEŁNIENIE PRZESTĘPSTWA, W TYM PRZESTĘPSTWA SKARBOWEGO (Z WYJĄTKIEM PRZYPADKÓW, KTÓRE ULEGŁY ZATARCIU)?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 2.1. – 2.4.)

TAK ☐ NIE ☐

2.1. NAZWA ORGANU, KTÓRY WYDAŁ ORZECZENIE

2.2. DATA ORZECZENIA (DD-MM-RRRR)

– –

2.3. OKREŚLENIE PRZESTEPSTWA, ZA POPEŁNIENIE KTÓREGO BAŁA PANI KARANA (BYŁ PAN KARANY)

2.4. CZY BYŁA PANI KARANA (BYŁ PAN KARANY) ZA POPEŁNIENIE INNEGO, NIŻ PRZYPADEK WSKAZANY W PKT 2. - 2.3. PRZESTĘPSTWA, W TYM PRZESTĘPSTWA SKARBOWEGO (Z WYJĄTKIEM PRZYPADKÓW, KTÓRE ULEGŁY ZATARCIU)?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 2.1 - 2.4.)

TAK ☐ NIE ☐

3. CZY AKTUALNIE TOCZĄ SIĘ WOBEC PANI (PANA) POSTĘPOWANIA O UKARANIE ZA POPEŁNIENIE PRZESTĘPSTWA LUB PRZESTĘPSTWA SKARBOWEGO?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 3.1. – 3.4.)

TAK ☐ NIE ☐

3.1. NAZWA ORGANU, KTÓRY PROWADZI SPRAWĘ

3.2. NR SPRAWY

3.3. OKREŚLENIE, W ZWIĄZKU Z PODEJRZENIEM POPEŁNIENIA JAKIEGO PRZESTEPSTWA TOCZY SIĘ WOBEC PANI (PANA) POSTĘPOWANIE

3.4. CZY AKTUALNIE TOCZĄ SIĘ WOBEC PANI (PANA) INNE, NIŻ WSKAZANE W PKT 3. – 3.3. POSTĘPOWANIA O UKARANIE ZA POPEŁNIENIE PRZESTĘPSTWA LUB PRZESTĘPSTWA SKARBOWEGO?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 3.1 – 3.4.)

TAK ☐ NIE ☐

3.5. CZY AKTUALNIE TOCZĄ SIĘ WOBEC PANI (PANA) POSTĘPOWANIA DYSCYPLINARNE W ZWIĄZKU Z NARUSZENIEM PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU)

TAK ☐ NIE ☐

4. CZY KIEDYKOLWIEK STWIERDZIŁA PANI (STWIERDZIŁ PAN) FAKT ZAINTERESOWANIA SWOJĄ OSOBĄ ZE STRONY ZAGRANICZNYCH SŁUŻB SPECJALNYCH LUB INNYCH OBCYCH INSTYTUCJI APARATU ŚCIGANIA (POLICJA, STRAŻ GRANICZNA) BĄDŹ GRUP ZORGANIZOWANEJ PRZESTĘPCZOŚCI (POLSKICH LUB ZAGRANICZNYCH)? CZY WIADOMO PANI (PANU) COŚ O ANALOGICZNYCH ZAINTERESOWANIACH SWOIM WSPÓŁMAŁŻONKIEM, INNYMI OSOBAMI POZOSTAJĄCYMI WE WSPÓLNYM GOSPODARSTWIE DOMOWYM BĄDŹ INNYMI CZŁONKAMI RODZINY? JEŚLI TAK, PROSZĘ ZAKREŚLIĆ WŁAŚCIWE POLE. PROSZĘ NIE PODAWAĆ ŻADNYCH SZCZEGÓŁÓW. ZOSTANĄ ONE Z PANIĄ (PANEM) OMÓWIONE PRZEZ PRZEDSTAWICIELA SŁUŻBY OCHRONY PAŃSTWA, PROWADZĄCEGO POSTĘPOWANIE SPRAWDZAJĄCE.
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU)

TAK ☐ NIE ☐

5. CZY KIEDYKOLWIEK PODCZAS POBYTU ZA GRANICĄ BYŁA PANI WYPYTYWANA (BYŁ PAN WYPYTYWANY) LUB W INNY SPOSÓB INDAGOWANA (INDAGOWANY) PRZEZ OBCE WŁADZE (IMIGRACYJNE, SKARBOWE, INNE) NA TEMATY ZWIĄZANE Z ZAGADNIENIAMI BEZPIECZEŃSTWA LUB OBRONNOŚCI PAŃSTWA? CZY WIADOMO PANI (PANU) COŚ O ANALOGICZNYCH ZAINTERESOWANIACH WOBEC SWOJEGO WSPÓŁMAŁŻONKA LUB INNYCH OSÓB POZOSTAJĄCYCH WE WSPÓLNYM GOSPODARSTWIE DOMOWYM BĄDŹ INNYCH CZŁONKÓW RODZINY? JEŚLI TAK, PROSZĘ ZAKREŚLIĆ WŁAŚCIWE POLE. PROSZĘ NIE PODAWAĆ ŻADNYCH DALSZYCH SZCZEGÓŁÓW. ZOSTANĄ ONE Z PANIĄ (PANEM) OMÓWIONE PRZEZ PRZEDSTAWICIELA SŁUŻBY OCHRONY PAŃSTWA, PROWADZĄCEGO POSTĘPOWANIE SPRAWDZAJĄCE.
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU)

TAK ☐ NIE ☐

6. CZY PANI (PAN) LUB PANI (PANA) WSPÓŁMAŁŻONEK ALBO PARTNER (PARTNERKA) PRZEBYWALIŚCIE ZA GRANICĄ DŁUŻEJ NIŻ 30 DNI PO UKOŃCZENIU 18 LAT?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „tak" proszę wypełnić tabelę)

TAK ☐ NIE ☐

imię i nazwisko	daty pobytu (od – do)	miejsce (kraj, miejscowość) i adres pobytu	powód pobytu

7. CZY PANI (PAN) LUB PANI (PANA) WSPÓŁMAŁŻONEK ALBO PARTNER (PARTNERKA) UTRZYMUJECIE LUB UTRZYMYWALIŚCIE W OKRESIE OSTATNICH 20 LAT KONTAKTY PRYWATNE LUB SŁUŻBOWE Z OBYWATELAMI INNYCH PAŃSTW?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „tak" – proszę wypełnić tabelę)

TAK ☐ NIE ☐

imię i nazwisko	imię i nazwisko obywatela innego państwa, z którym utrzymywano kontakt	kraj pochodzenia obywatela innego państwa, z którym utrzymywano kontakt	daty utrzymywania kontaktu (od – do)	powód i charakter kontaktu

CZĘŚĆ V: DANE DOTYCZĄCE STANU ZDROWIA

1. CZY KIEDYKOLWIEK BYŁA PANI PODDANA (BYŁ PAN PODDANY) BADANIU, PO KTÓRYM OKREŚLONO PANI (PANU) KATEGORIĘ ZDROWIA (NP. W WOJSKU, W MSWiA, ABW, AW, CBA, SKW, SWW)
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 1.1. – 1.2.)

TAK ☐ NIE ☐

1.1. CZY W WYNIKU BADANIA WSKAZANEGO W PKT 1 UZNANO PANIĄ ZA ZDOLNĄ (PANA ZA ZDOLNEGO) DO SŁUŻBY?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU)

TAK ☐ NIE ☐

1.2. KATEGORIA ZDROWIA PRZYZNANA PANI (PANU) W BADANIU WSKAZANYM W PKT 1. - 1.1.

2. CZY CIERPI PANI (PAN) LUB CIERPIAŁA PANI (CIERPIAŁ PAN) W PRZESZŁOŚCI NA CHOROBY PSYCHICZNE?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 2.1. – 2.6.)

TAK ☐ NIE ☐

2.1. NAZWA CHOROBY	2.2. W JAKIM OKRESIE? (OD – DO)

2.3. CZY W ZWIĄZKU Z CHOROBĄ WSKAZANĄ W PKT 2. - 2.2. LECZY SIĘ PANI (PAN) ALBO LECZYŁA SIĘ PANI (LECZYŁ SIĘ PAN) LUB BYŁA PANI KIEROWANA (BYŁ PAN KIEROWANY) NA LECZENIE?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 2.4. – 2.6.)

TAK ☐ NIE ☐

2.4. NAZWA PLACÓWKI, GDZIE LECZONO PANIĄ (PANA) W ZWIĄZKU CHOROBĄ WSKAZANĄ W PKT 2. – 2.2.
(LUB DANE LEKARZA, KTÓRY OPIEKOWAŁ SIĘ PANIĄ (PANEM) W ZWIĄZKU Z CHOROBĄ WSKAZANĄ W PKT 2. – 2.2.)

2.5. W JAKIM OKRESIE (OD – DO) BYŁA PANI LECZONA (BYŁ PAN) LECZONY W PLACÓWCE WSKAZANEJ W PKT 2.4.
(LUB POD OPIEKĄ LEKARZA WSKAZANEGO W PKT 2.4.)?

2.6. CZY CIERPI PANI (PAN) LUB CIERPIAŁA PANI (CIERPIAŁ PAN) W PRZESZŁOŚCI NA CHOROBY PSYCHICZNE INNE, NIŻ WSKAZANE W PKT 2. – 2.5.? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 2.1. – 2.6.)

TAK ☐ NIE ☐

3. CZY CIERPI PANI (PAN) LUB CIERPIAŁA PANI (CIERPIAŁ PAN) W PRZESZŁOŚCI NA INNE NIŻ CHOROBY PSYCHICZNE DOLEGLIWOŚCI LUB CHOROBY, POWODUJĄCE ISTOTNE ZAKŁÓCENIA CZYNNOŚCI PSYCHICZNYCH?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 3.1. – 3.6.)

TAK ☐ NIE ☐

3.1. NAZWA DOLEGLIWOŚCI (CHOROBY)	3.2. W JAKIM OKRESIE? (OD – DO)

3.3. CZY W ZWIĄZKU Z DOLEGLIWOŚCIĄ (CHOROBĄ) WSKAZANĄ W PKT 3. – 3.2. LECZY SIĘ PANI (PAN) ALBO LECZYŁA SIĘ PANI (LECZYŁ SIĘ PAN) LUB BYŁA PANI KIEROWANA (BYŁ PAN KIEROWANY) NA LECZENIE LUB TERAPIĘ?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 3.4. – 3.6.)

TAK ☐ NIE ☐

3.4. NAZWA PLACÓWKI, GDZIE LECZONO PANIĄ (PANA) W ZWIĄZKU DOLEGLIWOŚCIĄ (CHOROBĄ) WSKAZANĄ W PKT 3. – 3.2.
(LUB DANE LEKARZA, KTÓRY OPIEKOWAŁ SIĘ PANIĄ (PANEM) W ZWIĄZKU Z CHOROBĄ WSKAZANĄ W PKT 3. – 3.2.)

3.5. W JAKIM OKRESIE (OD – DO) BYŁA PANI LECZONA (BYŁ PAN LECZONY) W PLACÓWCE WSKAZANEJ W PKT 3.4.?
(LUB POD OPIEKĄ LEKARZA WSKAZANEGO W PKT 3.4.)

3.6. CZY CIERPI PANI (PAN) LUB CIERPIAŁA PANI (CIERPIAŁ PAN) W PRZESZŁOŚCI NA INNE NIŻ CHOROBY PSYCHICZNE DOLEGLIWOŚCI LUB CHOROBY, POWODUJĄCE ISTOTNE ZAKŁÓCENIA CZYNNOŚCI PSYCHICZNYCH, NIEWSKAZANE WCZEŚNIEJ W PKT 3. – 3.5.? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 3.1. – 3.6.)

TAK ☐ NIE ☐

4. CZY ZAŻYWA LUB ZAŻYWAŁA PANI (ZAŻYWAŁ PAN) W PRZESZŁOŚCI NARKOTYKI LUB INNE ŚRODKI O PODOBNYM DZIAŁANIU? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 4.1. – 4.7.)

TAK ☐ NIE ☐

4.1. NAZWA NARKOTYKU LUB ŚRODKA	4.2. ILE RAZY I W JAKIEJ DAWCE?	4.3. W JAKIM OKRESIE? (OD – DO)

4.4. CZY W ZWIĄZKU Z ZAŻYWANIEM NARKOTYKÓW LUB INNYCH ŚRODKÓW O PODOBNYM DZIAŁANIU LECZY SIĘ PANI (PAN) ALBO LECZYŁA SIĘ PANI (LECZYŁ SIĘ PAN) LUB BYŁA PANI KIEROWANA (BYŁ PAN KIEROWANY) NA LECZENIE LUB TERAPIĘ? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 4.5. – 4.7.)

TAK ☐ NIE ☐

4.5. NAZWA PLACÓWKI, GDZIE LECZONO PANIĄ (PANA) W ZWIĄZKU Z ZAŻYWANIEM NARKOTYKÓW (LUB DANE LEKARZA, KTÓRY OPIEKOWAŁ SIĘ PANIĄ (PANEM) W ZWIĄZKU Z ZAŻYWANIEM NARKOTYKÓW)

4.6. W JAKIM OKRESIE (OD – DO) BYŁA PANI LECZONA (BYŁ PAN LECZONY) W PLACÓWCE WSKAZANEJ W PKT 4.5.? (LUB POD OPIEKĄ LEKARZA WSKAZANEGO W PKT 4.5.)

4.7. CZY ZAŻYWA LUB ZAŻYWAŁA PANI (ZAŻYWAŁ PAN) W PRZESZŁOŚCI NARKOTYKI LUB INNE ŚRODKI O PODOBNYM DZIAŁANIU, NIEWSKAZANE WCZEŚNIEJ W PKT 4. – 4.6.? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 4.1. – 4.7.)

TAK ☐ NIE ☐

5. CZY SPOŻYWA ALBO SPOŻYWAŁA PANI (SPOŻYWAŁ PAN) PO UKOŃCZENIU 18 LAT ALKOHOL W ILOŚCIACH POWODUJĄCYCH UTRATĘ ŚWIADOMOŚCI? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 5.1. - 5.3.)

TAK ☐ NIE ☐

5.1. JAK CZĘSTO?	5.2. W JAKICH OKOLICZNOŚCIACH?

6. CZY W ZWIĄZKU ZE SPOŻYWANIEM ALKOHOLU LECZY SIĘ PANI (PAN) ALBO LECZYŁA SIĘ PANI (LECZYŁ SIĘ PAN) LUB BYŁA PANI KIEROWANA (BYŁ PAN KIEROWANY) NA LECZENIE LUB TERAPIĘ? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 6.1. – 6.3.)

TAK ☐ NIE ☐

6.1. W JAKIM OKRESIE? (OD – DO)

6.2. NAZWA PLACÓWKI, GDZIE LECZONO PANIĄ (PANA) W ZWIĄZKU ZE SPOŻYWANIEM ALKOHOLU (LUB DANE LEKARZA, KTÓRY OPIEKOWAŁ SIĘ PANIĄ (PANEM) W ZWIĄZKU ZE SPOŻYWANIEM ALKOHOLU)

6.3. CZY W ZWIĄZKU ZE SPOŻYWANIEM ALKOHOLU, POZA PRZYPADKAMI WSKAZANYMI W PKT 6. – 6.2., LECZY SIĘ PANI (PAN), ALBO LECZYŁA SIĘ PANI (LECZYŁ SIĘ PAN) LUB BYŁA PANI KIEROWANA (BYŁ PAN KIEROWANY) NA LECZENIE LUB TERAPIĘ? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 6.1. – 6.3.)

TAK ☐ NIE ☐

7. CZY PO UKOŃCZENIU 18 LAT SPOŻYWANIE ALKOHOLU BYŁO KIEDYKOLWIEK PRZYCZYNĄ PROBLEMÓW W PANI (PANA) PRACY LUB W ŻYCIU PRYWATNYM? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 7.1. – 7.2.)

TAK ☐ NIE ☐

7.1. PROSZĘ WSKAZAĆ, JAKIE PROBLEMY	7.2. KIEDY?

CZĘŚĆ VI: DANE DOTYCZĄCE SYTUACJI MAJĄTKOWO-FINANSOWEJ

1. WYSOKOŚĆ WYPŁACANEGO PANI (PANU) MIESIĘCZNEGO WYNAGRODZENIA W MIEJSCU PRACY WSKAZANYM W CZ. I PKT 18.1. – 18.3.

1a. WYSOKOŚĆ WYPŁACANEGO PANI (PANU) MIESIĘCZNEGO WYNAGRODZENIA W MIEJSCU PRACY WSKAZANYM W CZ. I PKT 18.4.

2. CZY POZA DOCHODAMI WSKAZANYMI W PKT 1 UZYSKUJE PANI (PAN) INNE DOCHODY LUB ZYSKI (*np. dochody otrzymywane bez świadczenia pracy, emerytury, renty, zasiłki, renty zagraniczne, dywidendy od posiadanych papierów wartościowych, odsetki od lokat bankowych – jeżeli miesięczny zysk przekracza 100 złotych (PLN), zyski z obrotu akcjami na giełdzie, zyski z udziałów w funduszach powierniczych, dochody z wynajmu nieruchomości, wygrane w grach losowych – o wysokości ponad 20.000 złotych (PLN), honoraria za publikacje lub z działalności dydaktycznej, dochody z realizacji umów zleconych, i inne*)
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 2.1. – 2.3.)

TAK ☐ NIE ☐

2.1. RODZAJ DOCHODU LUB ZYSKU

2.2. WYSOKOŚĆ WYPŁACANYCH PANI/PANU DOCHODÓW LUB ZYSKÓW

2.3. CZY POZA DOCHODAMI WSKAZANYMI W PKT 1. – 2.2. UZYSKUJE PANI (PAN) INNE DOCHODY LUB ZYSKI?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 2.1. – 2.3.)

TAK ☐ NIE ☐

3. WYSOKOŚĆ ROCZNYCH WYPŁACONYCH PANI (PANU) WYNAGRODZEŃ, INNYCH DOCHODÓW LUB ZYSKÓW ZA ROK POPRZEDZAJĄCY WYPEŁNIENIE NINIEJSZEJ ANKIETY

4. CZY Z RACJI ZAJMOWANEGO OBECNIE LUB W PRZESZŁOŚCI STANOWISKA BYŁA PANI (BYŁ PAN) ZOBOWIĄZANY SKŁADAĆ OŚWIADCZENIA O STANIE MAJĄTKOWYM?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 4.1. – 4.2.)

TAK ☐ NIE ☐

4.1. W JAKIM OKRESIE? (OD – DO)

4.2. KOMU? (PROSZĘ WSKAZAĆ WŁAŚCIWY ORGAN)

5. CZY SWOJE GOSPODARSTWO DOMOWE PROWADZI PANI SAMA (PAN SAM)?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „NIE" proszę wypełnić pkt 5.1. – 5.6.)

TAK ☐ NIE ☐

5.1. IMIĘ OSOBY PROWADZĄCEJ Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE

5.2. NAZWISKO OSOBY PROWADZĄCEJ Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE

5.3. NR PESEL OSOBY PROWADZĄCEJ Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE

5.4. NIP OSOBY PROWADZĄCEJ Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE

5.5. WYSOKOŚĆ ROCZNYCH WYPŁACONYCH OSOBIE WSKAZANEJ W PKT 5.1. – 5.4. WYNAGRODZEŃ, INNYCH DOCHODÓW LUB ZYSKÓW ZA ROK POPRZEDZAJĄCY WYPEŁNIENIE NINIEJSZEJ ANKIETY

5.6. PROSZĘ PODAĆ LICZBĘ OSÓB POZOSTAJĄCYCH NA PANI (PANA) UTRZYMANIU

6. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE NIERUCHOMOŚCI?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 6.1. - 6.12.)

TAK ☐ NIE ☐

6.1. IMIĘ WŁAŚCICIELA/WSPÓŁWŁAŚCICIELA NIERUCHOMOŚCI

6.2. NAZWISKO WŁAŚCICIELA/WSPÓŁWŁAŚCICIELA NIERUCHOMOŚCI

6.3. NAZWA NIERUCHOMOŚCI	
6.4. ADRES NIERUCHOMOŚCI	
6.5. NAZWA DOKUMENTU POTWIERDZAJĄCEGO NABYCIE NIERUCHOMOŚCI	
6.6. % WŁASNOŚCI NIERUCHOMOŚCI	6.7. ŹRÓDŁO SFINANSOWANIA NABYCIA NIERUCHOMOŚCI
6.8. SPOSÓB NABYCIA NIERUCHOMOŚCI	6.9. DATA NABYCIA NIERUCHOMOŚCI
6.10. CENA NABYCIA NIERUCHOMOŚCI	
6.11. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE INNE (POZA WSKAZANYMI W PKT 6.1. – 6.10.) NIERUCHOMOŚCI? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 6.12. – 6.22.) TAK ☐ NIE ☐	
6.12. IMIĘ WŁAŚCICIELA (WSPÓŁWŁAŚCICIELA) NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.	6.13. NAZWISKO WŁAŚCICIELA (WSPÓŁWŁAŚCICIELA) NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.
6.14. NAZWA NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.	
6.15. ADRES NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.	
6.16. NAZWA DOKUMENTU POTWIERDZAJĄCEGO NABYCIE NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.	
6.17. % WŁASNOŚCI NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.	6.18. ŹRÓDŁO SFINANSOWANIA NABYCIA NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.
6.19. SPOSÓB NABYCIA NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.	6.20. DATA NABYCIA NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.
6.21. CENA NABYCIA NIERUCHOMOŚCI WSKAZANEJ W PKT 6.11.	
6.22. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE INNE (POZA WSKAZANYMI W PKT 6.1 – 6.21.) NIERUCHOMOŚCI? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 6.1. – 6.10.) TAK ☐ NIE ☐	
7. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE FIRMĘ (PRZEDSIĘBIORSTWO) LUB AKCJE (UDZIAŁY) W SPÓŁCE (FIRMIE, PRZEDSIĘBIORSTWIE)? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 7.1. – 7.10.) TAK ☐ NIE ☐	
7.1. IMIĘ WŁAŚCICIELA (WSPÓŁWŁAŚCICIELA) FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW)	7.2. NAZWISKO WŁAŚCICIELA (WSPÓŁWŁAŚCICIELA) FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW)
7.3. NAZWA FIRMY (PRZEDSIĘBIORSTWA) LUB FIRMY (PRZEDSIĘBIORSTWA), KTÓREJ OSOBA WSKAZANA W PKT 7.1. – 7.2. POSIADA AKCJE (UDZIAŁY)	
7.4. % WŁASNOŚCI FIRMY (PRZEDSIĘBIORSTWA) LUB LICZBA AKCJI (UDZIAŁÓW)	7.5. ŹRÓDŁO SFINANSOWANIA FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW)

7.6. SPOSÓB NABYCIA FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW)	7.7. DATA NABYCIA FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW)
7.8. CENA NABYCIA FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW)	7.9. OBECNA SZACUNKOWA WARTOŚĆ FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW)

7.10. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE INNE, POZA WSKAZANYMI W PKT 7.1. – 7.9., FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJE (UDZIAŁY) W SPÓŁCE (FIRMIE, PRZEDSIĘBIORSTWIE)?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 7.11. – 7.20.)

TAK ☐ NIE ☐

7.11. IMIĘ WŁAŚCICIELA (WSPÓŁWŁAŚCICIELA) FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW), WSKAZANYCH W PKT 7.10.	7.12. NAZWISKO WŁAŚCICIELA (WSPÓŁWŁAŚCICIELA) FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW), WSKAZANYCH W PKT 7.10.

7.13. NAZWA FIRMY (PRZEDSIĘBIORSTWA) LUB FIRMY (PRZEDSIĘBIORSTWA), WSKAZANEJ W PKT 7.10, KTÓREJ OSOBA WSKAZANA W PKT 7.11. – 7.12. POSIADA AKCJE (UDZIAŁY)

7.14. % WŁASNOŚCI FIRMY (PRZEDSIĘBIORSTWA) LUB LICZBA AKCJI (UDZIAŁÓW), WSKAZANYCH W PKT 7.13.	7.15. ŹRÓDŁO SFINANSOWANIA FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW) WSKAZANYCH W PKT 7.13.
7.16. SPOSÓB NABYCIA FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW), WSKAZANYCH W PKT 7.13.	7.17. DATA NABYCIA FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW), WSKAZANYCH W PKT 7.13.
7.18. CENA NABYCIA FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW), WSKAZANYCH W PKT 7.13.	7.19. OBECNA SZACUNKOWA WARTOŚĆ FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJI (UDZIAŁÓW), WSKAZANYCH W PKT 7.13.

7.20. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE INNE, POZA WSKAZANYMI W PKT 7.1. – 7.19., FIRMY (PRZEDSIĘBIORSTWA) LUB AKCJE (UDZIAŁY) W SPÓŁCE (FIRMIE, PRZEDSIĘBIORSTWIE)? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 7.1. – 7.10.)

TAK ☐ NIE ☐

8. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE RUCHOMOŚCI, KTÓRYCH JEDNOSTKOWY KOSZT NABYCIA LUB JEDNOSTKOWA WARTOŚĆ PRZEKRACZA 20 000 ZŁ (PLN)?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 8.1. – 8.10.)

TAK ☐ NIE ☐

8.1. IMIĘ WŁAŚCICIELA (WSPÓŁWŁAŚCICIELA) RUCHOMOŚCI	8.2. NAZWISKO WŁAŚCICIELA (WSPÓŁWŁAŚCICIELA) RUCHOMOŚCI

8.3. NAZWA RUCHOMOŚCI

8.4. % WŁASNOŚCI RUCHOMOŚCI	8.5. ŹRÓDŁO SFINANSOWANIA NABYCIA RUCHOMOŚCI
8.6. SPOSÓB NABYCIA RUCHOMOŚCI	8.7. DATA NABYCIA RUCHOMOŚCI
8.8. CENA NABYCIA RUCHOMOŚCI	8.9. OBECNA SZACUNKOWA WARTOŚĆ RUCHOMOŚCI

8.10. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE INNE, NIŻ WSKAZANE W PKT 8. – 8.9., RUCHOMOŚCI, KTÓRYCH JEDNOSTKOWY KOSZT NABYCIA LUB JEDNOSTKOWA WARTOŚĆ PRZEKRACZA 20 000 ZŁ (PLN)?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 8.11. – 8.20.)

TAK ☐ NIE ☐

8.11. IMIĘ WŁAŚCICIELA/WSPÓŁWŁAŚCICIELA RUCHOMOŚCI WSKAZANEJ W PKT 8.10.	8.12. NAZWISKO WŁAŚCICIELA/WSPÓŁWŁAŚCICIELA RUCHOMOŚCI WSKAZANEJ W PKT 8.10.
8.13. NAZWA RUCHOMOŚCI WSKAZANEJ W PKT 8.10.	
8.14. % WŁASNOŚCI RUCHOMOŚCI WSKAZANEJ W PKT 8.10.	8.15. ŹRÓDŁO SFINANSOWANIA NABYCIA RUCHOMOŚCI, WSKAZANEJ W PKT 8.10.
8.16. SPOSÓB NABYCIA RUCHOMOŚCI WSKAZANEJ W PKT 8.10.	8.17. DATA NABYCIA WSKAZANEJ W PKT 8.10.
8.18. CENA NABYCIA RUCHOMOŚCI WSKAZANEJ W PKT 8.10.	8.19. OBECNA SZACUNKOWA WARTOŚĆ WSKAZANEJ W PKT 8.10.

8.20. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE INNE, NIŻ WSKAZANE W PKT 8. – 8.19., RUCHOMOŚCI, KTÓRYCH JEDNOSTKOWY KOSZT NABYCIA LUB JEDNOSTKOWA WARTOŚĆ PRZEKRACZA 20 000 ZŁ (PLN)? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 8.1. – 8.9.)

TAK ☐ NIE ☐

9. CZY POSIADA PANI (PAN) LUB JEST WSPÓŁPOSIADACZEM RACHUNKU ALBO RACHUNKÓW BANKOWYCH? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 9.1. – 9.5.)

TAK ☐ NIE ☐

9.1. STATUS

JEDYNY WŁAŚCICIEL ☐ **WSPÓŁWŁAŚCICIEL** ☐

9.2. NAZWA BANKU

9.3.. ADRES BANKU

9.4. NUMER RACHUNKU

9.5. CZY POSIADA PANI (PAN) LUB JEST WSPÓŁPOSIADACZEM RACHUNKU ALBO RACHUNKÓW BANKOWYCH – INNYCH, NIŻ WSKAZANE W PKT 9. – 9.4.? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 9.6. – 9.10.)

TAK ☐ NIE ☐

9.6. STATUS – ODNOŚNIE DO RACHUNKU Z PKT 9.5.

JEDYNY WŁAŚCICIEL ☐ **WSPÓŁWŁAŚCICIEL** ☐

9.7. NAZWA BANKU – ODNOŚNIE DO RACHUNKU Z PKT 9.5.

9.8. ADRES BANKU – ODNOŚNIE DO RACHUNKU Z PKT 9.5.

9.9. NUMER RACHUNKU Z PKT 9.5.

9.10. CZY POSIADA PANI (PAN) LUB JEST WSPÓŁPOSIADACZEM RACHUNKU ALBO RACHUNKÓW BANKOWYCH – INNYCH, NIŻ WSKAZANE W PKT 9. – 9.9.? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 9.1. – 9.5.)

TAK ☐ NIE ☐

10. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE JESTEŚCIE ZADŁUŻENI LUB POSIADACIE JAKIEKOLWIEK INNE ZOBOWIĄZANIA FINANSOWE *(np. kredyty, zaległości podatkowe, alimenty, spłaty hipoteki lub zastawu, należności wynikające z orzeczeń sądowych)* ?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 10.1. – 10.13.)

TAK ☐ NIE ☐

10.1. IMIĘ OSOBY POSIADAJĄCEJ ZOBOWIĄZANIE	10.2. NAZWISKO OSOBY POSIADAJĄCEJ ZOBOWIĄZANIE
10.3. NAZWA ZOBOWIĄZANIA FINANSOWEGO	
10.4. NAZWA I NUMER DOKUMENTU, NA PODSTAWIE KTÓREGO POWSTAŁO ZOBOWIĄZANIE	
10.5. NAZWA LUB IMIĘ I NAZWISKO WIERZYCIELA	
10.6. CAŁKOWITA KWOTA ZOBOWIĄZANIA	10.7. KWOTA POZOSTAŁA DO SPŁATY
10.8. WYSOKOŚĆ MIESIĘCZNEJ RATY ZOBOWIĄZANIA	10.9. LICZBA RAT POZOSTAŁYCH DO SPŁATY
10.10. DATA POWSTANIA ZOBOWIĄZANIA	10.11. DATA PRZEWIDYWALNEJ CAŁKOWITEJ SPŁATY

10.12. CZY KIEDYKOLWIEK MIAŁO MIEJSCE OPÓŹNIENIE SPŁATY ZOBOWIĄZANIA WSKAZANEGO W PKT 10.1. – 10.11.?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU)

TAK ☐ NIE ☐

10.13. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE JAKIEKOLWIEK INNE ZOBOWIĄZANIA FINANSOWE, NIEWSKAZANE W PKT 10.1. – 10.12.?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 10.14. – 10.26.)

TAK ☐ NIE ☐

10.14. IMIĘ OSOBY POSIADAJĄCEJ ZOBOWIĄZANIE, WSKAZANE W PKT 10.13.	10.15. NAZWISKO OSOBY POSIADAJĄCEJ ZOBOWIĄZANIE, WSKAZANE W PKT 10.13.
10.16. NAZWA ZOBOWIĄZANIA FINANSOWEGO WSKAZANEGO W PKT 10.13.	
10.17. NAZWA I NUMER DOKUMENTU, NA PODSTAWIE KTÓREGO POWSTAŁO ZOBOWIĄZANIE WSKAZANE W PKT 10.13.	
10.18. NAZWA LUB IMIĘ I NAZWISKO WIERZYCIELA ZOBOWIĄZANIA FINANSOWEGO WSKAZANEGO W PKT 10.13.	
10.19. CAŁKOWITA KWOTA ZOBOWIĄZANIA WSKAZANEGO W PKT 10.13.	10.20. KWOTA POZOSTAŁA DO SPŁATY ZOBOWIĄZANIA WSKAZANEGO W PKT 10.13.
10.21. WYSOKOŚĆ MIESIĘCZNEJ RATY ZOBOWIĄZANIA WSKAZANEGO W PKT 10.13.	10.22. LICZBA RAT POZOSTAŁYCH DO SPŁATY ZOBOWIĄZANIA WSKAZANEGO W PKT 10.13.
10.23. DATA POWSTANIA ZOBOWIĄZANIA WSKAZANEGO W PKT 10.13.	10.24. DATA PRZEWIDYWALNEJ CAŁKOWITEJ SPŁATY ZOBOWIĄZANIA WSKAZANEGO W PKT 10.13.

10.25. CZY KIEDYKOLWIEK MIAŁO MIEJSCE OPÓŹNIENIE SPŁATY ZOBOWIĄZANIA WSKAZANEGO W PKT 10.13.?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU)

TAK ☐ NIE ☐

10.26. CZY PANI (PAN) LUB OSOBY PROWADZĄCE Z PANIĄ (PANEM) WSPÓLNE GOSPODARSTWO DOMOWE POSIADACIE JAKIEKOLWIEK INNE ZOBOWIĄZANIA FINANSOWE, NIEWSKAZANE W PKT 10. – 10.25.? (PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić odpowiedni załącznik według schematu z pkt 10.1. – 10.12.)

TAK ☐ NIE ☐

11. CZY PO UKOŃCZENIU 18 LAT UCZESTNICTWO W GRACH HAZARDOWYCH BYŁO KIEDYKOLWIEK PRZYCZYNĄ PROBLEMÓW W PANI (PANA) PRACY LUB W ŻYCIU PRYWATNYM?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 11.1. – 11.2.)

TAK ☐ NIE ☐

11.1. PROSZĘ WSKAZAĆ, JAKIE PROBLEMY	11.2. KIEDY?

CZĘŚĆ VII: OSOBY POLECAJĄCE

A.

1. PIERWSZE IMIĘ	2. NAZWISKO
3. NR PESEL	**4. NR TELEFONU KONTAKTOWEGO**

5. ADRES ZAMIESZKANIA (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

6. NAZWA MIEJSCA ZATRUDNIENIA

7. ADRES MIEJSCA ZATRUDNIENIA (ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

8. ZAJMOWANE STANOWISKO

B.

1. PIERWSZE IMIĘ	2. NAZWISKO
3. NR PESEL	**4. NR TELEFONU KONTAKTOWEGO**

5. ADRES ZAMIESZKANIA (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

6. NAZWA MIEJSCA ZATRUDNIENIA

7. ADRES MIEJSCA ZATRUDNIENIA (ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)

8. ZAJMOWANE STANOWISKO

C.

1. PIERWSZE IMIĘ	2. NAZWISKO
3. NR PESEL	**4. NR TELEFONU KONTAKTOWEGO**

5. ADRES ZAMIESZKANIA (ULICA, NR DOMU, NR MIESZKANIA, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)
6. NAZWA MIEJSCA ZATRUDNIENIA
7. ADRES MIEJSCA ZATRUDNIENIA (ULICA, NR DOMU, KOD POCZTOWY, MIEJSCOWOŚĆ, KRAJ, NR TELEFONU)
8. ZAJMOWANE STANOWISKO

Oświadczam, iż wypełniłam (wypełniłem) ankietę osobiście, zgodnie ze swoją wiedzą, świadoma (świadomy), że każde fałszywe stwierdzenie lub pominięcie istotnego faktu będzie mogło stanowić podstawę odmowy wydania mi poświadczenia bezpieczeństwa.

Oświadczam, że zgadzam się na przeprowadzenie wobec mnie postępowania sprawdzającego według przepisów ustawy dnia o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. Nr , poz.).

MIEJSCOWOŚĆ I DATA WYPEŁNIENIA ANKIETY	PODPIS OSOBY SPRAWDZANEJ

U Z A S A D N I E N I E

Ochronę informacji niejawnych w Rzeczypospolitej Polskiej normuje ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (tekst pierwotny opublikowany w Dz. U. Nr 11, poz. 95), która w okresie swego obowiązywania doczekała się 23 nowelizacji. Charakter tych zmian był rozmaity: od zmian porządkujących, wynikających z nowelizacji bądź uchwalania nowych ustaw – po zasadnicze zmiany merytoryczne samej ustawy o ochronie informacji niejawnych.

Obowiązująca od 10 lat ustawa o ochronie informacji niejawnych pozwoliła stworzyć współczesny system ochrony informacji niejawnych oraz odegrała istotną rolę w okresie akcesji Polski do Sojuszu Północnoatlantyckiego. Obecnie jednak wiele jej przepisów jest już przestarzałych i niefunkcjonalnych. W ciągu mijających 10 lat dokonał się ogromny postęp technologiczny, zwłaszcza w zakresie środków łączności oraz systemów teleinformatycznych. Zawarte w ustawie i aktach wykonawczych rozwiązania dotyczące zwłaszcza bezpieczeństwa teleinformatycznego i fizycznego odstają od aktualnego poziomu technologicznego i nie są dostosowane do warunków i możliwości współczesnej techniki.

Warto przy tym zauważyć, że ustawa z 1999 r. była w pewnej mierze wzorowana na rozwiązaniach zawartych w dokumencie C-M(55)15(Final) określającym politykę bezpieczeństwa Sojuszu Północnoatlantyckiego, opracowanym w 1955 r. W samym NATO, wobec narastającego przeświadczenia, że liczące blisko 50 lat rozwiązania są już przestarzałe, przyjęto w 2002 r. nowy dokument regulujący politykę bezpieczeństwa – C-M(2002)49 – który wprowadza zasady znacznie bardziej elastyczne i umożliwia szerokie stosowanie zarządzania ryzykiem w miejsce dawniej obowiązujących standardów minimalnych. W tym kierunku szły też zmiany wprowadzane przez dyrektywy wykonawcze i wytyczne Biura Bezpieczeństwa NATO, a także dokumenty dotyczące polityki bezpieczeństwa Unii Europejskiej. Były one wykorzystywane w bieżącej działalności polskich krajowych władz bezpieczeństwa, jednak wdrażanie nowoczesnych rozwiązań jest w znacznym stopniu warunkowane zmianami na poziomie ustawy. Dlatego podczas opracowywania nowych rozwiązań ustawowych celowe wydaje się uwzględnienie nie tylko potrzeb polskich instytucji i podmiotów

stosujących ustawę, ale także standardów aktualnie stosowanych przez NATO i Unię Europejską.

Objęcie przez Polskę przewodnictwa w Radzie Unii Europejskiej w 2011 r. stawia przed polską administracją państwową szereg wyzwań wymagających podjęcia pilnych kroków. Jednym z nich jest postulowane od dawna przez Ministerstwo Spraw Zagranicznych dostosowanie polskiego systemu ochrony informacji niejawnych do reguł i praktyki obowiązującej w instytucjach Unii Europejskiej i w krajach członkowskich. Można z dużym prawdopodobieństwem przewidywać, że brak zmiany przepisów dotyczących ochrony informacji niejawnych istotnie utrudniłby, a w wielu przypadkach wręcz uniemożliwiłby realizację zadań związanych z prezydencją. Dotyczy to szczególnie możliwości znacznie bardziej elastycznego traktowania zasad ochrony informacji o niskich klauzulach tajności, co w strukturach unijnych umożliwia szybkie, bieżące wykorzystywanie tych informacji w pracy grup roboczych oraz ich sprawne przekazywanie i przetwarzanie w systemach teleinformatycznych.

System ochrony informacji niejawnych w Polsce wymaga zatem reform bardzo daleko idących, co uzasadnia konieczność podjęcia pracy nad nową ustawą, a nie nad kolejną nowelizacją. Należy też wziąć pod uwagę zakres dokonanych w ustawie do tej pory zmian – tylko jedna z kilkunastu nowelizacji wprowadzona w 2005 r. objęła blisko jedną trzecią artykułów. Biorąc pod uwagę zarówno ilość, jak i zakres zmian poczynionych dotychczas w ustawie o ochronie informacji niejawnych, zasadnie można domniemywać, że kolejna nowela tej ustawy przyczyniłaby się do powstania aktu prawnego o charakterze kompilacyjnym. Mogłaby pogłębić niejasności i niespójności systemowe pojawiające się już obecnie w jej treści i nie poprawiłaby jakości prawa normującego ochronę informacji niejawnych w Rzeczypospolitej Polskiej.

Biorąc pod uwagę wyżej przedstawione okoliczności Prezes Rady Ministrów zobowiązał Sekretarza Stanu w Kancelarii Prezesa Rady Ministrów (KPRM), Sekretarza Kolegium do Spraw Służb Specjalnych do przygotowania założeń do projektu nowej ustawy o ochronie informacji niejawnych. W toku roboczych konsultacji z przedstawicielami służb ochrony państwa zostały opracowane tezy dotyczące zmian w systemie ochrony informacji niejawnych, następnie poddane konsultacjom z członkami Kolegium do Spraw Służb Specjalnych. Tezy te stały się punktem wyjścia do prac nad założeniami projektu nowej ustawy, przygotowywanymi

przez przedstawicieli KPRM i służb ochrony państwa oraz konsultowanymi w trybie roboczym z przedstawicielami Rządowego Centrum Legislacji (RCL). Podczas tych konsultacji przedstawiciele RCL zwrócili uwagę, że forma i treść przygotowanego materiału pozwalają uznać go za gotowy projekt ustawy, a nie tylko projekt założeń do projektu ustawy. W związku z powyższym Szef KPRM uzyskał – na podstawie § 6 ust. 1a pkt 2 Regulaminu Rady Ministrów – zgodę Prezesa Rady Ministrów na odstąpienie od wymogu opracowania i uzgodnienia założeń projektu ustawy o ochronie informacji niejawnych.

Aktualnie dziedzina regulacji projektowanej ustawy jest unormowana następującymi aktami prawnymi:

– ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.) oraz przepisami wykonawczymi wydanymi na jej podstawie;

– ratyfikowanymi bilateralnymi umowami międzynarodowymi o wzajemnej ochronie informacji niejawnych zawartymi z: Albanią, Bułgarią, Chorwacją, Czechami, Estonią, Finlandią, Francją, Hiszpanią, Łotwą, Norwegią, RFN, Rosją, Rumunią, Słowacją, Szwecją, Ukrainą, USA, Wielką Brytanią i Irlandią Północną oraz Włochami;

– Umową między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzoną w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r. Nr 64, poz. 740) oraz Umową między Stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych, sporządzoną w Paryżu dnia 18 czerwca 1964 r. (Dz. U. z 2001 r. Nr 143, poz. 1594).

Istotą projektu nowej ustawy o ochronie informacji niejawnych jest takie unormowanie systemu ich ochrony, aby był on maksymalnie efektywny zarówno w sferze krajowej, jak i zagranicznej, przy jednoczesnej prostocie i elastyczności funkcjonowania, ale bez uszczerbku dla bezpieczeństwa informacji niejawnych. Podstawowym celem stało się uproszczenie istniejącego systemu i jego aktualizacja.

Dotychczasowe rozwiązania powodują bowiem z jednej strony wymóg nadawania klauzul tajności olbrzymiej liczbie informacji, w wielu przypadkach niewymagających ochrony oraz notoryczne zawyżanie klauzul bez żadnego racjonalnego uzasadnienia, z tego tylko powodu, że dana informacja, w pewnych okolicznościach może stanowić

informację niejawną. Z drugiej strony obowiązujące aktualnie prawo wymusza wręcz rezygnację z nadawania klauzul bardzo ważnym informacjom z powodu konieczności ich szybkiego przetwarzania i przekazywania do odbiorców.

Dwustopniowy system definiowania informacji niejawnych i rozdęte, a w praktyce całkowicie lekceważone wykazy zawarte w załączniku do ustawy, tylko pogłębiają chaos. Wynika stąd m. in. potrzeba rezygnacji z podziału informacji niejawnych na tajemnicę państwową i służbową (nieobowiązującego w takiej postaci w żadnym kraju NATO lub Unii Europejskiej); dziesięcioletnia praktyka funkcjonowania tego podziału wskazuje, że jest on sztuczny i nie ma większego sensu praktycznego. Kolejnym jakościowym założeniem merytorycznym jest odejście od rozbudowanych formalnych wykazów informacji niejawnych na rzecz jednoznacznego zobowiązania wytwórców informacji do kierowania się nowymi definicjami poszczególnych klauzul. Należy zwrócić uwagę, że zawieranie w ustawie wykazu informacji niejawnych nie jest standardowym rozwiązaniem w państwach o długiej tradycji demokratycznej, a w wielu z nich ograniczono się do sformułowania w przepisach krótkich definicji poszczególnych klauzul.

Duże znaczenie dla uproszczenia systemu ochrony informacji niejawnych i radykalnego zmniejszenia ich liczby, a także liczby jednostek organizacyjnych je przetwarzających (a co za tym idzie dużych, trudnych do oszacowania oszczędności budżetowych), powinna mieć rezygnacja z traktowania informacji dotyczących prawnie chronionych interesów obywateli i jednostek organizacyjnych jako informacji niejawnych. Ochronie określonej przepisami ustawy powinny podlegać tylko takie informacje, których ujawnienie przyniosłoby szkody interesom państwa, gdyż sposób postępowania z informacjami dotyczącymi obywateli i jednostek organizacyjnych, a objętymi tajemnicami różnego rodzaju, jest przewidziany w innych ustawach normujących te tajemnice. Nie bez znaczenia pozostaje tu lepsza niż dotychczas realizacja postulatu transparentności funkcjonowania administracji oraz rozszerzenie zakresu dostępu do informacji publicznej.

Inną ważną zmianą, która została wyraźnie określona w projekcie ustawy, a potem szczegółowo unormowana w aktach wykonawczych, będzie umożliwienie stosowania zarządzania ryzykiem przy określaniu wymogów bezpieczeństwa fizycznego i teleinformatycznego. Umożliwi to istotne ograniczenie nadmiernych

i anachronicznych wymogów oraz związanych z nimi wydatków przez dopasowanie stosowanych środków ochrony do liczby i wagi chronionych informacji oraz rzeczywistego (a nie formalnego) poziomu istniejących dla nich zagrożeń. Wprowadzenie tego rozwiązania powinno też znacząco ułatwić akredytację systemów teleinformatycznych przygotowanych do przekazywania i przetwarzania informacji niejawnych, co będzie miało kluczowe znaczenie w okresie prezydencji w Unii Europejskiej. Zastrzec tu należy, że ideą nie jest obniżenie standardów ochrony, ale ich adekwatne i efektywne stosowanie na rzecz odejścia od konieczności stosowania sztywnych wymogów formalnych.

Z punktu widzenia skuteczności polskiej prezydencji bardzo ważna jest propozycja dotycząca rezygnacji ze ścisłej kontroli obiegu dokumentów o niższych klauzulach, a zwłaszcza o klauzuli „zastrzeżone". Dzięki zliberalizowaniu zasad ochrony tych informacji zostanie wprowadzony system bardziej elastyczny, analogiczny do obowiązującego w strukturach Unii Europejskiej i w większości krajów członkowskich. Zmiana przepisów w tym zakresie była od dawna postulowana przez Ministerstwo Spraw Zagranicznych. Będzie można również osiągnąć znaczące oszczędności w budżetach jednostek administracji państwowej i samorządowej w związku z rezygnacją ze zbędnych środków ochrony informacji o niskich klauzulach.

Zmiany wynikające z przedłożonego projektu ustawy – w porównaniu do dotychczasowego stanu prawnego są następujące:

Rozdział 1 – „Przepisy ogólne" określa zakres obowiązywania ustawy i podmioty, do których ma ona zastosowanie, definiuje podstawowe pojęcia, wymienia przepisy kodeksu postępowania administracyjnego mające zastosowanie do postępowań określonych w ustawie oraz wskazuje na najważniejsze zasady regulujące udostępnianie informacji niejawnych.

Art. 2 precyzuje niektóre pojęcia używane w ustawie, w tym:

„przedsiębiorca" – ustawa będzie odnosić się już nie tylko do przedsiębiorców, jednostek naukowych i badawczo-rozwojowych, ale także do wszelkich innych jednostek organizacyjnych, które w ramach prowadzonej działalności gospodarczej realizują umowy lub zadania związane z dostępem do informacji niejawnych; dotychczasowa definicja tworzyła lukę pomijając spółdzielnie i inne jednostki działające na podstawie odrębnych ustaw;

„kierownik przedsiębiorcy” – brak definicji tego pojęcia powodował liczne wątpliwości i konieczność formułowania przez służby ochrony państwa doraźnych interpretacji w postępowaniach bezpieczeństwa przemysłowego, zwłaszcza w przypadku zarządów wieloosobowych, a także spółek cywilnych, jawnych, partnerskich, komandytowych oraz przedsiębiorców w stanie upadłości;

„przetwarzanie informacji niejawnych” – brak tej definicji powodował konieczność wyliczania w wielu miejscach dotychczasowej ustawy różnych rodzajów czynności wykonywanych wobec informacji niejawnych;

„ryzyko”, „szacowanie ryzyka” i „zarządzanie ryzykiem” – pojęcia kluczowe dla nowoczesnego podejścia do ochrony informacji niejawnych, zdefiniowane w Polskiej Normie PN-ISO/IEC 17799:2007.

Art. 3 istotnie rozszerza zakres stosowania kodeksu postępowania administracyjnego w postępowaniach sprawdzających. Nie było jednak możliwe wprowadzenie pełnego stosowania kpa, gdyż istotą postępowań z kpa jest ich pełna transparentność i możliwość udziału stron we wszystkich etapach postępowania, podczas gdy postępowanie sprawdzające jest w dużej mierze niejawne. Ponadto kwestia organów wyższego stopnia jest w ustawie regulowana odmiennie niż w kpa. Należy też zwrócić uwagę, że pominięcie postępowań odwoławczych w tym artykule ma charakter jedynie porządkujący, gdyż postępowania odwoławcze nie są odrębnym rodzajem postępowań obok postępowań sprawdzających w zakresie bezpieczeństwa osobowego lub bezpieczeństwa przemysłowego, tak więc wskazane w art. 3 przepisy kpa będą miały do postępowań odwoławczych takie samo zastosowanie, jak do wcześniejszych etapów postępowań sprawdzających i będzie to przedmiotem oceny sądów administracyjnych w postępowaniu skargowym.

Rozdział 2 – „Klasyfikowanie informacji niejawnych” definiuje poszczególne klauzule tajności oraz określa zasady nadawania, zmiany i znoszenia klauzul tajności.

Art. 5 zawiera nowe definicje informacji niejawnych oznaczonych poszczególnymi klauzulami, które będą obowiązywały w miejsce dotychczasowych, bardzo ogólnych definicji tajemnicy państwowej i służbowej, nieprecyzyjnych definicji poszczególnych klauzul oraz wykazów informacji niejawnych w załączniku do ustawy.

Możliwość stosowania klauzuli „ściśle tajne” zostanie ograniczona do bardzo nielicznych informacji, których ujawnienie spowodowałoby wyjątkowo poważne szkody dla Polski, a które dotyczą polityki międzynarodowej i obronności państwa, czynności operacyjno-rozpoznawczych służb wywiadu i kontrwywiadu, bądź też mają bezpośrednie znaczenie dla niepodległości i porządku konstytucyjnego RP.

Definicja klauzuli „tajne” będzie dotyczyła informacji, których ujawnienie spowodowałoby poważne szkody dla państwa w obszarze polityki międzynarodowej, obronności, ochrony suwerenności i porządku konstytucyjnego, interesów gospodarczych państwa, a także działań operacyjno-rozpoznawczych służb do tego uprawnionych.

Największa zmiana dotyczy dotychczasowej „tajemnicy służbowej”, ponieważ zrezygnowano z oznaczania klauzulami „poufne” lub „zastrzeżone” informacji chronionych na podstawie innych ustaw, a definicje tych klauzul odniesiono jedynie do ewentualnych szkód, które ujawnienie informacji mogłoby przynieść dla bezpieczeństwa i interesów RP.

W ten sposób dotychczasowe informacje stanowiące tajemnicę państwową lub służbową zostaną ograniczone do informacji niejawnych zawierających w pewnym sensie „tajemnicę państwową o 4 klauzulach”, przy czym znaczna część informacji do tej pory „ściśle tajnych” powinna być klauzulowana jako „tajne” lub „poufne”, „tajnych” jako „poufne” lub „zastrzeżone”, a większość informacji stanowiących tajemnicę służbową, z wyjątkiem odnoszących się do interesu państwa, powinna przestać być chroniona na podstawie ustawy o ochronie informacji niejawnych.

Art. 6 określa zasady znoszenia lub zmiany klauzuli tajności, odchodząc od zdefiniowanych z góry okresów obowiązywania klauzul na rzecz możliwości zniesienia lub zmiany klauzuli w przypadku ustania lub zmiany ustawowych przesłanek ochrony. Zostanie wprowadzony obowiązek przeglądu wszystkich wytworzonych dokumentów niejawnych raz na pięć lat (analogicznie do rozwiązań przyjętych w strukturach Unii Europejskiej) w celu określenia, czy informacje te spełniają nadal ustawowe przesłanki, określone w art. 5, które były podstawą nadania im klauzuli tajności. Jeżeli przegląd wykaże, że brak przesłanek do dalszej ochrony tych informacji na określonym poziomie, powinna nastąpić zmiana lub zniesienie nadanej klauzuli. Na większą elastyczność obowiązującego systemu będzie też miała wpływ możliwość określenia

z góry (niezależnie od klauzuli) daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności, a także możliwość odrębnego klazulowania poszczególnych części dokumentu.

Art. 7 określa jedyny rodzaj informacji podlegających ochronie bez względu na upływ czasu, w stosunku do których zniesienie klauzuli tajności w trybie określonym w art. 6 nie będzie możliwe. Są to informacje mogące identyfikować funkcjonariuszy, żołnierzy lub pracowników służb i instytucji uprawnionych do wykonywania czynności operacyjno-rozpoznawczych, a także osoby udzielające pomocy w wykonywaniu tych czynności.

Art. 9 wprowadza możliwość odwołania się od decyzji wytwórcy dotyczącej nadania klauzuli tajności do ABW lub SKW, a w przypadku sporu z jedną z tych służb – do Prezesa Rady Ministrów. W dotychczasowym systemie odbiorca mógł tylko apelować do wytwórcy o zmianę nieprawidłowej klauzuli. Ta możliwość powinna wpłynąć na ograniczenie liczby przypadków bezpodstawnego zawyżania lub zaniżania klauzul tajności.

Rozdział 3 – „Organizacja ochrony informacji niejawnych" określa zadania ABW, SKW, kierowników jednostek organizacyjnych oraz pełnomocników i pionów ochrony.

Art. 10 wskazuje na zadania ABW i SKW oraz jednoznacznie określa ich właściwość, co powinno wyeliminować w przyszłości zjawisko prowadzenia przez obie służby czynności wobec tych samych podmiotów, zwłaszcza w obszarze bezpieczeństwa przemysłowego.

Art. 11 wprowadza instytucję jednej krajowej władzy bezpieczeństwa odpowiedzialnej za ochronę informacji niejawnych wymienianych z NATO i Unią Europejską. Jest to model funkcjonujący w zdecydowanej większości krajów NATO i UE, gdzie za określanie standardów ochrony informacji otrzymywanych z zagranicy oraz za współpracę ze strukturami bezpieczeństwa NATO, UE i innych krajów odpowiada tylko jedna instytucja. Nowy model powinien skutecznie zlikwidować mankamenty dotychczasowego rozwiązania polegającego na równoległym pełnieniu funkcji krajowej władzy bezpieczeństwa przez szefów ABW i SKW, związane z funkcjonowaniem odmiennych standardów ochrony tych informacji w sferze cywilnej i wojskowej, na co niejednokrotnie zwracały uwagę inspekcje struktur bezpieczeństwa NATO i UE. Zmiana ta doprowadzi także do ustanowienia jednej polskiej reprezentacji w kontaktach

z partnerami zagranicznymi, gdyż reprezentowanie Polski przez dwie odrębne, równorzędne delegacje w różnych gremiach międzynarodowych odpowiedzialnych za bezpieczeństwo budziło do tej pory zdziwienie naszych partnerów. Skutkiem nowego rozwiązania powinno też być wdrożenie ujednoliconych standardów w zakresie ochrony informacji niejawnych wymienianych ze strukturami organizacji międzynarodowych oraz w ramach współpracy bilateralnej z zagranicą.

Funkcję krajowej władzy bezpieczeństwa będzie pełnił Szef ABW, natomiast jej zadania wobec podmiotów sfery wojskowej będą wykonywane za pośrednictwem Szefa SKW. Oznacza to, że w kompetencjach szefa SKW pozostanie prowadzenie postępowań sprawdzających oraz wydawanie poświadczeń, świadectw i certyfikatów w sferze wojskowej. Natomiast zadaniem Szefa ABW będzie zapewnienie jednolitości i zgodności systemu ochrony informacji niejawnych z odpowiednimi przepisami bezpieczeństwa organizacji międzynarodowych oraz organizacja działań w zakresie reprezentowania Rzeczypospolitej Polskiej przed organami organizacji międzynarodowych i krajowych władz bezpieczeństwa innych państw, a także wypełniania innych zadań właściwych krajowej władzy bezpieczeństwa.

Art. 12 reguluje zasady prowadzenia przez ABW i SKW kontroli stanu zabezpieczenia informacji niejawnych. Usuwa niejasność zawartą w dotychczasowych przepisach, które nakazywały służbom kontrolę ochrony informacji niejawnych, ale regulowały tylko kontrolę zabezpieczenia tajemnicy państwowej.

Ponadto uzupełniono zakres kontroli o możliwość żądania udostępnienia systemów teleinformatycznych nieposiadających akredytacji (czyli nieprzeznaczonych do przetwarzania informacji niejawnych), ale wyłącznie w przypadku uprzedniego ustalenia okoliczności wskazujących na przetwarzanie w tych systemach informacji niejawnych. Zapis ten jest efektem doświadczeń wynikających z kontroli prowadzonych przez ABW lub SKW, które niejednokrotnie natrafiały na przypadki wytwarzania dokumentów niejawnych w niecertyfikowanych systemach, ale bez możliwości kontroli zawartości tych komputerów udowodnienie stwierdzonych uchybień było bardzo trudne.

Nowym rozwiązaniem jest rozszerzenie kontroli prawidłowości postępowań sprawdzających. Do tej pory takiej kontroli podlegały wyłącznie postępowania prowadzone przez pełnomocników ochrony. Postępowania prowadzone przez ABW

i SKW nie podlegały kontroli z wyjątkiem postępowania odwoławczo-skargowego w przypadku odmowy lub cofnięcia poświadczenia bezpieczeństwa. Proponowane zapisy przewidują możliwość kontrolowania postępowań prowadzonych przez ABW i SKW – przez Prezesa Rady Ministrów. Zwiększenie kontroli nad działaniami służb powinno mieć istotny pozytywny wpływ na podwyższenie standardów postępowań i być gwarancją respektowania praw osób sprawdzanych.

Z kontroli postępowań sprawdzających pozostaną wyłączone postępowania prowadzone przez pełnomocników ochrony w służbach i instytucjach wskazanych w art. 24 ustawy. Celem tego rozwiązania jest ograniczenie do absolutnego minimum liczby osób mających dostęp do szczegółowych danych funkcjonariuszy i żołnierzy wykonujących zadania operacyjno-rozpoznawcze. Konsekwencją jest jednak ograniczenie ważności poświadczeń wydanych w służbach i instytucjach uprawnionych do samodzielnego prowadzenia poszerzonych postępowań sprawdzających jedynie do okresu pracy lub służby w tych jednostkach organizacyjnych.

Kontrole zabezpieczenia informacji niejawnych prowadzone przez SKW i ABW będą odbywać się, tak jak do tej pory, w oparciu o przepisy ustawy o Najwyższej Izbie Kontroli. Przepisy ustawy o NIK będą miały również zastosowanie do kontroli prawidłowości postępowań sprawdzających prowadzonych przez ABW lub SKW, a także przez Prezesa Rady Ministrów. Dodanie, jako mającego zastosowanie do tych kontroli, art. 98 ustawy o NIK powinno wyeliminować sytuacje odmowy okazania dokumentu lub braku odpowiedzi na pytania zadawane przez kontrolera, co uniemożliwia ustalenie stanu faktycznego.

Rozdział 4 – „Szkolenia w zakresie ochrony informacji niejawnych" określa zasady prowadzenia szkoleń poprzedzających udostępnienie informacji niejawnych.

Art. 19 nakłada na ABW i SKW obowiązek prowadzenia szkoleń kierowników jednostek organizacyjnych. Szkolenia takie będą prowadzone przez służby wspólnie z pełnomocnikami ochrony. Funkcjonariusze lub żołnierze SKW lub ABW będą szkolić kierowników jednostek organizacyjnych w zakresie funkcjonowania całego systemu ochrony informacji niejawnych i różnego rodzaju zagrożeń dla tych informacji, co powinno mieć istotny wpływ na wzrost świadomości osób odpowiedzialnych za zapewnienie ochrony informacji niejawnych w jednostkach organizacyjnych, natomiast

pełnomocnicy ochrony będą przedstawiać szczegółowe informacje związane ze specyfiką obiegu i ochrony informacji niejawnych w danej instytucji.

Wszystkie osoby mające dostęp do informacji niejawnych będą szkolone w zakresie ochrony tych informacji nie rzadziej niż co 5 lat. Do tej pory ustawa przewidywała cykliczność szkoleń wyłącznie w przypadku pełnomocników ochrony i ich zastępców.

Projekt nakłada na pełnomocników ochrony obowiązek przeprowadzenia szkoleń pracowników w zakresie ochrony informacji niejawnych co 5 lat. Dotyczy to również tych pracowników, którzy będą mieli dostęp tylko do informacji o klauzuli „zastrzeżone". 5 lat jest okresem dość długim, szczególnie dla tych pracowników, którzy nie mają na co dzień do czynienia z pracą z dokumentami niejawnymi.

Rozdział 5 – „Bezpieczeństwo osobowe" określa zasady prowadzenia postępowań sprawdzających wobec osób mających uzyskać dostęp do informacji niejawnych.

Art. 21 znosi istniejący do tej pory obowiązek prowadzenia postępowań sprawdzających wobec osób, które mają uzyskać dostęp do informacji niejawnych o klauzuli „zastrzeżone". W ten sposób zostaje wprowadzony system obowiązujący w większości krajów Europy oraz w NATO i UE zakładający, że poświadczenia bezpieczeństwa obowiązują od poziomu „poufne" wzwyż, a podstawą do udostępnienia informacji o najniższej klauzuli tajności jest potrzeba wynikająca z wykonywania określonych obowiązków służbowych. Dostęp do informacji niejawnych o klauzuli „zastrzeżone" będzie możliwy na podstawie pisemnego upoważnienia kierownika jednostki organizacyjnej po odbyciu stosownego przeszkolenia.

Art. 22 i 23 wprowadzają dwa rodzaje postępowań sprawdzających w miejsce dotychczasowych trzech. Zwykłe postępowania sprawdzające będą prowadzone przez pełnomocników ochrony wobec osób ubiegających się o dostęp do informacji niejawnych o klauzuli „poufne". Poszerzone postępowania sprawdzające będą prowadzone przez ABW lub SKW wobec osób ubiegających się o dostęp do informacji niejawnych o klauzuli „tajne" i „ściśle tajne", a w niektórych przypadkach również „poufne". Novum jest wprowadzenie zasady prowadzenia przez służby postępowań wobec wszystkich kierowników jednostek organizacyjnych niezależnie od klauzuli, aby uniknąć sytuacji, w której pełnomocnik ochrony będzie prowadził postępowanie sprawdzające wobec swojego pracodawcy. Z tego samego powodu w art. 23 precyzyjnie określono właściwość w zakresie prowadzenia postępowań sprawdzających

wobec szefów służb i pełnomocników ochrony w służbach uprawnionych do samodzielnego prowadzenia poszerzonych postępowań sprawdzających.

Postępowania sprawdzające wobec pracowników, funkcjonariuszy, żołnierzy oraz osób ubiegających się o przyjęcie do pracy lub służby będą prowadziły samodzielnie, tak jak do tej pory, wskazane w ustawie służby lub organy. Ich lista została uzupełniona o Biuro Ochrony Rządu. Nie będą prowadzone postępowania sprawdzające w stosunku do osób ubiegających się o dostęp do informacji niejawnych o klauzuli „zastrzeżone", co już omówiono w uzasadnieniu do art. 21.

Art. 24, określając wątpliwości mogące stać się przesłankami odmowy wydania poświadczenia bezpieczeństwa, precyzuje pojęcie niewłaściwego postępowania z informacjami niejawnymi, aby ograniczyć dowolność interpretacyjną i nie dopuścić do sytuacji, w której podstawą odmowy stałyby się niewielkie uchybienia w tym zakresie.

Art. 25, określając czynności prowadzone w toku postępowania sprawdzającego, zapewnia osobie sprawdzanej możliwość ustosunkowania się do pojawiających się wątpliwości już w postępowaniu zwykłym.

Art. 27 określa sytuacje, w których postępowanie sprawdzające może zostać zawieszone i ponownie podjęte, a także wskazuje na tryb składania zażalenia na postanowienie o zawieszeniu postępowania.

Art. 30 znosi automatyczny zakaz posiadania poświadczenia bezpieczeństwa przez osoby skazane prawomocnym wyrokiem, nakazując ocenę wątpliwości związanych z tym faktem. Pozwoli to na wyeliminowanie przypadków automatycznego cofania poświadczeń bezpieczeństwa osobom skazanym na bardzo niskie wyroki za czyny niemające faktycznie żadnego wpływu na ocenę rękojmi zachowania tajemnicy przez osobę sprawdzaną.

Art. 33 reguluje zasady prowadzenia kontrolnego postępowania sprawdzającego w przypadku ujawnienia informacji kwestionujących dawanie rękojmi zachowania tajemnicy przez osobę posiadającą poświadczenie bezpieczeństwa. Wprowadzona została procedura wstępnej weryfikacji niepotwierdzonych negatywnych informacji dotyczących osoby sprawdzanej – w dotychczasowym systemie służby niejednokrotnie stawały przed dylematem, czy wszczynać postępowanie kontrolne w oparciu o niesprawdzone informacje, biorąc pod uwagę dużą dolegliwość takiej decyzji dla

osoby sprawdzanej (przede wszystkim wyłączenie dostępu do informacji niejawnych skutkujące w wielu przypadkach niemożnością wykonywania obowiązków służbowych na zajmowanym stanowisku. Z tego powodu określono też czas na prowadzenie takiego postępowania – 6 miesięcy, z możliwością wydłużenia w wyjątkowych przypadkach o kolejne 6 miesięcy. Termin 12 miesięcy staje się terminem zawitym, postępowanie kontrolne niezakończone w tym terminie zostaje umorzone z mocy prawa.

Sprecyzowano, który organ jest właściwy do wszczęcia kontrolnego postępowania sprawdzającego stwierdzając, że jest to ten organ, który byłby właściwy do wszczęcia w danym momencie kolejnego postępowania sprawdzającego. Zarazem wprowadzono możliwość wszczęcia takiego postępowania przez ABW lub SKW niezależnie od miejsca aktualnego zatrudnienia osoby sprawdzanej, ale wyłącznie w przypadkach uzasadnionych względami bezpieczeństwa państwa, np. uzyskania przez służbę informacji kontrwywiadowczych wymagających szczególnej ochrony, które nie mogą być przekazane pełnomocnikowi ochrony właściwemu do prowadzenia kontrolnego postępowania sprawdzającego.

Art. 34 precyzuje, że nie przeprowadza się postępowania sprawdzającego wobec osób legitymujących się ważnym poświadczeniem bezpieczeństwa do danej klauzuli, z wyjątkiem poświadczeń wydanych przez służby upoważnione do wykonywania czynności operacyjno-rozpoznawczych, prowadzące samodzielnie postępowania sprawdzające wobec swoich funkcjonariuszy (wymienione w art. 23 ust. 5 ustawy), ponieważ postępowania sprawdzające w tych służbach zostały wyłączone spod kontroli prawidłowości postępowań sprawdzających, o której mowa w art. 12.

Do katalogu osób mających dostęp do informacji niejawnych bez postępowania sprawdzającego została dopisana osoba wybrana na urząd Prezydenta RP ze względu na szczególną pozycję takiej osoby w systemie władzy państwowej.

Postępowania sprawdzające wobec kandydatów na wysokie stanowiska państwowe będą kończyły się wydaniem poświadczenia bezpieczeństwa, a nie opinii, ponieważ niejednokrotnie zdarzało się, że osoby, które uzyskały pozytywną opinię, ale nie zostały powołane na stanowisko, po upływie krótkiego czasu musiały ponownie poddawać się postępowaniu sprawdzającemu w celu uzyskania poświadczenia bezpieczeństwa.

Rozdział 6 – „Postępowanie odwoławcze i skargowe, wznowienie postępowania" określa tryb odwoływania się od decyzji o odmowie lub cofnięciu poświadczenia

bezpieczeństwa oraz składania skarg do sądu administracyjnego na decyzję organu odwoławczego, wprowadza także możliwość wznowienia zakończonego ostateczną decyzją postępowania sprawdzającego lub kontrolnego.

Art. 35 precyzuje, że odwołanie do Prezesa Rady Ministrów od decyzji o odmowie lub cofnięciu poświadczenia bezpieczeństwa przysługuje nie tylko osobom, wobec których postępowanie było prowadzone przez ABW lub SKW, ale także w przypadku postępowań prowadzonych przez służby uprawnione do samodzielnego prowadzenia poszerzonych postępowań sprawdzających.

Art. 36 jednoznacznie określa, jakie decyzje lub postanowienia mogą zostać wydane przez organ odwoławczy, określa także składniki tych decyzji i postanowień.

Art. 39 – 41 przewidują możliwość wznowienia postępowania, jeżeli decyzja o odmowie lub cofnięciu poświadczenia została wydana w związku z postępowaniem karnym lub wyrokiem skazującym, a postępowanie karne zostało następnie umorzone lub zakończone uniewinnieniem. Jest to nowe rozwiązanie na gruncie ustawy.

Rozdział 7 – „Kancelarie tajne. Środki bezpieczeństwa fizycznego" określa zasady organizacji kancelarii tajnych i środki bezpieczeństwa fizycznego, do wdrożenia których są zobowiązane jednostki organizacyjne przetwarzające informacje niejawne. Proponowane zmiany mają na celu przede wszystkim wprowadzenie zasad racjonalnego stosowania metod i środków służących ochronie informacji niejawnych oraz adekwatności rozwiązań dla określonych klauzul tajności. W tym celu zostaje wprowadzony obowiązek ustalenia przez kierowników jednostek organizacyjnych poziomu zagrożenia ujawnienia informacji niejawnych i szacowania ryzyka. Zmiany zmierzają w kierunku złagodzenia wymagań dla podmiotów dysponujących wyłącznie informacjami o niskich klauzulach tajności (tj. „zastrzeżone lub „poufne") – pozostawiając wysokie wymagania przy zabezpieczaniu informacji oznaczonych klauzulą „ściśle tajne" lub „tajne".

Art. 42 stwierdza, że obowiązek organizacji kancelarii tajnej będą miały jedynie jednostki organizacyjne dysponujące informacjami oznaczonymi klauzulami „ściśle tajne" lub „tajne". Zasady obiegu informacji niejawnych oznaczonych klauzulą „poufne" będzie określał kierownik jednostki organizacyjnej.

W uzasadnionych przypadkach będzie można zorganizować kancelarię tajną obsługującą dwie lub więcej jednostek organizacyjnych. Warunkiem funkcjonowania takiej kancelarii będzie porozumienie kierowników jednostek w zakresie podległości i finansowania oraz uzyskanie zgody ABW lub SKW. Zgoda ta będzie elementem decydującym – pozwoli na ocenę zgodności zastosowanych rozwiązań z przepisami o ochronie informacji niejawnych. Możliwość obsługiwania wielu podmiotów przez jedną kancelarię tajną wychodzi naprzeciw postulatom jednostek, które z przyczyn obiektywnych nie mogły zorganizować takiej kancelarii lub jej organizacja wiązała się z poniesieniem wysokich nakładów finansowych. Takie rozwiązanie postulowane było również przez podmioty, które dysponowały niewielką liczbą dokumentów niejawnych.

Wprowadzono obowiązek informowania odpowiednio ABW lub SKW o utworzeniu lub likwidacji kancelarii tajnej z określeniem klauzuli tajności informacji będących w dyspozycji jednostki organizacyjnej. Obowiązek ten będzie spoczywał na kierowniku jednostki organizacyjnej. Wprowadzenie takiego wymogu umożliwi ABW i SKW sprawowanie pełnego nadzoru nad bezpieczeństwem informacji o najwyższych klauzulach tajności. Wykaz jednostek organizacyjnych, które zorganizowały kancelarie tajne, będzie dostępny dla wszystkich zainteresowanych podmiotów. Rozwiązanie powinno wyeliminować przypadki przekazywania dokumentów niejawnych do jednostek nieprzygotowanych na przyjmowanie takich dokumentów.

Art. 43 i 45 wprowadzają obowiązek określenia poziomu zagrożeń nieuprawnionego dostępu do informacji niejawnych oraz stosowania środków ochrony fizycznej odpowiednich do tego poziomu (szczegółowe rozwiązania zostaną przedstawione w rozporządzeniu Rady Ministrów). Zobowiązano kierownika jednostki organizacyjnej do zatwierdzenia dokumentacji określającej poziom zagrożeń.

Art. 44 przewiduje możliwość tworzenia w jednostkach organizacyjnych znajdujących się w zakresie działania najważniejszych organów administracji państwowej innych niż kancelarie tajne komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych. Do tej pory takie rozwiązanie było możliwe wyłącznie w sferze wojskowej, a rozszerzenie działania tego przepisu jest realizacją postulatów MSZ, Policji, Straży Granicznej i innych instytucji. Przepis ten będzie w szczególności miał zastosowanie w odniesieniu do placówek MSZ za granicą oraz do terenowych komórek organizacyjnych Policji i Straży Granicznej. Kierownicy tych komórek będą mogli

wykonywać obowiązki pełnomocników ochrony w zakresie zapewnienia bezpieczeństwa fizycznego informacji niejawnych oraz ochrony systemów teleinformatycznych, jak również inne zadania pełnomocnika ochrony, których realizacja przez kierownika może w istotny sposób usprawnić funkcjonowanie systemu przetwarzania i ochrony informacji niejawnych w danej komórce, jak np. realizacja okresowej kontroli ewidencji, materiałów i obiegu dokumentów. Jedynym wyjątkiem będzie prowadzenie postępowań sprawdzających, które pozostanie w wyłącznej kompetencji pełnomocników ochrony.

Rozdział 8 – „Bezpieczeństwo teleinformatyczne" określa zasady ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych.

Art. 48 wprowadza nową zasadę polegającą na tym, że akredytacji bezpieczeństwa teleinformatycznego dla systemów przetwarzających informacje oznaczone klauzulą „zastrzeżone" będzie udzielał kierownik jednostki organizacyjnej, w której będzie funkcjonował system lub - w przypadku systemu obsługującego wiele podmiotów – kierownik jednostki organizującej system. Obowiązkiem kierownika jednostki organizacyjnej, który udzielił akredytacji dla systemu przetwarzającego informacje oznaczone klauzulą „zastrzeżone", będzie przekazanie ABW lub SKW – zgodnie z kompetencją – dokumentacji bezpieczeństwa teleinformatycznego akredytowanego systemu. ABW lub SKW w przypadku systemów teleinformatycznych przetwarzających informacje o klauzuli „zastrzeżone" mogą zlecić przeprowadzenie dodatkowych czynności zwiększających bezpieczeństwo systemu. Kierownik jednostki organizacyjnej zobowiązany jest w ciągu 30 dni poinformować ABW lub SKW o realizacji zaleceń. Jednocześnie ABW lub SKW, w szczególnie uzasadnionych przypadkach, może nakazać wstrzymanie przetwarzania informacji niejawnych w systemach akredytowanych przez kierownika jednostki organizacyjnej. Ma to na celu niedopuszczenie do sytuacji, gdy kierownik jednostki organizacyjnej akredytuje systemy niespełniające podstawowych zasad bezpieczeństwa teleinformatycznego lub systemy istotne dla funkcjonowania państwa, których zabezpieczenie nie będzie odpowiadało wymaganym standardom.

Natomiast systemy teleinformatyczne przetwarzające informacje niejawne o klauzuli „poufne" lub wyższej będą akredytowane przez ABW lub SKW zgodnie z ich właściwością. Wprowadzono instytucję świadectwa akredytacji bezpieczeństwa

teleinformatycznego, które jest potwierdzeniem udzielenia przez ABW lub SKW akredytacji dla systemu przetwarzającego informacje niejawne o klauzuli „poufne" lub wyższej oraz określa warunki ważności świadectwa i zasady przeprowadzenia audytów związanych z nadzorem nad systemem teleinformatycznym. Pojęcie świadectwa akredytacji zastąpi dotychczasowy certyfikat akredytacji. Powyższa zmiana ma na celu zwiększenie czytelności przepisów rozdziału 8 i pozostawienie pojęcia „certyfikat" tylko dla urządzeń i narzędzi kryptograficznych, środków ochrony elektromagnetycznej oraz urządzeń lub narzędzi realizujących zabezpieczenia teleinformatyczne.

Warunkami, jakie muszą być spełnione dla wydania świadectwa bezpieczeństwa teleinformatycznego są: dokonanie pozytywnej oceny dokumentacji bezpieczeństwa teleinformatycznego oraz pozytywny wynik audytu bezpieczeństwa teleinformatycznego. W przypadku systemów przetwarzających informacje o klauzuli „poufne" ABW lub SKW może odstąpić od przeprowadzenia audytu bezpieczeństwa i akredytować system na podstawie przekazanej dokumentacji bezpieczeństwa.

Wprowadzono termin 6 miesięcy na udzielenie bądź odmowę udzielenia akredytacji, w szczególnych przypadkach wynikających z rozległości i stopnia skomplikowania systemu będzie on mógł być wydłużony o maksymalnie 6 miesięcy.

W art. 49 wskazano, że najistotniejszym elementem dokumentu szczególnych wymagań bezpieczeństwa jest ocena ryzyka dla bezpieczeństwa informacji niejawnych oraz zarządzanie tymże ryzykiem. Przeprowadzenie szacowania ryzyka jest podstawowym działaniem, jakie należy przeprowadzić przed przystąpieniem do sporządzenia dokumentacji bezpieczeństwa oraz jest procesem, który powinien być stale prowadzony przez podmioty dysponujące systemami służącymi do przetwarzania informacji niejawnych. W przypadku gdy może się to okazać korzystne dla całego systemu ochrony informacji niejawnych, przebieg i wyniki szacowania ryzyka mogą być sporządzone w odrębnym dokumencie.

Art. 50 określa zasadę, że urządzenia i narzędzia kryptograficzne przeznaczone do ochrony informacji niejawnych podlegają procesowi certyfikacji prowadzonej przez ABW lub SKW. W porównaniu z poprzednim brzmieniem ustawy zaproponowano, aby certyfikacji podlegały urządzenia i narzędzia kryptograficzne służące do ochrony informacji niejawnych od klauzuli „zastrzeżone". W poprzedniej wersji ustawy obowiązek ten dotyczył urządzeń i narzędzi kryptograficznych służących do ochrony

informacji niejawnych od klauzuli „poufne". Zmiana ta ma na celu – między innymi – umożliwienie polskim wytwórcom narzędzi i urządzeń kryptograficznych uzyskiwania certyfikatów, które umożliwią stosowanie tych urządzeń w ramach NATO i UE. Wprowadzono także zasadę certyfikowania środków ochrony elektromagnetycznej przeznaczonych dla informacji niejawnych o klauzuli „poufne" lub wyższej. Jest to unormowanie aktualnego stanu faktycznego, polegające na tym, że środki ochrony elektromagnetycznej, zgodnie z polityką bezpieczeństwa NATO i UE, podlegają certyfikacji.

Certyfikacja środków ochrony elektromagnetycznej oraz urządzeń i narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych prowadzona będzie przez ABW lub SKW z pominięciem właściwości obu służb określonej w art. 10 ustawy, gdyż nie jest możliwe określenie z góry, w jednostkach organizacyjnych której sfery takie środki, narzędzia i urządzenia będą wykorzystane, a jest prawdopodobne, że będą one mogły być wykorzystywane w obu sferach. Wprowadzenie w tym zakresie kryterium przynależności producenta do określonej sfery przyznałoby w praktyce monopol na takie procesy certyfikacji dla ABW, co nie wydaje się działaniem racjonalnym.

Art. 51 wyłącza z obowiązku akredytacji bezpieczeństwa teleinformatycznego systemy teleinformatyczne, których istotą jest to, że służą wyłącznie do pozyskiwania i przekazywania w sposób niejawny informacji uzyskanych w trakcie czynności operacyjno-rozpoznawczych przez uprawnione do tego podmioty. Przepis ten obejmuje swoim zakresem tego typu systemy teleinformatyczne, które używane są w sposób niejawny przez uprawnione do tego podmioty, realizujące czynności operacyjno-rozpoznawcze. Powyższe systemy teleinformatyczne i środki techniczne funkcjonują w takim środowisku i w taki sposób, że niemożliwe jest zastosowanie wobec nich wymogów związanych z bezpieczeństwem teleinformatycznym. Powyższy wyjątek dotyczy systemów teleinformatycznych, które nie są zlokalizowane w budynkach należących do podmiotów realizujących czynności operacyjno-rozpoznawcze i ograniczony jest jedynie do pozyskiwania i przekazywania informacji, co nie wyczerpuje ustawowej definicji przetwarzania.

Z akredytacji wyłączono też systemy teleinformatyczne wykorzystywane przez służby wywiadowcze poza granicami RP podczas wykonywania czynności

operacyjno-rozpoznawczych oraz wydzielone stanowiska na terytorium RP służące służbom wywiadowczym do odbierania i przetwarzania tych informacji.

Rozdział 9 – Bezpieczeństwo przemysłowe określa zasady ochrony informacji niejawnych przekazywanych przedsiębiorcom podczas wykonywania umów albo zadań wynikających z przepisów prawa.

Art. 54 stwierdza, że świadectwo bezpieczeństwa przemysłowego potwierdza zdolność przedsiębiorcy do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej. Jest to rozwiązanie stosowane powszechnie w krajach NATO i Unii Europejskiej. Wprowadzenie świadectw bezpieczeństwa przemysłowego do poziomu „poufne" ma też bezpośredni związek ze zmianą definicji klauzul tajności. Skoro informacje „poufne" będą mogły się odnosić tylko do bezpieczeństwa i interesów państwa, powinny być chronione na takich zasadach, jak obecna tajemnica państwowa.

W przypadku przedsiębiorców wykonujących działalność osobiście zniesiono obowiązek uzyskiwania świadectw bezpieczeństwa przemysłowego i większość rygorów z tym związanych. W takim przypadku dokumentem potwierdzającym rękojmię zachowania tajemnicy przez przedsiębiorcę będzie poświadczenie bezpieczeństwa.

Uregulowano możliwość tymczasowego i jednorazowego dostępu przedsiębiorcy do informacji niejawnych analogicznie, jak to ma miejsce w przypadku bezpieczeństwa osobowego.

Art. 60 zwalnia przedsiębiorców ubiegających się o świadectwo bezpieczeństwa przemysłowego trzeciego stopnia z kosztownego obowiązku tworzenia pionu ochrony. W takim przypadku obowiązek przeszkolenia pracowników przedsiębiorcy w zakresie ochrony informacji niejawnych będzie spoczywał na pełnomocniku ochrony jednostki zamawiającej.

Art. 64 określa przesłanki odmowy, a art. 66 przesłanki cofnięcia świadectwa bezpieczeństwa przemysłowego. Jest to istotna zmiana w stosunku do stanu obecnego, w którym nie ma precyzyjnych uregulowań tej kwestii.

Art. 65 przewiduje możliwość przeprowadzenia z urzędu wybranych sprawdzeń przedsiębiorcy w celu ustalenia, czy nie utracił on zdolności ochrony informacji niejawnych. Uregulowano też zasady współpracy ABW i SKW przy okazji takich

sprawdzeń albo podczas kontroli zabezpieczenia informacji niejawnych, jeżeli przedsiębiorca ma świadectwo bezpieczeństwa przemysłowego wydane przez jedną z tych służb, a umowę realizuje na rzecz jednostki organizacyjnej znajdującej się w zakresie kompetencji drugiej służby.

Rozdział 10 – „Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego" porządkuje ten obszar poprzez umieszczenie w jednej jednostce redakcyjnej zasad postępowania z aktami postępowania sprawdzającego i postępowania przemysłowego.

Art. 72 precyzyjnie wskazuje przypadki, w których można udostępnić akta postępowania sprawdzającego, stwierdzając jednoznacznie, że – oprócz wprost wskazanych w ustawie przypadków – akta postępowania sprawdzającego mogą być udostępnione wyłącznie dla celów postępowania sprawdzającego wobec tej samej osoby. Wyklucza to wykorzystywanie akt postępowań sprawdzających w polityce kadrowej, postępowaniach dyscyplinarnych lub jakichkolwiek innych tego rodzaju sytuacjach.

Rozdział 11 – „Zmiany w przepisach obowiązujących" przewiduje możliwość finansowania wydatków bieżących i inwestycyjnych ABW lub SKW z opłat za przeprowadzenie certyfikacji urządzeń kryptograficznych lub środków ochrony elektromagnetycznej. Ponadto dokonano przeglądu obowiązującego ustawodawstwa, eliminując użycie pojęcia „służby ochrony państwa" – zastępując je sformułowaniem „ABW lub SKW" oraz pojęć „tajemnica państwowa" i „tajemnica służbowa" – zastępując je określeniami poszczególnych klauzul albo terminem „informacje niejawne". Usunięto również przepisy przewidujące nadawanie określonym dokumentom klauzul tajności bez związku z przesłankami określonymi w art. 5 ustawy, ale w przypadku szczególnie wrażliwych informacji przekazywanych przez obywateli organom państwa, takich jak oświadczenia majątkowe lub tajemnica skarbowa, wprowadzono obowiązek ich ochrony na poziomie przewidzianym dla ochrony informacji niejawnych o klauzuli „zastrzeżone". W przypadku przepisów określających dostęp dotychczasowych służb ochrony państwa do określonych informacji niezbędnych do prowadzenia postępowań sprawdzających, rozszerzono ten dostęp na wszystkie służby prowadzące rozszerzone postępowania sprawdzające, aby zapewnić równorzędny standard tych postępowań.

I tak na przykład w ustawie – Ordynacja podatkowa w art. 13a i art. 179 § 1 termin „tajemnica państwowa" został zastąpiony przez „informacje niejawne", w art. 82 § 4 dotyczącym sposobu ochrony dokumentów oznaczonych jako „tajemnica skarbowa" termin „tajemnica służbowa" zastępuje się pojęciem „informacje niejawne o klauzuli <zastrzeżone>", w art. 195 pkt 2, 196 § 4 oraz 286 § 3 zamiast „tajemnica państwowa lub służbowa" wprowadza się „informacje niejawne", a w art. 298 pkt 5a pojęcie „służby ochrony państwa" zastępuje się przez „ABW lub SKW", a ponadto uzupełnia się ten przepis o SWW, CBA i BOR, gdyż nie ma żadnego uzasadnienia sytuacja, w której służby pozbawione są dostępu do informacji posiadanych przez ABW, SKW, AW, Policję, Żandarmerię Wojskową, Straż Graniczną i Służbę Więzienną.

Rozdział 12 – „Przepisy przejściowe i końcowe" nakazuje przeprowadzenie w ciągu trzech lat przeglądu wszystkich materiałów wytworzonych pod rządami starej ustawy pod kątem ewentualnej zmiany lub zniesienia klauzuli tajności.

Wszystkie poświadczenia, zaświadczenia i świadectwa wydane pod rządami starej ustawy zachowają ważność na okres w nich wskazany. Dotyczy to również poświadczeń dla kierowników jednostek organizacyjnych wydanych przez pełnomocników ochrony, poświadczeń dla pełnomocników ochrony wydanych przez ABW lub SKW po przeprowadzeniu zwykłych, a nie poszerzonych postępowań sprawdzających oraz poświadczeń, zaświadczeń i świadectw wydanych przez ABW lub SKW niezależnie od właściwości ABW i SKW określonej w art. 10 ustawy. Wyjątkiem są akredytacje systemów teleinformatycznych, które zachowują ważność do czasu dokonania w nich istotnych zmian, jednak nie dłużej niż przez 5 lat.

Do postępowań wszczętych przed wejściem w życie nowej ustawy będą miały zastosowanie dotychczasowe przepisy.

Ankieta Bezpieczeństwa Osobowego jest załącznikiem do ustawy. W treści ankiety odstąpiono od niektórych pytań uznając, że odpowiedź na nie nie ma istotnego znaczenia dla oceny dawania rękojmi zachowania tajemnicy przez osobę sprawdzaną, natomiast w przypadku innych pytań doprecyzowano ich treść lub wprowadzono nowe pytania, co wynikło z praktycznych doświadczeń postępowań sprawdzających. Odstąpiono od obowiązkowego oznaczania ankiety klauzulą tajności, ponieważ zawarte w niej informacje zazwyczaj nie będą spełniać ustawowych przesłanek nadania klauzuli określonych w art. 5. Ze względu jednak na bardzo wrażliwy charakter niektórych

informacji przekazywanych w ankiecie przyjęto, że ankiety wypełnione do postępowań zwykłych będą chronione według zasad określonych w ustawie dla informacji o klauzuli „zastrzeżone", a do postępowań poszerzonych – „poufne". Jeżeli natomiast w treści ankiety znajdą się informacje spełniające kryteria nadania jej klauzuli tajności (np. w przypadku ankiet wypełnianych przez funkcjonariuszy służb wywiadowczych), taka klauzula oczywiście będzie mogła być nadana odpowiednio do treści ankiety.

Przewidywane skutki uchwalenia projektowanej ustawy można jedynie oszacować poprzez odniesienie do skutków powodowanych przez aktualnie obowiązującą ustawę o ochronie informacji niejawnych. W tym kontekście należy oczekiwać, że koszty funkcjonowania projektowanego systemu ochrony informacji nie będą wyższe niż aktualnie ponoszone przez podmioty zobowiązane do stosowania przepisów ustawy o ochronie informacji niejawnych. W niektórych zaś przypadkach należy oczekiwać obniżenia tych kosztów (dotyczyć to będzie przypadków zmiany unormowań co do bezpieczeństwa fizycznego oraz zarządzania ryzykiem w miejsce określania wymogów minimalnych standardów ochrony np. w sferze bezpieczeństwa teleinformatycznego, a także wynikać ze zmian zakresów definicji poszczególnych klauzul tajności).

Podstawowe znaczenie dla wykonywania przepisów projektowanej ustawy o ochronie informacji niejawnych będą mieć następujące akty prawne:

– rozporządzenie Prezesa Rady Ministrów wydane na podstawie art. 11 ust. 6 ustawy, które określi sposób współdziałania Szefa ABW i Szefa SKW w zakresie wykonywania przez Szefa ABW funkcji krajowej władzy bezpieczeństwa, w tym kwestię nadzoru nad systemem ochrony informacji niejawnych wymienianych z innymi państwami oraz konieczność zapewnienia jednolitości stosowania procedur związanych z wykonywaniem zadań krajowej władzy bezpieczeństwa w sferze cywilnej i wojskowej.

– rozporządzenie Prezesa Rady Ministrów wynikające z art. 12 ust. 6 projektu ustawy; ten akt wykonawczy normować będzie sposób przygotowania i tryb przeprowadzania kontroli w zakresie ochrony informacji niejawnych. Istotną kwestią w jego treści będzie określenie uzgadniania tej kontroli w stosunku do Kancelarii Sejmu, Senatu i Prezydenta Rzeczypospolitej Polskiej. W rozporządzeniu tym uwzględnione zostaną zadania funkcjonariuszy ABW oraz żołnierzy i funkcjonariuszy SKW nadzorujących i wykonujących czynności

kontrolne, a także dokumentowanie czynności kontrolnych oraz sporządzanie: protokołu kontroli, wystąpienia pokontrolnego i informacji o wynikach kontroli. Rozporządzenie to będzie zatem normować sposób i tryb ingerencji kontrolnej ABW i SKW wobec innych podmiotów ustawy, artykułując z jednej strony funkcję gwarancyjną – czyli przestrzeganie przez organy kontrolne granic uprawnień, zaś ze strony drugiej – artykułować będzie funkcję egzekucyjną – czyli stanowić będzie narzędzie wykonywania ustawą przyznanych kompetencji do kontroli ochrony informacji niejawnych realizowanej przez podmioty ustawą do ich ochrony zobowiązane.

– rozporządzenie Rady Ministrów wynikające z art. 47 ust. 1 projektu ustawy; jego zakres normatywny wynikać będzie z kwestii nowego podejścia do pragmatyki bezpieczeństwa fizycznego, a mianowicie – w miejsce dotychczasowego przestrzegania formalnych wymogów minimalnych – wprowadzone zostaje zracjonalizowane i indywidualne określanie rzeczywistych poziomów zagrożeń dla ochrony informacji niejawnych. Projektowane rozporządzenie precyzować będzie procedurę i podstawowe kryteria określania poziomu zagrożeń oraz normować dobór środków bezpieczeństwa fizycznego właściwych do wskazanego poziomu zagrożeń, a także wymagania w zakresie organizacji i funkcjonowania kancelarii tajnych. Ponadto – stosownie do projektowanych zmian ustawowych – przepisy wykonawcze zmierzać będą w kierunku złagodzenia wymagań dla podmiotów dysponujących wyłącznie informacjami o niskich klauzulach tajności (tj. „zastrzeżone” lub „poufne”) – pozostawiając adekwatnie wyższe wymagania przy zabezpieczaniu informacji oznaczonych klauzulą „tajne” lub „ściśle tajne”. W rozporządzeniu, o którym mowa, uwzględnione zostaną ponadto m. in. następujące kwestie:

  1) rodzaje zagrożeń, które należy uwzględnić w określaniu poziomu zagrożeń;
  2) adekwatne do nich środki ochrony fizycznej;
  3) podstawowe elementy planu ochrony;
  4) kryteria tworzenia stref ochronnych;
  5) strukturę organizacyjną kancelarii oraz podstawowe zadania jej kierownika;
  6) tryb obiegu informacji niejawnych.

– rozporządzenie Prezesa Rady Ministrów wynikające z art. 49 ust. 11 projektu ustawy; zakres normatywny tego rozporządzenia będzie obejmował problematykę bezpieczeństwa teleinformatycznego w sposób odmienny niż dotychczasowe przepisy prawa. Podstawowe założenie ustawowe w tej materii, tzn. wprowadzenie zarządzania ryzykiem – także w dziedzinie bezpieczeństwa teleinformatycznego – spowoduje, że przepisy wykonawcze normować będą tę problematykę poprzez pryzmat określenia należytych procedur i środków. Powinny one w sposób elastyczny, ale bez uszczerbku dla bezpieczeństwa przetwarzanych w systemach teleinformatycznych informacji niejawnych, spełniać adekwatne do poziomu rozwoju technologicznego i przyjęte obecnie na świecie standardy wymagań bezpieczeństwa teleinformatycznego. Ponadto wskazany w tym rozporządzeniu sposób opracowywania dokumentacji bezpieczeństwa systemów teleinformatycznych uwzględniać będzie zmienioną metodykę postępowania podmiotów odpowiedzialnych oraz podmiotów właściwych do badań, certyfikacji lub akredytacji.

Przedmiot projektowanej regulacji nie jest objęty prawem Unii Europejskiej.

OCENA SKUTKÓW REGULACJI

Celem regulacji jest wprowadzenie kompleksowych, spójnych i konsekwentnych oraz łatwych do stosowania w praktyce regulacji dotyczących ochrony informacji niejawnych. Wydanie przepisów zmieniających dotychczasowy stan prawny wynika z konieczności:

1) wprowadzenia mechanizmów efektywnościowych do systemu ochrony informacji niejawnych, w tym zarządzania ryzykiem,
2) unowocześnienia i dostosowania systemu ochrony informacji niejawnych do warunków nowoczesnych technologii,
3) dostosowania regulacji do zmieniających się standardów w NATO i Unii Europejskiej, określonych w przepisach regulujących postępowanie z informacjami niejawnymi wymienianymi w ramach współpracy z NATO i UE, a także do analogicznych zasad obowiązujących w wewnętrznych przepisach innych krajów członkowskich (nie istnieją natomiast przepisy UE harmonizujące ochronę informacji niejawnych w poszczególnych krajach, gdyż ta sfera pozostaje w wyłącznej kompetencji suwerennych państw),
4) usunięcia luk, niejasności i niespójności systemowych oraz uproszczenie obowiązującego prawa.

Konieczność opracowania nowego aktu prawnego wynika przede wszystkim z potrzeb praktyki, ponieważ stosowanie obowiązującej ustawy sprawia trudności, w tym rodzi wątpliwości interpretacyjne, oraz z potrzeby poprawy efektywności systemu ochrony informacji niejawnych.

Pozostawienie w dotychczasowym kształcie przepisów regulujących ochronę informacji niejawnych powodowałoby następujące skutki:

1) zwiększałoby prawdopodobieństwo wystąpienia ryzyka i zagrożeń wynikających z niedostosowania aktualnych rozwiązań, w szczególności w zakresie bezpieczeństwa teleinformatycznego i fizycznego, do warunków nowoczesnych technologii (ICT),

2) utrzymywałoby regulacje i praktyki niedostosowane do standardów obowiązujących w instytucjach unijnych i państwach członkowskich, co w konsekwencji utrudniłoby realizację zadań związanych z objęciem i sprawowaniem przez Polskę przewodnictwa w Radzie Unii Europejskiej,

3) uniemożliwiłoby budowanie sprawnego systemu ochrony informacji niejawnych, szczelnie chroniącego informacje najważniejsze dla bezpieczeństwa i ochrony interesów państwa, a jednocześnie efektywnego i ekonomicznego oraz prostego w stosowaniu.

Alternatywne rozwiązanie, polegające na kolejnej nowelizacji obowiązującego prawa, nie usunęłoby problemów wynikających z kompilacyjnego charakteru obowiązującej ustawy.

Powyższe argumenty, uwzględniające zarówno skutki pozostawienia status quo, jak również słabości alternatywnego rozwiązania, polegającego na nowelizacji obowiązującej ustawy, przemawiają za koniecznością uchwalenia nowej ustawy o ochronie informacji niejawnych.

1. Podmioty, na które oddziałuje regulacja:

   1) Szef Agencji Bezpieczeństwa Wewnętrznego,

   2) Szef Służby Kontrwywiadu Wojskowego,

   3) organy władzy publicznej,

   4) Siły Zbrojne RP i ich jednostki organizacyjne, jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane,

   5) Narodowy Bank Polski,

   6) państwowe osoby prawne i państwowe jednostki organizacyjne,

   7) przedsiębiorcy, zamierzający ubiegać się lub ubiegający się o zawarcie lub wykonujących umowy związane z dostępem do informacji niejawnych,

   8) kierownicy jednostek organizacyjnych, w których przetwarzane są informacje niejawne,

   9) pełnomocnicy ochrony informacji niejawnych.

2. Konsultacje społeczne:

   W ramach konsultacji projekt został udostępniony w Biuletynie Informacji Publicznej oraz przekazany następującym podmiotom:

   1) Związkowi Banków Polskich,

   2) stowarzyszeniom dziennikarzy,

   3) organizacjom pozarządowym działającym w obszarze praw obywatelskich i wolności słowa, np. Helsińska Fundacja Praw Człowieka,

   4) stowarzyszeniom pełnomocników ochrony informacji niejawnych,

   5) stowarzyszeniom i organizacjom funkcjonującym w obszarze bezpieczeństwa teleinformatycznego oraz wytwarzania dóbr i usług związanych z ochroną informacji niejawnych,

   6) organizacjom przedsiębiorców, np. Business Center Club, Polskiej Konfederacji Pracodawców Prywatnych „Lewiatan", Konfederacji Pracodawców Polskich.

   Organizacje te zgłosiły ok. 300 uwag, które w dużej części zostały uwzględnione. W wyniku uwzględnienia tych uwag przewidziano obowiązek ochrony wypełnionych ankiet bezpieczeństwa analogicznie do ochrony informacji niejawnych, jak również w przepisach zmieniających przepisy innych ustaw nałożono obowiązek ochrony składanych przez obywateli oświadczeń majątkowych na zasadach analogicznych do ochrony informacji niejawnych o klauzuli „poufne", sprecyzowano definicje takich pojęć jak „rękojmia zachowania tajemnicy", „system teleinformatyczny" i „przetwarzanie informacji niejawnych", wprowadzono obowiązkowe przeglądy wytworzonych informacji niejawnych pod kątem możliwości obniżenia lub zniesienia klauzul tajności tych informacji, sprecyzowano i znacząco zawężono możliwość kontrolowania przez ABW lub SKW systemów teleinformatycznych służących do przetwarzania informacji jawnych, wprowadzono wymóg posiadania wyższego wykształcenia przez kandydatów na pełnomocników ochrony, odstąpiono od wymogu posiadania przez administratorów i inspektorów bezpieczeństwa teleinformatycznego poświadczeń upoważniających do dostępu do informacji niejawnych o klauzuli wyższej niż przetwarzane w systemie.

Projekt ustawy przekazano także do zaopiniowania organom państwowym, na których działanie ustawa będzie miała bezpośredni wpływ, a które nie ubiorą udziału w uzgodnieniach międzyresortowych, w tym:

1) Szefom Kancelarii Sejmu, Senatu i Prezydenta,
2) Pierwszemu Prezesowi Sądu Najwyższego,
3) Generalnemu Inspektorowi Ochrony Danych Osobowych,
4) Prezesowi Narodowego Banku Polskiego,
5) Prezesowi Najwyższej Izby Kontroli,
6) Przewodniczącemu Komisji Nadzoru Finansowego,
7) Szefowi Biura Bezpieczeństwa Narodowego.

Spośród ponad 80 uwag zgłoszonych przez te organy przeszło połowa została uwzględniona. W wyniku uwzględnienia tych uwag istotnie rozszerzono zakres stosowania kodeksu postępowania administracyjnego, wprowadzono możliwość wznowienia postępowania, wprowadzono termin zawity do kontrolnych postępowań sprawdzających, przewidziano obowiązek uzgadniania kontroli ochrony informacji niejawnych w Kancelarii Prezydenta analogicznie do rozwiązań obowiązujących w przypadku Kancelarii Sejmu i Senatu, zobowiązano ABW do szkolenia posłów i senatorów w zakresie ochrony informacji niejawnych, przewidziano obligatoryjne wydanie rozporządzenia regulującego współpracę Szefów ABW i SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa, ograniczono możliwość zobowiązania osoby sprawdzanej do poddania się specjalistycznym badaniom lekarskim do poszerzonego postępowania sprawdzającego, wprowadzono tryb zażalenia na postanowienie o zawieszeniu postępowania sprawdzającego, wprowadzono przepis nakładający obowiązek określenia w jednostkach organizacyjnych zasad obiegu i ochrony informacji niejawnych o klauzuli „zastrzeżone".

Sekretarz Komitetu Integracji Europejskiej zgłosił zastrzeżenie dotyczące propozycji przepisów uzależniających dopuszczenie do stosowania w systemach teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych urządzeń lub narzędzi kryptograficznych certyfikowanych przez organy Unii Europejskiej lub krajowe władze bezpieczeństwa krajów UE od akceptacji Szefa

ABW lub Szefa SKW. Zastrzeżenie wiązało się ze wskazaniem przez Sekretarza KIE możliwości kolizji tych przepisów z regulacjami Unii Europejskiej zakazującymi wprowadzania ograniczeń przywozowych i ograniczeń we wprowadzaniu do obrotu towarów, które uzyskały odpowiedni certyfikat zgodności w innym państwie członkowskim.

W toku prac legislacyjnych przepisy te zostały częściowo usunięte z projektu, pozostał jedynie ustęp przewidujący taką możliwość w przypadku urządzeń lub narzędzi kryptograficznych stosowanych w systemach teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone".

Należy wyjaśnić, że proponowany przepis nie zakazuje przywozu do Polski ani wprowadzania do obrotu w Polsce jakichkolwiek urządzeń lub narzędzi kryptograficznych, więc oczywiście nie zakazuje również przywozu ani wprowadzania do obrotu takich urządzeń lub narzędzi, które uzyskały certyfikaty w innych krajach Unii Europejskiej. Nie wprowadza więc żadnego ograniczenia w swobodnym przepływie towarów między krajami członkowskimi. Przepis określa jedynie możliwość i warunki uznania w Polsce, dla ochrony polskich informacji niejawnych, wydanego w innym kraju Unii Europejskiej certyfikatu stwierdzającego zdolność produktu do ochrony informacji dotyczących bezpieczeństwa tego kraju. Warto podkreślić, że kwestia ochrony informacji niejawnych w poszczególnych krajach członkowskich nie jest w żaden sposób regulowana przez prawo unijne i pozostaje w wyłącznym zakresie kompetencji suwerennych państw.

Komisja Wspólna Rządu i Samorządu Terytorialnego przyjęła stanowisko w dniu 26 sierpnia 2009 r., w którym nie zgłosiła zastrzeżeń do treści projektu ustawy.

Projekt ustawy o ochronie informacji niejawnych został udostępniony w Biuletynie Informacji Publicznej z chwilą przekazania tego projektu do uzgodnień z członkami Rady Ministrów.

W trybie ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414, z późn. zm.), zgłoszenie zainteresowania pracami nad projektem wniosły następujące podmioty:

1) Stowarzyszenie Dziennikarzy Polskich z siedzibą ul. Foksal 3/5, 00-366 Warszawa,

2) Centrum im. Adama Smitha z siedzibą ul. Bednarska 16, 00-321 Warszawa,

3) Fundacja Instytut Sobieskiego z siedzibą ul. Nowy Świat 27, 00-029 Warszawa.

W trakcie prac uwagi zgłoszone przez wskazane powyżej podmioty zostały częściowo uwzględnione poprzez doprecyzowanie zapisów w dokumencie.

3. Wpływ regulacji na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego

W pierwszym okresie obowiązywania nowej ustawy koszty funkcjonowania systemu ochrony informacji niejawnych nie będą znacząco różne od dotychczasowych kosztów funkcjonowania tego systemu.

W dłuższej perspektywie można prognozować stopniową tendencję do obniżania wydatków budżetowych. Jako przyczyny należy wskazać przede wszystkim następujące projektowane elementy:

1) zmiany unormowań dotyczących bezpieczeństwa fizycznego i teleinformatycznego,

2) zmiany zakresów definicji poszczególnych klauzul tajności i związana z tym możliwość niższego „klauzulowania" informacji,

3) możliwość obiegu informacji o klauzuli „poufne" poza systemem kancelarii tajnych i, co za tym idzie, brak potrzeby tworzenia kancelarii tajnych i pionów ochrony w niektórych jednostkach organizacyjnych,

4) możliwość zorganizowania, w uzasadnionych przypadkach, kancelarii tajnej obsługującej dwie lub więcej jednostek organizacyjnych,

5) zmiany upraszczające postępowania sprawdzające i rezygnacja z postępowań sprawdzających przed uzyskaniem dostępu do informacji niejawnych o klauzuli „zastrzeżone".

Wejście w życie ustawy spowoduje wydatki oraz oszczędności dla budżetu państwa. Wydatki zostaną pokryte z budżetów jednostek organizacyjnych przetwarzających informacje niejawne.

Szacunkowy koszt wydatków rozkłada się następująco:

1) koszty prowadzenia postępowań sprawdzających przez ABW wobec kierowników jednostek organizacyjnych niezależnie od klauzuli tajności – ABW, realizując nowe obowiązki w tym zakresie, będzie musiała wyznaczyć dodatkowych funkcjonariuszy do realizacji tych zadań, uwzględniając możliwe przesunięcia ze względu na zmniejszenie liczby realizowanych postępowań sprawdzających po przejęciu przez Biuro Ochrony Rządu uprawnień do samodzielnego prowadzenia procedur,

2) koszty Biura Ochrony Rządu wynikające z przeprowadzania samodzielnego postępowania sprawdzającego wobec własnych pracowników, funkcjonariuszy oraz osób ubiegających się o przyjęcie do służby lub pracy (art. 24). Aby skutecznie prowadzić liczbę postępowań sprawdzających na dotychczasowym poziomie, należy liczyć się z koniecznością zatrudnienia 8 osób do realizacji zadań związanych z bezpieczeństwem osobowym w Biurze Pełnomocnika Ochrony BOR, co oznacza dodatkowe obciążenie dla budżetu BOR w wysokości ok. 500 tys. zł rocznie,

3) koszty przeprowadzenia przeglądu w ciągu dwóch lat wszystkich materiałów wytworzonych pod rządami starej ustawy pod kątem ewentualnej zmiany lub zniesienia klauzuli tajności są trudne do oszacowania.

4) koszty doradztwa i szkoleń ABW i SKW oraz jednostek organizacyjnych, w których przetwarzane są informacje niejawne, w tym koszty cykliczności szkoleń. W niewielkim stopniu mogą wzrosnąć koszty ABW i SKW związane z konieczności prowadzenia doradztwa w pierwszym okresie obowiązywania nowej ustawy oraz rozszerzeniem obowiązków szkoleniowych. Jednocześnie nie przewiduje się ani znaczącego zwiększenia dochodów budżetu państwa z tytułu prowadzenia przez służby szkoleń, ani znaczącego zwiększenia kosztów ponoszonych przez jednostki organizacyjne w związku z tymi szkoleniami. Z jednej strony, na ABW i SKW spadnie obowiązek przeprowadzenia dodatkowych szkoleń dla kierowników jednostek przetwarzających informacje „ściśle tajne" i „tajne" oraz nowych zastępców pełnomocnika ochrony (niektóre jednostki mogą powoływać więcej niż jednego zastępcę pełnomocnika ochrony), z drugiej strony zmniejszeniu ulegnie liczba jednostek będących podmiotami

ustawy o ochronie informacji niejawnych z uwagi na nowe definicje informacji niejawnych.

Oczekiwane oszczędności w wyniku wejścia w życie ustawy:

1) oszczędności wynikające z pełnienia funkcji krajowej władzy bezpieczeństwa przez jeden organ, niewielkie, wynikające ze zmian organizacyjnych,

2) oszczędności w jednostkach organizacyjnych nie dysponujących dostępem do informacji oznaczonych klauzulami „ściśle tajne" lub „tajne", które unikną kosztów utworzenia i funkcjonowania kancelarii tajnych. Spodziewane oszczędności tych podmiotów rocznie wyniosą od 20 do 100 tys. zł plus co najmniej jeden etat kalkulacyjny.

W długim okresie regulacja wpłynie na spadek liczby informacji prawnie chronionych. Skala tego spadku – jak również skala oszczędności z tego tytułu - jest trudna do oszacowania.

4. Wpływ regulacji na rynek pracy

Nie stwierdzono istotnego wpływu nowych rozwiązań na rynek pracy.

5. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw

W odróżnieniu od obowiązującego stanu prawnego – rozszerzona została grupa przedsiębiorców, gdyż dotychczasowe przepisy eliminowały niektóre podmioty gospodarcze, np. spółdzielnie, z możliwości ubiegania się o realizację umów związanych z dostępem do informacji niejawnych. Z drugiej strony, przewidywać można zmniejszenie liczby jednostek organizacyjnych będących podmiotami ustawy ze względu na pozostawienie poza sferą regulacji nowej ustawy o ochronie informacji niejawnych informacji dotyczących prawnie chronionych interesów obywateli i jednostek organizacyjnych, jako chronionych innymi, ustawowo unormowanymi, tajemnicami.

W przypadku przedsiębiorców realizujących umowy związane z dostępem do informacji niejawnych o klauzuli „poufne" może nastąpić pewien wzrost kosztów spowodowany koniecznością ubiegania się o świadectwo bezpieczeństwa

przemysłowego. Zmiana zakresu definicji poszczególnych klauzul powinna jednak zmarginalizować ten problem, gdyż informacje obecnie oznaczane taką klauzulą w części będą oznaczane jako „zastrzeżone" albo w ogóle nie będą klasyfikowane jako informacje niejawne. Można także przewidywać redukcję pionów ochrony i rezygnację z tworzenia kancelarii tajnych, co obniży koszty funkcjonowania przedsiębiorców przetwarzających tylko informacje niejawne o klauzulach „poufne" i „zastrzeżone".

Wprowadzenie rozwiązań:

1) dających możliwość ubiegania się o wykonywanie umów związanych z dostępem do informacji niejawnych przez przedsiębiorców wykonujących działalność osobiście wyłącznie na podstawie poświadczenia bezpieczeństwa, bez konieczności ubiegania się o świadectwo bezpieczeństwa przemysłowego,
2) brak obowiązku powoływania pionu ochrony przez przedsiębiorców ubiegających się o świadectwo bezpieczeństwa przemysłowego trzeciego stopnia,
3) możliwość tworzenia kancelarii tajnych obsługujących dwóch lub więcej przedsiębiorców (np. spółki zależne)

wpłynie na obniżenie kosztów przedsiębiorców zamierzających ubiegać się lub ubiegających się o zawarcie lub wykonujących umowy związane z dostępem do informacji niejawnych.

Z uwagi na wprowadzenie nowych rozwiązań co do zarządzania ryzykiem, wzrośnie zapotrzebowanie na usługi firm oferujących szkolenia w tym zakresie oraz oferujących oprogramowanie lub inne usługi, np. w zakresie sporządzania dokumentacji. Szacunkowo ponad 5 tys. podmiotów posiada akredytowane systemy bezpieczeństwa teleinformatycznego i część z nich będzie zainteresowana szkoleniami w zakresie zarządzania ryzykiem.

6. Wpływ regulacji na sytuację i rozwój regionów

Nie stwierdzono istotnego wpływu nowych rozwiązań na sytuację i rozwój regionów.

7. Wpływ regulacji na bezpieczeństwo państwa

Wpływ bezpośredni: Nie stwierdzono istotnego bezpośredniego wpływu regulacji na bezpieczeństwo państwa.

Wpływ pośredni: W krótszym okresie istnieje relatywnie niskie ryzyko obniżenia bezpieczeństwa niektórych informacji w wyniku zmiany zakresu definicji poszczególnych klauzul oraz obniżenia wymogów dotyczących ochrony informacji o niskich klauzulach, np. zniesienia obowiązku prowadzenia postępowań sprawdzających wobec osób, które mają uzyskać dostęp do informacji niejawnych o klauzuli „zastrzeżone". Istnieje także ryzyko obniżenia bezpieczeństwa informacji dotyczących prawnie chronionych interesów obywateli i jednostek organizacyjnych, które przestaną być chronione na podstawie ustawy o ochronie informacji niejawnych.

W dłuższym okresie zwiększenie efektywności systemu ochrony informacji niejawnych, poprzez koncentrację środków na ochronie informacji najważniejszych z punktu widzenia bezpieczeństwa i interesów państwa, wpłynie pozytywnie na bezpieczeństwo państwa.

8. Wpływ na jakość demokracji. Dostęp do informacji publicznej

Regulacja wyznacza granicę między dostępem do informacji publicznej a nakazem ochrony informacji i obowiązkiem zachowania tajemnicy. Granica ta, w konsekwencji zmian w definicjach poszczególnych klauzul tajności, zostaje przesunięta powiększając zakres informacji publicznej. Regulacja może wpłynąć na zwiększenie jawności życia publicznego i ułatwić dostęp do informacji publicznej. Tym samym regulacja poszerza sferę wolności i praw jednostek, zmniejszając ograniczenia prawa do informacji o działalności organów władzy publicznej.

5-02-dg

P)

Minister Spraw Zagranicznych

DPUE-920-1259-09-10/ma/3
SM/266
dot.: RM-10-10-10 z 26.01.2010 r.

Warszawa, dnia 11 lutego 2010 r.

Pan Maciej Berek
Sekretarz Rady Ministrów

opinia o zgodności z prawem Unii Europejskiej *projektu ustawy o ochronie informacji niejawnych oraz o zmianie niektórych ustaw* wyrażona na podstawie art. 13 ust. 3 pkt 2 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2007 r. Nr 65, poz. 437 z późn. zm.) przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej

Szanowny Panie Ministrze,

w związku z przedłożonym projektem *ustawy o ochronie informacji niejawnych oraz o zmianie niektórych ustaw* pozwalam sobie wyrazić następującą opinię:

Projekt jest zgodny z prawem Unii Europejskiej.

Z poważaniem

Z upoważnienia
Ministra Spraw Zagranicznych
Podsekretarz Stanu
Maciej Szpunar

Do wiadomości:

Pan Jacek Cichocki
Kancelaria Prezesa Rady Ministrów
Sekretarz Stanu
Sekretarz Kolegium do spraw Służb Specjalnych

Projekt

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia ……..…. r.

w sprawie sposobu oznaczania materiałów zawierających informacje niejawne, umieszczania na nich klauzul tajności, a także zmiany lub znoszenia nadanej klauzuli tajności

Na podstawie art. 6 ust. 9 ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. …….), zwanej dalej „ustawą", zarządza się, co następuje:

§ 1

1. Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim w sposób wyraźny i w pełnym brzmieniu klauzuli tajności.
2. W przypadku, gdy poszczególnym częściom materiału zostały nadane różne klauzule tajności, bądź gdy niektóre z tych części są jawne, to wówczas wyodrębnione części należy:
   1) oddzielić od siebie poprzez oznaczenie ich odpowiednią klauzulą tajności lub określeniem „jawne";
   2) umieścić odpowiednie oznaczenie przed rozpoczęciem i po zakończeniu tekstu lub obrazu, z jego lewej strony nad i pod wyodrębnionymi częściami.
3. Jeżeli poszczególnym częściom materiału zostały nadane różne klauzule tajności, materiał ten oznacza się klauzulą o najwyższym spośród tych klauzul stopniu tajności.
4. Wprowadza się następujące oznaczenia klauzul tajności:
   1) „00" - dla klauzuli „ściśle tajne";
   2) „0" - dla klauzuli „tajne";
   3) „Pf" - dla klauzuli „poufne";
   4) „Z" - dla klauzuli „zastrzeżone".

§ 2

Użyte w rozporządzeniu określenia oznaczają:

1) dokument elektroniczny – dokument w rozumieniu art. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.[1]);
2) poczta elektroniczna – środek komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm. [2]);
3) metadane – dane opisujące kontekst, treść i strukturę dokumentów przetwarzanych poprzez informatyczny nośnik danych w rozumieniu art. 3 pkt 1 ustawy wymienionej w pkt 1 i ich zarządzanie w czasie.

[1] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501 oraz z 2008 r. Nr 127, poz. 817.

[2] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 96, poz. 959 i Nr 173, poz. 1808, z 2007 r. Nr 50, poz. 331, z 2008 r. Nr 171, poz. 1056 oraz Nr 216, poz. 1371.

§ 3

1. Materiały zawierające informacje niejawne utrwalone na piśmie, dalej zwane „pismem”, oznacza się w następujący sposób:
   1) na każdej stronie pisma umieszcza się:
      a) w lewym górnym rogu sygnaturę literowo-cyfrową, na którą składają się oddzielone myślnikami: literowe oznaczenie jednostki lub komórki organizacyjnej, numer, pod którym pismo zostało zarejestrowane w odpowiedniej ewidencji i oznaczenie klauzuli tajności, łamane przez rok lub dwie ostatnie cyfry roku, w którym pismo zostało wykonane, a także w zależności od potrzeb inne oznaczenia ułatwiające ustalenie miejsca jego wykonania w jednostce lub komórce organizacyjnej nadawcy lub też przynależność pisma do określonej sprawy;
      b) w prawym górnym rogu, w kolejności pionowej:
         – klauzulę tajności;
         – numer egzemplarza pisma, a w przypadku, gdy pismo wykonano w jednym egzemplarzu napis „Egz. pojedynczy”;
      c) w prawym dolnym rogu klauzulę tajności oraz numer strony łamany przez liczbę stron całego pisma;
   2) na pierwszej stronie pisma umieszcza się dodatkowo:
      a) w lewym górnym rogu nazwę jednostki lub komórki organizacyjnej;
      b) w prawym górnym rogu:
         – nazwę miejscowości i datę podpisania pisma;
         – pod klauzulą tajności określenie daty lub wydarzenia wskazujących na jej zniesienie lub zmianę, o których mowa w art. 6 ust. 2 ustawy;
         – w przypadku pisma, któremu nadano bieg korespondencyjny pod numerem egzemplarza w kolejności pionowej: stanowisko, imię i nazwisko adresata oraz nazwę miejscowości, a w przypadku wielu adresatów dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika”;
   3) na ostatniej stronie pisma umieszcza się dodatkowo:
      a) z lewej strony pod treścią:
         – liczbę załączników oraz liczbę stron lub innych jednostek miary wszystkich załączników, jeżeli są dołączone do pisma;
         – klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w odpowiedniej ewidencji;
         – liczbę stron lub inną jednostkę miary każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary;
         – w przypadku, gdy adresatowi wysyła się inną liczbę załączników, niż pozostawia w aktach, dodatkowo napis „tylko adresat” - jeżeli załączniki mają być przekazane adresatowi bez pozostawiania ich w aktach, napis „do zwrotu” - jeżeli załączniki mają zostać zwrócone osobie uprawnionej do jego podpisania;
      b) z prawej strony pod treścią pisma i adnotacją o załącznikach w kolejności pionowej: stanowisko oraz imię i nazwisko osoby uprawnionej do jego podpisania;
      c) w lewym dolnym rogu w kolejności pionowej:

- liczbę wykonanych egzemplarzy;
- adresatów poszczególnych egzemplarzy pisma lub adnotację „adresaci według rozdzielnika”;
- nazwisko lub inne dane identyfikujące wykonawcę.

2. W przypadku pisma, któremu nadano bieg korespondencyjny, na pierwszej stronie w prawym górnym rogu pod numerem egzemplarza można zamieścić dyspozycję dla adresata o treści:
   1) „udzielanie informacji tylko za pisemną zgodą nadawcy”;
   2) „kopiowanie tylko za pisemną zgodą nadawcy”;
   3) „odpis tylko za pisemną zgodą nadawcy”;
   4) „kopiowanie stron od ...do… tylko za pisemną zgodą nadawcy”;
   5) „odpis od ... do ... tylko za pisemną zgodą nadawcy”;
   6) „wypis (wyciąg) od ... do ... tylko za pisemną zgodą nadawcy”.

§ 4

1. Na pismach stanowiących załączniki, na pierwszej stronie w prawym górnym rogu umieszcza się dodatkowo napis: „Załącznik nr ... do pisma nr ... z dnia ...”.
2. Napis, o którym mowa w ust. 1, zamieszcza się także - w miarę możliwości - na innych niż pismo materiałach.
3. Jeżeli przy piśmie przewodnim przesyła się załączniki oznaczone różnymi klauzulami tajności, to:
   1) klauzula pisma przewodniego uwzględnia klauzulę załącznika o najwyższym stopniu tajności;
   2) na piśmie przewodnim zamieszcza się dyspozycję co do klauzuli tajności pisma po trwałym odłączeniu załączników; na każdej stronie pod numerem egzemplarza zamieszcza się napis: „... (nazwa klauzuli tajności) po odłączeniu załączników” lub „jawne po odłączeniu załączników”.
4. Przy rejestracji pisma przewodniego w odpowiedniej ewidencji w rubryce „Informacje uzupełniające/Uwagi” należy wpisać adnotacje, o których mowa w ust. 3 pkt 2.

§ 5

1. Dokumenty elektroniczne przetwarzane wyłącznie w systemie teleinformatycznym, o którym mowa w art. 2 pkt 6 ustawy, podlegające ewidencji w elektronicznym systemie ewidencji dokumentów, oznacza się w sposób określony w § 3.
2. W przypadku dokumentów, o których mowa w ust. 1, na każdej stronie w prawym górnym rogu pod klauzulą tajności umieszcza się napis „Egz. elektroniczny”.

§ 6

1. Na piśmie wysyłanym za pośrednictwem narzędzia lub urządzenia kryptograficznego, na pierwszej stronie wymienia się:
   1) rodzaj dokumentu w zależności od narzędzia lub urządzenia za pośrednictwem, którego dokument ma zostać wysłany;
   2) numer, pod którym dokument został zarejestrowany we właściwej ewidencji, liczbę stron, datę i godzinę nadania;
   3) nazwę jednostki lub komórki organizacyjnej będącej adresatem pisma.
2. Informację potwierdzającą fakt nadania dokumentu za pośrednictwem narzędzia lub urządzenia, o którym mowa w ust. 1, jednostka lub komórka organizacyjna

posiadająca takie narzędzie lub urządzenie umieszcza na pierwszej stronie przekazanego do wysłania dokumentu.

3. Odbiór dokumentu, o którym mowa w ust. 1, adresat potwierdza we właściwej ewidencji nazwą stanowiska oraz czytelnym imieniem i nazwiskiem.
4. Na dokumencie otrzymanym za pośrednictwem narzędzia lub urządzenia, o którym mowa w ust. 1, na pierwszej stronie wymienia się:
   1) rodzaj dokumentu w zależności od narzędzia lub urządzenia, za pośrednictwem którego dokument został otrzymany;
   2) numer, pod jakim dokument został zarejestrowany we właściwej ewidencji, liczbę stron dokumentu, datę i godzinę otrzymania.

§ 7

1. Na materiałach innych niż pismo, klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny widoczny sposób, bezpośrednio, a jeżeli to nie jest możliwe - na ich obudowie lub opakowaniu.
2. Zawarte w materiałach, o których mowa w ust. 1, informacje niejawne utrwalone w formie dźwięku albo obrazu powinny - o ile to możliwe - być poprzedzone i kończyć się wskazaniem klauzuli tajności tych informacji.

§ 8

Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach klauzule tajności umieszcza się po prawej stronie w górnym i w dolnym rogu zewnętrznych ścianek okładki oraz - jeżeli jest to możliwe - na stronie tytułowej.

§ 9

Materiały w postaci prezentacji multimedialnych oznacza się w następujący sposób:

1) na każdym slajdzie lub stronie umieszcza się:
   a) w prawym górnym rogu klauzulę tajności;
   b) w prawym dolnym rogu klauzulę tajności, numer slajdu lub strony, łamany przez liczbę slajdów lub stron;
2) na pierwszym slajdzie lub stronie umieszcza się dodatkowo:
   a) w lewym górnym rogu nazwę jednostki lub komórki organizacyjnej oraz sygnaturę literowo-cyfrową, o której mowa w § 3 ust. 1 pkt 1 lit. a;
   b) w prawym górnym rogu określenie daty lub wydarzenia, o których mowa w art. 6 ust. 2 ustawy.

§ 10

1. Informacje niejawne w postaci poczty elektronicznej przetwarzane są wyłącznie w systemie teleinformatycznym, o którym mowa w art. 2 pkt 6 ustawy.
2. W przypadku informacji, o których mowa w ust. 1, nie wymaga się stosowania dodatkowych oznaczeń, poza wskazaniem na jej początku i po jej zakończeniu klauzuli tajności tych informacji.

§ 11

W pismach zawierających informacje niejawne przekazanych przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych, krajowy

odpowiednik klauzuli tajności umieszcza się w prawym górnym i dolnym rogu pierwszej i ostatniej strony pisma.

§ 12

1. Na pismach zawierających informacje niejawne, wobec których zniesiono przyznaną klauzulę tajności:
   1) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności;
   2) nad pierwszą w kolejności skreśloną klauzulą tajności umieszcza się napis „Jawne" oraz datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji.
2. Na pismach zawierających informacje niejawne, wobec których zmieniono przyznaną klauzulę tajności:
   1) skreśla się wszystkie dotychczasowe oznaczenia klauzuli tajności;
   2) nad skreślonymi klauzulami tajności umieszcza się nowe klauzule tajności;
   3) nad pierwszą w kolejności skreśloną klauzulą tajności umieszcza się datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji.
3. Skreśleń i adnotacji, o których mowa w ust. 1-2, dokonuje odpowiednio kierownik kancelarii lub kierownik archiwum lub inne upoważnione przez nich albo przez kierownika jednostki organizacyjnej osoby.
4. Skreśleń i adnotacji, o których mowa w ust. 1-2, dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.
5. W stosunku do materiałów, o których mowa w § 6-9, przepisy ust. 1-4 stosuje się odpowiednio, uwzględniając sposób oznakowania tych materiałów.
6. W materiałach, o których mowa w § 5, informacje o zmianach umieszcza się jedynie w odpowiednich ewidencjach lub w metadanych systemów teleinformatycznych elektronicznej ewidencji dokumentów.

§ 13

1. Na kopiach, odpisach, wypisach, wyciągach lub tłumaczeniach materiałów zawierających informacje niejawne o klauzuli „poufne" lub wyższej umieszcza się:
   1) na wszystkich stronach w prawym górnym rogu odpowiednio napis: „Kopia", „Odpis", „Wypis", „Wyciąg" lub „Tłumaczenie z języka - (nazwa języka) - (nazwisko tłumacza)";
   2) na pierwszej stronie dodatkowo numer, pod jakim zostały zarejestrowane w odpowiedniej ewidencji, numer egzemplarza wykonanej kopii, odpisu, wypisu, wyciągu lub tłumaczenia;
   3) na ostatniej stronie dodatkowo napis „Za zgodność z oryginałem" i odcisk tuszowej pieczęci z nazwą jednostki lub komórki organizacyjnej, w której sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie.
2. Zgodność z oryginałem kopii, odpisu, wypisu lub wyciągu, o których mowa w ust. 1, potwierdza czytelnie imieniem i nazwiskiem kierownik jednostki lub komórki organizacyjnej albo inna osoba przez niego upoważniona, a tłumaczenia - osoba dokonująca tłumaczenia.
3. Fakt sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia, o których mowa w ust. 1, odnotowuje się, z zastrzeżeniem ust. 5, na ostatniej stronie dokumentu, z którego sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie, przez umieszczenie adnotacji informującej o:

1) nazwie jednostki lub komórki organizacyjnej, w której sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie;
2) liczbie egzemplarzy sporządzonych kopii, odpisów, wypisów, wyciągów lub tłumaczeń;
3) dacie sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia;
4) numerze, pod jakim kopia, odpis, wypis, wyciąg lub tłumaczenie zostały zarejestrowane w odpowiedniej ewidencji.

4. Adnotacje, o których mowa w ust. 3 pkt 1-3, wpisuje się przed wykonaniem kopii, odpisu, wypisu, wyciągu lub tłumaczenia, natomiast numer, pod jakim zostały zarejestrowane w odpowiedniej ewidencji, nanosi się po wykonaniu kopii, odpisu, wypisu, wyciągu lub tłumaczenia.
5. Na kopiach, odpisach, wypisach, wyciągach i tłumaczeniach materiałów, o których mowa w § 5 oraz § 9-10, zawierających informacje niejawne o klauzuli „poufne" lub wyższej dokonuje się adnotacji określonych w ust. 3.
6. W przypadku wykonania kopii, odpisu, wypisu, wyciągu i tłumaczenia z materiałów, o których mowa w ust. 5 dokonujący tej czynności informuje o tym ich nadawcę lub wykonawcę.
7. W przypadku wykonywania kopii, odpisu, wypisu, wyciągu lub tłumaczenia materiałów archiwalnych zgromadzonych w archiwach państwowych oraz archiwach państwowych wyodrębnionych, nie dokonuje się czynności, o których mowa w ust. 3, z tym że do materiałów dołącza się kartę informacyjną, na której każdorazowo umieszcza się informację o wykonaniu kopii, odpisu, wypisu, wyciągu lub tłumaczenia. W karcie powinno zamieszczać się adnotacje, o których mowa w ust. 3.

§ 14

Traci moc rozporządzenie Prezesa Rady Ministrów z dnia 5 października 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzuli tajności, a także zmiany nadanej klauzuli tajności (Dz.U. Nr 205, poz. 1696).

§ 15

Rozporządzenie wchodzi w życie z dniem ……..

Prezes Rady Ministrów

UZASADNIENIE

Rozporządzenie stanowi wykonanie delegacji ustawowej wyrażonej w art. 6 ust. 9 ustawy z dnia …….. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. ……..), zwanej dalej „ustawą”.

Konieczność wydania nowego rozporządzenia Prezesa Rady Ministrów w sprawie sposobu oznaczania materiałów zawierających informacje niejawne, umieszczania na nich klauzul tajności, a także zmiany lub znoszenia nadanej klauzuli tajności wynika z niezbędności dostosowania przepisów aktu wykonawczego do fundamentalnych zmian wprowadzonych do systemu ochrony informacji niejawnych wraz z ustawą.

Podstawą przygotowania projektu stała się potrzeba kompleksowego unormowania oznaczania informacji niejawnych niezależnie od sposobu ich utrwalania.

W § 1 zawarto ogólne informacje na temat sposobu i rodzaju oznaczeń klauzul tajności wprowadzonych w ustawie, korzystając z dotychczasowego dorobku i wprowadzając jednocześnie możliwość nadawania poszczególnym częściom materiału różnych klauzul tajności.

W § 2 wprowadzono „słowniczek” zawierający wyjaśnienie występujących w rozporządzeniu terminów teleinformatycznych.

W § 3 określono sposób oznaczania materiałów zawierających informacje niejawne, utrwalone w formie pisemnej, zatem najczęściej występującej i nazywanej generalnie „pismem”. W § 4 uregulowano sposób oznaczania pism stanowiących załączniki.

W stosunku do dotychczasowych regulacji w tym zakresie zaproponowane zmiany obejmują likwidację podawania numeru dokumentu z Dziennika Ewidencji Wykonanych Dokumentów, zwanego dalej „DEWD”, bowiem dążąc do uproszczenia sposobu rejestrowania postanowiono o likwidacji tej ewidencji. Wartym wskazania jest, iż odstąpienie od prowadzenia tej dodatkowej ewidencji było m.in. powodowane rozszerzającym się zastosowaniem systemów teleinformatycznych, co w coraz większym stopniu skutkować będzie ograniczeniem, a docelowo nawet wyeliminowaniem papierowego obiegu dokumentacji.

Co ważne, przy identyfikowaniu osoby przygotowującej pismo ograniczono się tylko do pojęcia „wykonawcy”, zamiast stosowanego wcześniej rozróżnienia występującego w DEWD – „wykonujący” oraz „sporządzający”. Zasadnym jest wyjaśnienie, iż o zastąpieniu pojęcia „sporządzający” i „wykonawca”, jednym określeniem „wykonawca” zadecydowało dążenie do jak największego uproszczenia dotychczasowo obowiązujących przepisów, przy jednoczesnym wprowadzeniu pojęcia generalno-abstrakcyjnego zawierającego większy zakres semantyczny, a zarazem umożliwiającego ewentualne zastosowanie wewnętrznych uregulowań uszczegóławiających stosowanie przepisów niniejszego rozporządzenia. Porządkowo zastosowano również jednolitą terminologię, co do wskazania osoby przygotowującej dokument lub materiał jako „wykonawcy” i co do podejmowanych przez nią czynności, czyli przygotowania dokumentacji jako „wykonania”.

Co ważne, zmiana przepisów wymagała odstąpienia od dotychczasowych rozwiązań dotyczących „przedłużania” lub „skracania” okresów ochrony. Wskutek takich działań zlikwidowano obowiązek przeglądu dokumentów - co niewątpliwie mogłoby się wiązać ze zmianą obowiązujących oznaczeń - przed ewentualnym udostępnieniem lub przekazaniem dokumentu osobom spoza jednostki lub komórki organizacyjnej. Co istotne, określenie, w jakim terminie lub po wystąpieniu, jakiego wydarzenia, dokument stanie się jawny stało się suwerenną decyzją osoby uprawnionej do jego podpisania lub oznaczania innego niż dokument materiału – art. 6 ust. 2 ustawy.

Wymieniając elementy, które powinny być umieszczone na piśmie przyjęto wnioskowanie dedukcyjne, czyli przechodzono od ogółu do szczegółu – najpierw wskazano, jakie mają być oznaczenia na wszystkich stronach dokumentu, a następnie, jakie mają być odrębne oznaczenia charakteryzujące jego pierwszą i ostatnią stronę.

Zrezygnowano z określenia „osoba podpisująca" na rzecz terminologii nowej ustawy „osoba uprawniona do podpisania".

Odstąpiono od określenia „dzienniki" na rzecz ogólnego pojęcia „odpowiednie ewidencje", w którym mogą zawierać się zarówno dzienniki, książki, jak i rejestry, bez względu na stosowane nazewnictwo.

W kolejnych jednostkach redakcyjnych określono sposób oznaczania pozostałych rodzajów – ze względu na sposób utrwalenia – materiałów zawierających informacje niejawne.

W § 5 określono sposób oznaczania oficjalnych dokumentów przetwarzanych wyłącznie w systemie teleinformatycznym, dopuszczonym do przetwarzania informacji niejawnych, które podlegają ewidencji w elektronicznym systemie ewidencji dokumentów i nie muszą mieć wersji papierowej. Z uwagi na upowszechnianie się teleinformatyzacji jednostek organizacyjnych dodanie tego przepisu jest w pełni uzasadnione.

W § 6 określono sposób postępowania związany z oznaczaniem dokumentów przekazywanych za pośrednictwem narzędzi lub urządzeń kryptograficznych. Podmioty ustawy należące do Sił Zbrojnych Rzeczpospolitej Polskiej i jednostek organizacyjnych, a także innych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych podczas prowadzonych prac legislacyjnych sygnalizowały potrzebę uregulowania tego zagadnienia w akcie normatywnym powszechnie obowiązującym.

W § 7 uregulowano sposób oznaczania materiałów innych niż pismo (np. elektronicznych nośników informacji) za pomocą, których utrwalono informacje niejawne i właściwie w tym przypadku oparto się na obowiązujących dotychczas rozwiązaniach.

W § 8 określono sposób oznaczania trwale oprawionych zbiorów dokumentów, rejestrów, książek, broszur i reprodukcji. W tym przypadku również oparto się na obowiązujących dotychczas rozwiązaniach.

W § 9 zaistniała potrzeba uregulowania, wcześniej pomijanych kwestii sposobu oznaczania materiałów w postaci prezentacji multimedialnych. Powszechność przedstawiania efektów podjętych działań w formie slajdów lub stron wymagała dookreślenia, jakie elementy będą umieszczane na danych materiałach.

W § 10 uregulowano sposób postępowania w zakresie oznaczania informacji niejawnych w postaci poczty elektronicznej. Tematyka ta nie była wcześniej podejmowana. Informacje będą przetwarzane wyłącznie w akredytowanym systemie teleinformatycznym, ale aby usprawnić przekaz i uczynić go bardziej efektywnym oraz szybszym nie będą wymagane szczególne sposoby oznaczania i rejestracji, chyba, że zajdzie potrzeba ich skopiowania w postaci wydruku. Zastosowanie będą miały wówczas postanowienia § 13.

W § 11 określono sposób postępowania w przypadku nadawania krajowego odpowiednika klauzuli tajności na pismach zawierających informacje niejawne przekazanych przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych. Wraz ze wzrostem współpracy międzynarodowej oraz z uwagi na członkostwo w Unii Europejskiej, ale także w instytucjach Wspólnotowych uregulowanie tej porządkowej kwestii stało się niezbędne.

W § 12 odniesiono się do kwestii oznaczeń, które należy nanieść na materiały zawierające informacje niejawne, w przypadku zniesienia lub zmiany klauzuli tajności. Istotnym faktem jest, iż zgodnie z art. 6 ust. 2 ustawy to osoba uprawniona do podpisania

dokumentu lub oznaczania innego niż dokument materiału ustala okoliczności lub datę, po których nastąpi zniesienie lub zmiana klauzuli tajności i nie będą już obowiązywały ustalone ustawowo okresy ochrony, z zastrzeżeniem art. 7 ustawy. Co ważne, w danym przepisie uwzględniono również nanoszenie odpowiednich zmian na materiałach niejawnych stanowiących *novum* w przedmiotowym rozporządzeniu, z uwzględnieniem ich specyfiki.

W § 13 uregulowano kwestie oznaczania kopii, odpisów, wypisów, wyciągów lub tłumaczeń pism zawierających informacje niejawne. Co istotne, określone wymagania dotyczące oznaczeń takich kopii, odpisów, wypisów, wyciągów lub tłumaczeń oraz oznaczeń materiałów podlegających tym czynnościom dotyczą wyłącznie informacji niejawnych o klauzuli „poufne" lub wyższej. Oznacza to odmienne traktowanie informacji o klauzuli „zastrzeżone", czyli de facto odstąpienie od rozliczalności kopii, odpisów, wypisów, wyciągów lub tłumaczeń pism zawierających informacje niejawne o tej klauzuli tajności. Jest to zmiana dostosowana do standardów obowiązujących w UE, co jest niezwykle istotne w kontekście prezydencji Polski w tej organizacji.

Ocena Skutków Regulacji

1. **Podmioty, na które oddziałuje rozporządzenie**

Zakres oddziaływania znowelizowanych przepisów rozporządzenia jest ograniczony do podmiotów wymienionych w art. 1 ust. 2 ustawy o ochronie informacji niejawnych.

2. **Wpływ regulacji na sektor finansów publicznych, w tym na budżet państwa i budżety jednostek samorządu terytorialnego**

Wejście w życie rozporządzenia nie wywoła zwiększenia wydatków z budżetu państwa i budżetu jednostek samorządu terytorialnego.

3. **Wpływ regulacji na rynek pracy**

Wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy.

4. **Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw**

Wejście w życie rozporządzenia nie wpłynie na konkurencyjność gospodarki i przedsiębiorczość.

5. **Wpływ regulacji na sytuację i rozwój regionalny**

Wejście w życie rozporządzenia pozostanie bez wpływu na sytuację i rozwój regionalny.

6. **Zgodność z przepisami prawa Unii Europejskiej**

Przedmiotowe rozporządzenie pozostaje poza zakresem prawa Unii Europejskiej. Projekt rozporządzenia nie zawiera przepisów technicznych i w związku z tym nie podlega procedurze notyfikacji aktów prawnych, określonej w rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039 i z 2004 r. Nr 65, poz. 597).

36-02-aa

Projekt

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia _____ r.

w sprawie zakresu, trybu i sposobu współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa

(Dz. U. z dnia _____ r.)

Na podstawie art. 11 ust. 6 ustawy z dnia _____ r. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. z _____ r. Nr ____, poz. ____) zarządza się, co następuje:

§ 1

Współdziałanie Szefa ABW i Szefa SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa polega w szczególności na:

1) udzielaniu Szefowi ABW przez Szefa SKW informacji niezbędnych do pełnienia funkcji krajowej władzy bezpieczeństwa;
2) asystowaniu imiennie upoważnionych funkcjonariuszy ABW podczas wykonywania niektórych czynności właściwych dla krajowej władzy bezpieczeństwa przez SKW oraz imiennie upoważnionych żołnierzy i funkcjonariuszy SKW podczas wykonywania niektórych czynności właściwych dla krajowej władzy bezpieczeństwa przez ABW;
3) uzgadnianiu działań podejmowanych w ramach wykonywania funkcji krajowej władzy bezpieczeństwa;
4) uzgadnianiu składu delegacji reprezentujących Rzeczypospolitą Polską przed organizacjami międzynarodowymi i krajowymi władzami bezpieczeństwa innych państw oraz ustalania treści stanowisk przedstawianych przez takie delegacje;
5) prowadzeniu, dostępie oraz udzielaniu informacji ze zbiorów danych dotyczących wykonywania funkcji krajowej władzy bezpieczeństwa.

§ 2

1. Szef ABW określa, po zasięgnięciu opinii Szefa SKW, warunki i wymagania konieczne do zapewnienia efektywnej organizacji i koordynacji współdziałania z Szefem SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa.
2. Organizacja współdziałania może obejmować w szczególności potrzebę:
   1) powołania zespołu składającego się z funkcjonariuszy ABW i żołnierzy oraz funkcjonariuszy SKW, którego pracami kieruje upoważniony funkcjonariusz ABW;
   2) organizacji doraźnych kontaktów roboczych, planowych odpraw sprawozdawczych i innych spotkań uzgodnieniowych;
   3) wskazania punktu kontaktowego, w tym utworzenia stałego dyżuru telefonicznego;
   4) oddelegowania żołnierza lub funkcjonariusza SKW albo funkcjonariusza ABW do pełnienia służby odpowiednio w ABW lub SKW;
   5) stworzenia lub wskazania systemu teleinformatycznego służącego wymianie informacji.
3. Podjęcie współdziałania nie może zakłócać prawidłowego wykonywania zadań ABW i SKW wynikających z odrębnych przepisów.

§ 3

1. Współdziałanie, o którym mowa w § 1 pkt 1, obejmuje:
   1) informowanie o prowadzonych i planowanych procedurach określonych w przepisach dotyczących ochrony informacji niejawnych międzynarodowych;
   2) przekazywanie wzorów stosowanej lub przewidywanej dokumentacji mającej zastosowanie w nadzorze nad informacjami niejawnymi międzynarodowymi;
   3) informowanie o przyjętej i przewidywanej praktyce stosowania wymagań bezpieczeństwa dotyczących ochrony informacji niejawnych międzynarodowych;
   4) zapoznawanie z wewnętrznymi regulacjami prawnymi dotyczącymi organizacji i funkcjonowania systemu ochrony informacji niejawnych międzynarodowych;
   5) prezentowanie organizacji i stanu systemu ochrony informacji niejawnych międzynarodowych oraz działań podejmowanych w celu zapewnienia prawidłowości jego funkcjonowania;
   6) informowanie o wpływie oraz prowadzeniu korespondencji, której treść posiada znaczenie dla zapewnienia prawidłowego nadzoru nad systemem ochrony informacji międzynarodowych;

7) przekazywanie danych koniecznych do wypełniania zadań informacyjnych, ewidencyjnych, i analitycznych;
8) udostępnianie sprawozdań, raportów, notatek lub innych dokumentów o tym charakterze w zakresie, w jakim:
   a) zawierają wyniki czynności nadzorczych, wyjaśniających i innych opisujących stan systemu ochrony informacji niejawnych międzynarodowych;
   b) relacjonują udział w pracach zespołów, grup, komitetów i innych spotkań poświęconych ochronie informacji niejawnych międzynarodowych.
   c) dotyczą innych spraw objętych zakresem współdziałania.

2. Szef ABW określa, po zasięgnięciu opinii Szefa SKW, częstotliwość przekazywania lub udostępniania oraz rodzaj wymaganych informacji, materiałów i dokumentów.

3. Szef SKW przekazuje lub udostępnia Szefowi ABW wymagane informacje, materiały i dokumenty niezwłocznie, o ile nie wskazano terminu przekazania lub udostępnienia.

4. Szef ABW udziela Szefowi SKW informacji, o których mowa w ust. 1, w zakresie niezbędnym do zapewnienia skuteczności i jednolitości systemu ochrony informacji niejawnych międzynarodowych.

§ 4

1. Współdziałanie, o którym mowa w § 1 pkt 2 dotyczy czynności związanych z:
   1) procedurą tworzenia i nadzorowania kancelarii tajnych międzynarodowych;
   2) procedurą akredytacji systemów teleinformatycznych, w których przetwarzane są lub będą informacje niejawne międzynarodowe;
   3) prowadzeniem inspekcji w podmiotach, w których są lub będą przetwarzane informacje niejawne międzynarodowe;
   4) prowadzeniem czynności wyjaśniających związanych z naruszeniem przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych międzynarodowych;
   5) szkoleniami oraz innymi przedsięwzięciami edukacyjnymi i doradczymi.

2. Szef SKW informuje Szefa ABW o zamiarze podjęcia wymienionych w ust. 1 czynności i umożliwia, na wniosek Szefa ABW, asystowanie upoważnionych funkcjonariuszy ABW w tych czynnościach.

3. Szef SKW może odmówić realizacji wniosku o umożliwienie asysty, jeżeli jego realizacja wiązałaby się ze szczególnie poważnymi trudnościami.

4. Szef ABW informuje Szefa SKW o możliwości asystowania upoważnionych żołnierzy lub funkcjonariuszy SKW w czynnościach, o których mowa w ust. 1, tylko jeżeli jest to uzasadnione koniecznością zapewnienia asysty osób posiadających określone kompetencje lub ze względów szkoleniowych albo z uwagi na spodziewaną korzyść w zakresie ujednolicenia postępowania w danej dziedzinie.

§ 5

1. Współdziałanie, o którym mowa w § 1 pkt 3, dotyczy:
   1) spraw, o których mowa w § 1 pkt 1, 2, 4 i 5;
   2) wykładni przepisów dotyczących ochrony informacji niejawnych międzynarodowych;
   3) materiałów wykorzystywanych lub przekazywanych w czasie szkoleń z zakresu ochrony informacji niejawnych międzynarodowych;
   4) wydawania poświadczeń bezpieczeństwa i innych dokumentów stwierdzających zdolność osoby lub podmiotu do ochrony informacji niejawnych międzynarodowych;
   5) zawierania i realizacji międzynarodowych umów o ochronie informacji niejawnych;
   6) opiniowania projektów zmian w przepisach dotyczących ochrony informacji niejawnych międzynarodowych;
   7) udzielania odpowiedzi na zapytania w sprawach związanych z ochroną informacji niejawnych międzynarodowych, kierowane przez organizacje międzynarodowe, krajowe władze bezpieczeństwa innych państw oraz inne instytucje i osoby;
   8) innych przedsięwzięć mogących mieć wpływ na wywiązywanie się Rzeczypospolitej Polskiej z zobowiązań dotyczących ochrony informacji niejawnych międzynarodowych.
2. Szef ABW określa, w uzgodnieniu z Szefem SKW, jednolite zasady oraz, jeżeli to konieczne, szczegółowy sposób postępowania oraz w sprawach, o których mowa w ust. 1.
3. Odmienność postępowania, o którym mowa w ust. 2, może występować jedynie w przypadku, gdy osiągnięcie jednolitości nie jest możliwe ze względu na przepisy prawa, charakterystykę obszaru działania, uwarunkowania techniczne i inne.

§ 6

1. Współdziałanie, o którym mowa w § 1 pkt 4, dotyczy przypadków udziału przedstawicieli Rzeczypospolitej Polskiej w:

1) posiedzeniach komitetów, grup roboczych i zespołów eksperckich dotyczących ochrony informacji niejawnych międzynarodowych;
2) negocjacjach umów międzynarodowych o ochronie informacji niejawnych;
3) spotkaniach z przedstawicielami struktur organizacji międzynarodowych odpowiedzialnych za ochronę informacji niejawnych międzynarodowych oraz przedstawicielami krajowych władz bezpieczeństwa innych państw;
4) innych przedsięwzięciach dotyczących ochrony informacji niejawnych międzynarodowych

2. Szef ABW i Szef SKW informują się nawzajem o planowanym spotkaniu, jego tematyce proponowanym składzie delegacji oraz treści przedstawianych przez nią stanowisk. Brak zastrzeżeń oznacza uzgodnienie tych spraw.

3. Informacje, o których mowa w ust. 2, są przekazywane w terminie pozwalającym na wyrażenie zastrzeżeń i podjęcia próby ich usunięcia.

4. Określenie składu delegacji oznacza wskazanie liczby i stanowisk osób wchodzących w jej skład.

5. W przypadku braku uzgodnienia, o którym mowa w ust. 2, skład delegacji oraz treść przedstawianych przez nią stanowisk określa Szef ABW.

§ 7

1. Zbiory danych, których mowa w § 1 pkt 5 dotyczą:
1) stanu procedur dotyczących badania zdolności osoby lub podmiotu do ochrony informacji niejawnych międzynarodowych a także rozstrzygnięć i innych dokumentów wydanych w ich toku;
2) zatwierdzonych kancelarii tajnych międzynarodowych;
3) akredytowanych systemów teleinformatycznych.

2. Szef ABW i Szef SKW, każdy w swoim zakresie, prowadzi zbiory danych, o których mowa w ust. 1, zapewniając do nich dostęp, w tym, o ile to możliwe, w formie zapisu informatycznego, na zasadzie wzajemności.

§ 8

Szef ABW i Szef SKW mogą:
1) wskazać jednostki, komórki organizacyjne lub upoważnionych funkcjonariuszy lub żołnierzy odpowiednio ABW i SKW, którzy współdziałają ze sobą bezpośrednio;
2) zawierać porozumienia określające szczegółowe formy współdziałania.

§ 9

1. Szef ABW dokonuje oceny współdziałania z Szefem SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa i przedstawia ją raz w roku Przewodniczącemu Kolegium do Spraw Służb Specjalnych.

2. Ocena, o której mowa w ust. 1, udostępniana jest Szefowi SKW na co najmniej 7 dni przed jej przedstawieniem Przewodniczącemu Kolegium do Spraw Służb Specjalnych.

3. W przypadku zastrzeżeń Szefa SKW co do oceny współdziałania, zastrzeżenia te przekazuje się Przewodniczącemu Kolegium do Spraw Służb Specjalnych wraz z oceną.

§ 10

Rozporządzenie wchodzi w życie _____.

Prezes Rady Ministrów

UZASADNIENIE

Rozporządzenie stanowi wykonanie delegacji ustawowej wyrażonej w art. 11 ust. 6 i 7 ustawy z dnia …….. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. ……..), zwanej dalej „ustawą".

Konieczność wydania rozporządzenia Prezesa Rady Ministrów w sprawie zakresu, trybu i sposobu współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa Agencji Bezpieczeństwa Wewnętrznego wynika z niezbędności określenia przepisów regulujących wykonywanie obowiązków wskazanych w art. 11 ust. 1 w związku z ust. 3 i 5 ustawy.

Stanowią one, że Szef ABW nadzorując system ochrony informacji niejawnych międzynarodowych w Polsce wykonuje to zadanie (czyli funkcję krajowej władzy bezpieczeństwa) w sferze wojskowej nie samodzielnie, lecz za pośrednictwem Szefa SKW i jest odpowiedzialny za organizację współdziałania w tym zakresie. Mając zatem na względzie, że tak ukonstytuowana współzależność równorzędnych organów (wykazująca zarazem cechy nadrzędności jednego z nich) może powodować zasadnicze trudności w praktyce stosowania prawa, a także z uwagi na fundamentalną zmianę dotychczasowego, ugruntowanego 11-letnią praktyką stanu prawnego w zakresie odpowiedzialności tych dwóch organów za ochronę informacji niejawnych międzynarodowych (od pełnej niezależności do powierzenia jej Szefowi ABW), jedynym rozwiązaniem zapewniającym uzyskanie oczekiwanych skutków regulacji – zcentralizowanie nadzoru zmierzające do ujednolicenia standardów – jest wydanie rozporządzenia Prezesa Rady Ministrów w zaproponowanym zakresie i treści.

Podstawą przygotowania projektu stała się zasada ograniczenia do niezbędnego minimum liczby zmian w odniesieniu do obecnie funkcjonującego systemu ochrony informacji niejawnych międzynarodowych. Zaproponowane unormowania mają zasadniczo jedynie zapewnić Szefowi ABW bieżący i efektywny dostęp do wiedzy o stosowanych w sferze wojskowych standardach oraz realny wpływ na ich ewentualną modyfikację. Z kolei Szefowi SKW pozostawiają bardzo szeroką autonomię działania, którego jednak część będzie miał obowiązek konsultować z Szefem ABW. Generalnym założeniem rozporządzenia jest takie zaprojektowanie współdziałania pomiędzy Szefem ABW a Szefem SKW, aby stanowiska, decyzje i działania krajowej władzy bezpieczeństwa stanowiły wynik uzgodnień, wymiany opinii i koordynacji. Zachowanie dla Szefa ABW prawa do suwerennego i wiążącego Szefa SKW postępowania stanowią co do zasady wyjątek; są ostatecznością w przypadku braku uzgodnienia lub wynikają z konieczności zapewnienia skutecznej organizacji współdziałania.

W § 1 określono podstawowe płaszczyzny współpracy Szefa ABW i SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa ABW. Wśród nich wskazano asystowanie imiennie upoważnionych funkcjonariuszy ABW podczas wykonywania niektórych czynności właściwych dla krajowej władzy bezpieczeństwa przez SKW oraz imiennie upoważnionych żołnierzy i funkcjonariuszy SKW podczas wykonywania niektórych czynności właściwych dla krajowej władzy bezpieczeństwa przez ABW, które ma na celu zapewnienie na zasadach wzajemności wymianę doświadczeń w najbardziej bezpośredni, skuteczny i ekonomiczny sposób,

czyli poprzez uczestnictwo jako obserwator w podejmowanych działaniach. Z kolei uzgadnianie składu delegacji reprezentujących Rzeczypospolitą Polską przed organizacjami międzynarodowymi i krajowymi władzami bezpieczeństwa innych państw oraz ustalania treści stanowisk przedstawianych przez takie delegacje ma stanowić skuteczne narzędzie do występowania przed partnerami zagranicznymi zawsze z jednolitym stanowiskiem i jedną reprezentacją, czego w obecnym stanie prawnym nie można w praktyce osiągnąć.

W § 2 określono przykładowo praktyczne sposoby zapewnienia efektywnej organizacji i koordynacji współdziałania Szefa ABW i Szefa SKW. Mając na względzie, że za organizację współdziałania zgodnie z art. 11 ust. 5 ustawy ma odpowiadać Szef ABW, to jemu pozostawiono – po zasięgnięciu opinii Szefa SKW – ostateczny wybór konkretnych środków.

W § 3 uszczegółowiono zakres tematyczny udzielanych Szefowi ABW przez Szefa SKW informacji niezbędnych do pełnienia funkcji krajowej władzy bezpieczeństwa. Pozostawiono Szefowi ABW określenie, po zasięgnięciu opinii Szefa SKW, innych parametrów dotyczących tej formy współpracy (częstotliwość i rodzaj przekazywanych informacji). Zapewniono również, że Szef ABW będzie udzielał Szefowi SKW informacji w zakresie niezbędnym do zapewnienia skuteczności i jednolitości systemu ochrony informacji niejawnych międzynarodowych.

W § 4 wskazano rodzaje działań jednej z instytucji (ABW lub SKW), w których udział obserwatorów z instytucji drugiej może być uzasadniony. Uwzględniono również sytuację, w której ze względu na szczególnie poważne trudności Szef SKW może odmówić Szefowi ABW zgody na asystę podległych mu funkcjonariuszy. Nie przewidziano sytuacji odwrotnej, gdyż żołnierze lub funkcjonariusze SKW będą mogli uczestniczyć w działaniach ABW tylko w wyniku zaproszenia.

W § 5 wymienione zostały sprawy, które wymagają ujednolicenia zasad postępowania, przy czym ostateczna decyzja co do sposobu postępowania w danej sprawie należy do Szefa ABW. Zastrzeżono jednocześnie przypadki, w których można zachować odmienność w sferze wojskowej i cywilnej.

W § 6 wskazano okoliczności wymagające uzgodnienia składu delegacji reprezentujących Rzeczypospolitą Polską oraz ustalania treści stanowisk przedstawianych przez takie delegacje. Zastosowano przy tym regułę wzajemnego informowania się w tym zakresie oraz zasadę, że brak zastrzeżeń oznacza uzgodnienie sprawy. Także w tym przypadku Szef ABW będzie miał decydujący głos w sprawach spornych.

W § 7 określono zakres danych przekazywanych sobie na zasadach wzajemności ze zbiorów prowadzonych samodzielnie przez ABW i SKW.

W § 8 wskazano możliwość bezpośredniego współdziałania jednostek, komórek organizacyjnych i funkcjonariuszy lub żołnierzy ABW i SKW oraz zawierania porozumień określające szczegółowe formy współdziałania.

W § 9 przewidziano procedurę nadzoru współdziałania Szefa ABW i Szefa SKW przez Przewodniczącego Kolegium do Spraw Służb Specjalnych. Podstawą ma być coroczna ocena tego współdziałania dokonywana przez Szefa ABW, przedstawiana Szefowi SKW a następnie, z ewentualnymi zastrzeżeniami Szefa SKW, Przewodniczącemu Kolegium do Spraw Służb Specjalnych.

Projekt

ROZPORZĄDZENIE

PREZESA RADY MINISTRÓW

z dnia …….

w sprawie szczegółowego sposobu przygotowania i trybu przeprowadzania przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego kontroli stanu zabezpieczenia informacji niejawnych

(Dz. U. z dnia …….)

Na podstawie art. 12 ust. 6 ustawy z dnia _____ o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. Nr_____) zarządza się, co następuje:

§ 1. 1. Rozporządzenie określa szczegółowy tryb przygotowania i prowadzenia kontroli w zakresie ochrony informacji niejawnych, w tym uzgadniania kontroli w stosunku do Kancelarii Sejmu Rzeczypospolitej Polskiej, Senatu Rzeczypospolitej Polskiej oraz Prezydenta Rzeczypospolitej Polskiej.

2. Kontrola obejmuje badanie:

1) stanu zabezpieczenia informacji niejawnych;
2) przestrzegania przepisów w zakresie ochrony informacji niejawnych;
3) prawidłowości prowadzenia postępowań sprawdzających, z wyłączeniem postępowań, o których mowa w art. 23 ust. 5 ustawy;
4) stanu zabezpieczenia sieci lub systemów teleinformatycznych.

§ 2. Szef Agencji Bezpieczeństwa Wewnętrznego, zwanej dalej „ABW" lub Szef Służby Kontrwywiadu Wojskowego, zwanej dalej „SKW" w postępowaniu kontrolnym w szczególności:

1) opracowuje ogólne założenia prowadzenia kontroli i sprawuje ogólny nadzór nad jej realizacją;
2) reprezentuje podległe służby wobec innych organów, instytucji i podmiotów w sprawach objętych działaniami kontrolnymi;
3) wykonuje czynności związane z rozpatrywaniem zastrzeżeń;

4) kieruje opracowaniem informacji o wynikach kontroli;
5) podejmuje działania zmierzające do wykorzystania uwag i wniosków przez adresatów wystąpień pokontrolnych.

§ 3. Upoważniony do przeprowadzania kontroli funkcjonariusz ABW lub funkcjonariusz albo żołnierz SKW zwany dalej „kontrolerem", wykonując czynności kontrolne:

1) przeprowadza kontrolę w jednostce kontrolowanej, zgodnie z przepisami ustawy, trybem określonym w rozporządzeniu oraz programem kontroli;
2) dokonuje w sposób wnikliwy i obiektywny ustaleń kontroli oraz rzetelnie je dokumentuje;
3) bierze udział w postępowaniu w sprawie rozpatrywania zastrzeżeń;
4) wykonuje inne zadania w zakresie postępowania kontrolnego, zlecone odpowiednio przez Szefa ABW lub Szefa SKW.

§ 4. 1. ABW lub SKW prowadzi kontrole planowe na podstawie rocznego planu kontroli, zatwierdzonego odpowiednio przez Szefa ABW lub Szefa SKW, po uzyskaniu opinii Kolegium do Spraw Służb Specjalnych.

2. Szef ABW lub Szef SKW może zarządzić doraźną kontrolę, nieujętą w planie, jeżeli uzyska informacje wskazujące na występowanie zagrożeń dla systemu zabezpieczenia informacji niejawnych lub nieprawidłowości dotyczących postępowań sprawdzających.

§ 5. 1. Kontrole przeprowadza się na podstawie opracowanego programu kontroli. Program kontroli wykonuje się w jednym egzemplarzu.

2. Program kontroli planowej zatwierdza upoważniony funkcjonariusz ABW lub funkcjonariusz albo żołnierz SKW.

3. Program kontroli doraźnej zatwierdza odpowiednio Szef ABW lub Szef SKW.

4. Zmiany w programach kontroli zatwierdza upoważniony funkcjonariusz ABW lub funkcjonariusz albo żołnierz SKW.

5. Program kontroli w stosunku do Kancelarii Sejmu Rzeczypospolitej Polskiej, Senatu Rzeczypospolitej Polskiej oraz Prezydenta Rzeczypospolitej Polskiej zatwierdza Prezes Rady Ministrów, po uprzednim uzgodnieniu, określonych w tym programie czynności, odpowiednio z Marszałkiem Sejmu Rzeczypospolitej Polskiej, Marszałkiem Senatu Rzeczypospolitej Polskiej lub Szefem Kancelarii Prezydenta Rzeczypospolitej Polskiej.

§ 6. Przy opracowywaniu programu kontroli uwzględnia się w szczególności:

1) wyniki wcześniejszych kontroli;
2) wyniki analiz określonych problemów z zakresu ochrony informacji niejawnych;
3) informacje pochodzące od organów państwowych i samorządowych, jednostek organizacyjnych i podmiotów, o których mowa w art. 1 ust. 2 ustawy;
4) opinie, wnioski oraz inne ustalenia w zakresie ochrony informacji niejawnych, dokonane przez Kolegium do Spraw Służb Specjalnych.

§ 7. W programie kontroli zamieszcza się w szczególności:

1) nazwę kontrolowanej jednostki organizacyjnej oraz jej dokładny adres;
2) oznaczenie i temat kontroli;
3) określenie kierunku badań kontrolnych i problemów wymagających oceny;
4) szczegółowe określenie zakresu przedmiotowego i podmiotowego kontroli;
5) wskazówki metodyczne, w odniesieniu do określenia sposobu i technik przeprowadzania kontroli, zwłaszcza problemów, na które należy zwrócić szczególną uwagę w badaniach kontrolnych, dowodów niezbędnych do dokonania ustaleń i sposobu ich badania, powiązania tematyki z aktami normatywnymi, wskazówek o charakterze techniczno-organizacyjnym, wzorów wykazów i zestawień;
6) ewentualne wskazanie potrzeby zasięgnięcia opinii biegłego lub powołania specjalisty;
7) szczegółowe założenia organizacyjne kontroli, w tym wskazanie kontrolera mającego ją przeprowadzić.

§ 8. 1. Kontroler przeprowadza kontrolę na podstawie imiennego upoważnienia określającego jednostkę kontrolowaną i podstawę prawną do podjęcia kontroli, wystawionego przez upoważnionego funkcjonariusza ABW lub funkcjonariusza albo żołnierza SKW.

2. Upoważnienie sporządza się w jednym egzemplarzu, który załącza się do akt kontroli.

3. Upoważnienie podlega ścisłemu ewidencjonowaniu.

4. Wzór upoważnienia stanowi załącznik nr 1 do rozporządzenia.

§ 9. 1. Kontroler dokumentuje przebieg i wyniki czynności kontrolnych, zakładając i prowadząc w tym celu akta kontroli.

2. Akta kontroli obejmują w szczególności materiały dowodowe oraz inne dokumenty wymienione w rozporządzeniu, które oznacza się klauzulą tajności, zgodnie z wymogami określonymi w ustawie.

3. Akta kontroli prowadzi się zgodnie z tokiem dokonywanych czynności, włączając do nich materiały dowodowe oraz protokół kontroli, wystąpienie pokontrolne, informację o wykorzystaniu uwag i wykonaniu wniosków zawartych w wystąpieniu. Strony akt powinny być ponumerowane, ponadto akta muszą być zszyte i umieszczone w teczce. Całość klasyfikuje się według dokumentu o najwyższej klauzuli tajności. Akta kontroli rejestruje się w ewidencji kontroli.

4. Na początku każdego tomu akt zamieszcza się wykaz dokumentacji zawartej w danym tomie, wymieniając nazwy dokumentów i wskazując odpowiednie strony akt.

§ 10. 1. Zabezpieczenie materiału dowodowego zebranego w toku postępowania kontrolnego w postaci dokumentu lub rzeczy potwierdza się protokołem zabezpieczenia dokumentu lub rzeczy stanowiących materiał dowodowy, a ich zwrot potwierdza się pokwitowaniem.

2. Wzór protokołu zabezpieczenia dokumentu lub rzeczy stanowiących materiał dowodowy stanowi załącznik nr 2 do rozporządzenia.

§ 11. 1. Załączniki do protokołu oględzin utrwalone za pomocą aparatury i środków technicznych służących do utrwalania obrazu lub dźwięku zabezpiecza się w sposób uniemożliwiający ich zamianę na inne.

2. Wzór protokołu oględzin stanowi załącznik nr 3 do rozporządzenia.

§ 12. 1. Warunkiem przyjęcia przez kontrolera wyjaśnienia lub oświadczenia jest wskazanie osoby składającej to wyjaśnienie lub oświadczenie oraz jej podpis. Warunkiem przyjęcia wyjaśnienia jest ponadto wskazanie stanowiska służbowego osoby go składającej.

2. Wzór protokołu przyjęcia ustnych wyjaśnień stanowi załącznik nr 4 do rozporządzenia.

3. Wzór protokołu przyjęcia ustnego oświadczenia stanowi załącznik nr 5 do rozporządzania.

§ 13. W razie zasięgania przez kontrolera informacji lub uzyskiwania wyjaśnień na podstawie art. 12 pkt 6 ustawy, informacje lub wyjaśnienia powinny być utrwalone na piśmie i podpisane przez osobę, która je złożyła.

§ 14. 1. Postanowienie o powołaniu biegłego wydaje upoważniony przez Szefa ABW lub Szefa SKW funkcjonariusz albo żołnierz.

2. Wzór postanowienia o powołaniu biegłego stanowi załącznik nr 6 do rozporządzenia.

§ 15. W przypadku powołania biegłego podstawą wydania przez niego opinii oraz sporządzenia szczegółowego sprawozdania z badań mających wpływ na ustalenia kontroli jest umowa zawarta między biegłym a upoważnionym przez Szefa ABW lub Szefa SKW funkcjonariuszem albo żołnierzem, określająca wzajemne prawa i obowiązki stron, w szczególności przedmiot badań, ich zakres, termin sporządzenia opinii i sprawozdania oraz wysokość wynagrodzenia.

§ 16. 1. Postanowienie o powołaniu specjalisty wydaje kontroler.

2. Dokumenty sporządzone przez kontrolera, utrwalające przebieg czynności dokonanych przy udziale specjalisty, podpisują kontroler oraz specjalista.

3. Wzór postanowienia o powołaniu specjalisty stanowi załącznik nr 7 do rozporządzenia.

§ 17. Kontroler niezwłocznie informuje kierownika jednostki kontrolowanej o faktach, które mogą mieć bezpośredni wpływ na bezpieczeństwo informacji niejawnych. Pisemne potwierdzenie przekazania informacji dołącza się do akt kontroli.

§ 18. 1. Dokonane w toku kontroli ustalenia kontroler opisuje w protokole kontroli.

2. Protokół kontroli oprócz danych zawartych w art. 53 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.) powinien zawierać:

1) oznaczenie jednostki kontrolowanej, jej adres, imię i nazwisko kierownika, z uwzględnieniem zmian w okresie objętym kontrolą;

2) stopień, imię i nazwisko kontrolera, nazwę organu prowadzącego kontrolę oraz numer i datę upoważnienia do kontroli;

3) datę rozpoczęcia i zakończenia czynności kontrolnych, z wymienieniem dni przerw w kontroli;

4) określenie zakresu i przedmiotu kontroli oraz okresu objętego kontrolą;

5) opis stwierdzonego w wyniku kontroli stanu faktycznego, w tym ustalonych nieprawidłowości, z uwzględnieniem przyczyn ich powstania i zakresu;

6) wzmiankę o prawie, sposobie i terminie zgłoszenia zastrzeżeń co do ustaleń zawartych w protokole oraz o prawie odmowy podpisania protokołu, a także o prawie złożenia wyjaśnień, o których mowa w art. 59 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli;

7) adnotację o dokonaniu wpisu do księgi ewidencji kontroli, jeżeli taka księga jest prowadzona przez jednostkę kontrolowaną;

8) adnotację o dokonanych w protokole kontroli poprawek, skreśleń i uzupełnień;

9) oznaczenie miejsca i daty podpisania protokołu;

10) podpisy kontrolera i kierownika jednostki kontrolowanej na ostatniej stronie;

11) parafy kontrolera i kierownika jednostki kontrolowanej na każdej stronie protokołu.

3. Protokół kontroli sporządza się w dwóch egzemplarzach. Jeden egzemplarz protokołu otrzymuje kierownik jednostki kontrolowanej, a drugi załącza się do akt kontroli.

4. Wyjaśnienia, o których mowa w art. 59 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli, stanowią załącznik do protokołu kontroli.

§ 19. 1. Kierownikowi jednostki kontrolowanej lub osobie przez niego upoważnionej przysługuje prawo zgłoszenia, przed podpisaniem protokołu kontroli, umotywowanych zastrzeżeń co do ustaleń zawartych w protokole.

2. Zastrzeżenia należny zgłosić na piśmie w terminie 14 dni od dnia otrzymania protokołu kontroli.

3. Kontroler poddaje analizie zgłoszone zastrzeżenia i jeśli zachodzi potrzeba podejmuje dodatkowe czynności. W przypadku stwierdzenia zasadności zgłoszonych zastrzeżeń kontroler sporządza aneks do protokołu kontroli w brzmieniu:

a) „skreśla się ustalenia na str. …….";

b) „uzupełnia się ustalenia ze str. …. o treść: ……:;

c) „treść ze strony …. otrzymuje brzmienie: ……".

4. W razie nieuwzględnienia zastrzeżeń w całości kontroler przekazuje kierownikowi jednostki kontrolowanej swoje stanowisko.

5. Zastrzeżenia, o których mowa w art. 56 ust. 1 ustawy o NIK rozpatruje odpowiednio Szef ABW lub Szef SKW.

6. Zastrzeżenia do ustaleń zawartych w protokole kontroli dotyczącym kontroli przeprowadzanej w Sejmie Rzeczypospolitej Polskiej lub Senacie Rzeczypospolitej Polskiej rozpatruje Szef ABW.

§ 20. 1. Kierownik jednostki kontrolowanej lub osoba przez niego upoważniona może odmówić podpisania protokołu kontroli, składając w terminie 7 dni od dnia jego otrzymania pisemne wyjaśnienie tej odmowy.

2. W razie zgłoszenia zastrzeżeń, o których mowa w § 19, termin do złożenia wyjaśnienia o odmowie podpisania protokołu liczy się od dnia otrzymania stanowiska w sprawie rozpatrzenia tych zastrzeżeń.

§ 21. 1. Po podpisaniu protokołu kontroli kontroler opracowuje wystąpienie pokontrolne do kierownika jednostki kontrolowanej zawierające ocenę kontrolowanej działalności, w tym wskazanie osób odpowiedzialnych za tę działalność, a w razie stwierdzenia nieprawidłowości, także uwagi i wnioski w sprawie ich usunięcia. W wystąpieniu zawarta jest ponadto informacja o prawie kierownika jednostki kontrolowanej do złożenia zastrzeżeń, a także o terminie nadesłania informacji o sposobie wykorzystania ocen, uwag i wniosków zawartych w wystąpieniu oraz o terminie ponownej kontroli.

2. Jeżeli wyniki kontroli wskazują na konieczność podjęcia określonych czynności przez jednostkę nadrzędną wystąpienie, o którym mowa w ust. 1 przekazuje się kierownikowi jednostki nadrzędnej nad jednostką kontrolowaną.

3. Ocenę wskazującą na niezasadność zajmowania stanowiska lub pełnienia funkcji przez osobę odpowiedzialną za stwierdzone nieprawidłowości w jednostce kontrolowanej, wraz ze szczegółowym uzasadnieniem, kontroler przedstawia w wystąpieniu pokontrolnym właściwej jednostce organizacyjnej lub właściwemu organowi.

§ 22. Wystąpienie pokontrolne podpisuje upoważniony odpowiednio przez Szefa ABW lub Szefa SKW funkcjonariusz albo żołnierz.

§ 23. 1. Kierownik jednostki kontrolowanej lub organ, któremu przekazano wystąpienie pokontrolne, może w terminie 7 dni od dnia jego otrzymania zgłosić umotywowane

zastrzeżenia w sprawie zawartych w nim ocen, uwag i wniosków odpowiednio do Szefa ABW lub Szefa SKW.

2. Zastrzeżenia do wystąpienia pokontrolnego rozpatruje odpowiednio Szef ABW lub Szef SKW.

3. Jeżeli stwierdzone w wyniku kontroli nieprawidłowości wskazują na konieczność podjęcia działań przez właściwe organy państwowe lub samorządowe, w szczególności w celu zmiany obowiązującego prawa, kontroler opracowuje wystąpienie pokontrolne do tych organów.

§ 24. Kierownik jednostki kontrolowanej lub organ, któremu przekazano wystąpienie pokontrolne, jest obowiązany, w terminie określonym w wystąpieniu, poinformować Szefa ABW lub Szefa SKW o sposobie wykorzystania uwag i wniosków oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

§ 25. Informacje o wynikach przeprowadzonych kontroli Szef ABW lub Szef SKW przekazuje Przewodniczącemu Kolegium do Spraw Służb Specjalnych, a w razie potrzeby innym właściwym organom.

§ 26. Informacja o wynikach przeprowadzonych kontroli zawiera w szczególności:

1) określenie jednostki kontrolowanej, celu kontroli, jej zakresu, czasu przeprowadzenia i okresu objętego kontrolą;
2) istotne ustalenia kontroli ukazujące skalę stwierdzonych zjawisk, przyczyny ich powstania, skutki, jakie wywołują lub mogą wywołać, w odniesieniu do stanu zabezpieczenia informacji niejawnych;
3) ogólną ocenę oraz wynikające z niej uwagi i wnioski, zwłaszcza co do stosowania lub dokonania zmian obowiązującego prawa bądź podjęcia określonych działań organizacyjnych.

§ 27. Traci moc rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową (Dz. U. Nr 171, poz. 1430).

§ 28. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezes Rady Ministrów

Załącznik nr 1 do Rozporządzenia

……. dnia ……..

.....
pieczęć nagłówkowa
Agencji Bezpieczeństwa Wewnętrznego
lub Służby Kontrwywiadu Wojskowego

UPOWAŻNIENIE Nr ……..

Na podstawie art. ……. ustawy z dnia …… o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz.U. Nr …….) upoważniam Pana/Panią

…….....
stopień, imię i nazwisko kontrolera

do przeprowadzenia kontroli

.....
oznaczenie i temat kontroli

.....
nazwa i adres jednostki kontrolowanej

Wyżej wymieniony(a) jest upoważniony(a) do dostępu do informacji niejawnych stanowiących tajemnicę państwową do klauzuli „ściśle tajne".

Upoważnienie niniejsze ważne jest za okazaniem legitymacji służbowej.

Ważność upoważnienia upływa z dniem …….…….....

m.p.

.....
imienna pieczęć i podpis osoby wydającej upoważnienie

Ważność upoważnienia przedłuża się do dnia .....

m.p.

.....
imienna pieczęć i podpis osoby wydającej upoważnienie

Załącznik nr 2 do Rozporządzenia

..... …….. dnia ……..
pieczęć nagłówkowa
Agencji Bezpieczeństwa Wewnętrznego
lub Służby Kontrwywiadu Wojskowego

Protokół zabezpieczenia dokumentu lub rzeczy stanowiących materiał dowodowy

Na podstawie art. ……. ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. …….) w związku z art. 38 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.)

……..
stopień, imię i nazwisko kontrolera

działając w obecności ……..
imię, nazwisko i stanowisko służbowe osoby uczestniczącej w zabezpieczeniu dokumentu/rzeczy

dokonał(a) w dniu ……
zabezpieczenia dokumentu/rzeczy* w postaci
……..
dokładny opis zabezpieczonego dokumentu/rzeczy
……..
……..
……..

Dokument/rzecz* został(a) zabezpieczony(a) poprzez

……..
sposób zabezpieczenia dokumentu/rzeczy*, uniemożliwiający zastąpienie go/jej inną

……..
……..
……..
……..

……. dnia ……..

....
podpis osoby uczestniczącej (podpis kontrolera)
w zabezpieczeniu dokumentu/rzeczy

Załącznik nr 3 do Rozporządzenia

.....
pieczęć nagłówkowa
Agencji Bezpieczeństwa Wewnętrznego
lub Służby Kontrwywiadu Wojskowego

Protokół oględzin

Na podstawie art. ……. ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. …….) w związku z art. 39 ust. 3 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.)

……..
stopień, imię i nazwisko kontrolera

działając w obecności ……..
imię, nazwisko i stanowisko służbowe osoby uczestniczącej w oględzinach

……

dokonał(a) w dniu ……

……..

……..
określenie przedmiotu

w wyniku których ustalono, co następuje:

……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..

……..
……..
W toku oględzin dokonano utrwalenia stanu ……..
……..
……..
……..
……..
……..
……..
za pomocą ..……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
który (które)* stanowi (stanowią)* załącznik (załączniki)* do protokołu.

……. dnia ……..

....
podpis osoby uczestniczącej w oględzinach (podpis kontrolera)

* Niepotrzebne skreślić.

Załącznik nr 4 do Rozporządzenia

.....
pieczęć nagłówkowa
Agencji Bezpieczeństwa Wewnętrznego
lub Służby Kontrwywiadu Wojskowego

Protokół przyjęcia ustnych wyjaśnień

Na podstawie art. ……. ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. …….) w związku z art. 40 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.)

……..
stopień, imię i nazwisko kontrolera

w dniu …….. uprzedził(a) ..……

……..
imię, nazwisko i stanowisko służbowe składającego wyjaśnienia

……

o treści art. …….. ustawy z dnia …….. o ochronie informacji niejawnych oraz o zmianie niektórych innych ustaw oraz art. 40 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli oraz przyjął od niego ustne wyjaśnienia w sprawie ……..
……..
……..
……..
……..
……..
……..
o następującej treści …..……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..

……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..

Przed podpisaniem składający wyjaśnienia zapoznał(a) się z treścią niniejszego protokołu.

……. dnia …….

....
podpis osoby składającej wyjaśnienia (podpis kontrolera)

Załącznik nr 5 do Rozporządzenia

.....
pieczęć nagłówkowa
Agencji Bezpieczeństwa Wewnętrznego
lub Służby Kontrwywiadu Wojskowego

Protokół przyjęcia ustnego oświadczenia

Na podstawie art. ……. ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. …….) w związku z art. 41 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.)

……..
stopień, imię i nazwisko kontrolera

w dniu …….. przyjął (przyjęła) od ……..……...…
imię, nazwisko składającego oświadczenie

……..

ustne oświadczenie w sprawie ……..……..
……..
……..
……..
……..
……..
……..
o następującej treści …..……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..

……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..
……..

Przed podpisaniem składający oświadczenie zapoznał(a) się z treścią niniejszego protokołu.

……. dnia …….

.....
podpis osoby składającej wyjaśnienia

.....
(podpis kontrolera)

Załącznik nr 6 do Rozporządzenia

.....
pieczęć nagłówkowa
Agencji Bezpieczeństwa Wewnętrznego
lub Służby Kontrwywiadu Wojskowego

…… dnia ……

Postanowienie o powołaniu biegłego

Na podstawie art. ……. ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. …….) w związku z art. 49 ust. 1 i 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.) powołuję biegłego z dziedziny …….

……..

w osobie ...……

dla zbadania ……..

przedmiot i zakres badań

oraz sporządzenia szczegółowego sprawozdania z przeprowadzonych badań i wydania na ich podstawie opinii w terminie do dnia ……..

.....
stopień, imię i nazwisko oraz podpis upoważnionego
przez Szefa Agencji Bezpieczeństwa Wewnętrznego
lub Służby Kontrwywiadu Wojskowego
funkcjonariusza albo żołnierza

Załącznik nr 7 do Rozporządzenia

..... …… dnia ……

pieczęć nagłówkowa
Agencji Bezpieczeństwa Wewnętrznego
lub Służby Kontrwywiadu Wojskowego

Postanowienie o powołaniu specjalisty do udziału w czynnościach badawczych

Na podstawie art. ……. ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. ……..) w związku z art. 49 ust. 4 i 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701, z późn. zm.) powołuję specjalistę w dziedzinie ……

w osobie ...……

do uczestniczenia w dniu (dniach) ……...……..

w ……..

……..

miejsce i przedmiot czynności badawczych

.....
stopień, imię i nazwisko oraz podpis kontrolera

UZASADNIENIE

Rozporządzenie Prezesa Rady Ministrów w sprawie szczegółowego trybu przygotowania i prowadzenia przez Agencję Bezpieczeństwa Wewnętrznego i Służbę Kontrwywiadu Wojskowego kontroli w zakresie ochrony informacji niejawnych stanowi realizację upoważnienia ustawowego zawartego w art. 16 ust. 6 ustawy z dnia …….. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. ……..).

W rozporządzeniu doprecyzowano niektóre zapisy, głównie dotyczące trybu zgłaszania zastrzeżeń do protokołu kontroli i wystąpienia pokontrolnego oraz zmieniono niektóre zapisy powielające niektóre czynności.

W § 19 szczegółowo został przedstawiony tryb zgłaszania zastrzeżeń do protokołu kontroli, ich rozpatrywania, w tym także szczegółowo opisana forma przedstawiania stanowiska w sprawie rozpatrzenia zastrzeżeń. Podobnie doprecyzowano zapisy w § 22-23 dotyczące trybu zgłaszania i rozpatrywania zastrzeżeń do wystąpień pokontrolnych. Przyjęto, że zastrzeżenia do protokołu kontroli rozpatruje w pierwszej kolejności kontroler, który przedstawia swoje stanowisko kierownikowi jednostki kontrolowanej. Przyjęto także, że wystąpienia pokontrolne podpisują upoważnieni funkcjonariusze ABW lub funkcjonariusze albo żołnierze SKW. Decyzje ostateczne w kwestiach rozstrzygnięć zgłoszonych zastrzeżeń zarówno do protokołów kontroli jak też wystąpień pokontrolnych podejmują odpowiednio Szef ABW lub Szef SKW.

Zmianie uległy zapisy dotyczące zatwierdzania programów kontroli planowych. Dotychczas wszystkie programy kontroli, w tym także planowe zatwierdzał odpowiednio Szef ABW lub Szef SKW. Po nowelizacji program kontroli planowej będzie zatwierdzał upoważniony funkcjonariusz ABW lub funkcjonariusz albo żołnierz SKW. Zmiana taka wyeliminuje konieczność dwukrotnego zatwierdzania przez Szefa ABW lub Szefa SKW programów kontroli planowych (Szef ABW lub Szef SKW zatwierdzają roczny plan kontroli planowych - § ust. 1).

Bez zmian merytorycznych pozostawione zostały załączniki do rozporządzenia – uwzględniono jedynie zmiany wynikające z przepisów ustawy.

44-02-aa

Projekt

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia _____ r.

w sprawie sposobu i trybu przekazywania informacji oraz sposobu udzielania pomocy instytucjom i służbom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego

(Dz. U. z dnia _____ r.)

Na podstawie art. 13 ust. 4 ustawy z dnia _____ r. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. z _____ r. Nr ____, poz. ____) zarządza się, co następuje:

§ 1. Rozporządzenie określa szczegółowy zakres, warunki i tryb:

1) przekazywania przez kierowników jednostek organizacyjnych służbom lub organom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających albo postępowań bezpieczeństwa przemysłowego, zwanym dalej „uprawnionymi służbami lub organami", informacji oraz udostępniania im dokumentów niezbędnych do stwierdzenia, czy osoba objęta postępowaniem sprawdzającym, zwana dalej „osobą sprawdzaną", daje rękojmię zachowania tajemnicy albo do potwierdzenia zdolności przedsiębiorcy do ochrony informacji niejawnych;
2) udzielania przez Centralne Biuro Antykorupcyjne, Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy kontroli skarbowej, zwanych dalej „służbami współdziałającymi", niezbędnej pomocy uprawnionym służbom lub organom przy wykonywaniu czynności w ramach prowadzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających albo postępowań bezpieczeństwa przemysłowego.

§ 2. Uprawnione służby lub organy zwracają się z pisemnym wnioskiem do kierownika jednostki organizacyjnej o przekazanie informacji oraz udostępnienie niezbędnych dokumentów w celu weryfikacji danych zawartych w ankiecie bezpieczeństwa osobowego albo kwestionariuszu bezpieczeństwa przemysłowego.

§ 3. Wniosek, o którym mowa w § 2, powinien zawierać:

1) określenie uprawnionej służby lub organu prowadzącego postępowanie sprawdzające, kontrolne postępowanie sprawdzające albo postępowanie bezpieczeństwa przemysłowego i występującego z wnioskiem;
2) datę i miejsce sporządzenia wniosku;
3) podstawę prawną;
4) niezbędne dane identyfikacyjne osoby sprawdzanej lub przedsiębiorcy, którego wniosek dotyczy, w tym:

a) imię, nazwisko lub nazwisko rodowe osoby sprawdzanej albo nazwę przedsiębiorcy
b) imię ojca osoby sprawdzanej,

c) datę i miejsce urodzenia osoby sprawdzanej;
5) w zależności od potrzeb, dane dotyczące:
a) miejsca zamieszkania osoby sprawdzanej albo adresu przedsiębiorcy,
b) numeru i serii dowodu osobistego lub innego dokumentu, na podstawie którego można ustalić tożsamość osoby sprawdzanej,
c) obywatelstwa osoby sprawdzanej,
d) numeru ewidencyjnego Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) osoby sprawdzanej lub Numeru Identyfikacji Podatkowej (NIP) osoby sprawdzanej albo przedsiębiorcy;
6) określenie dokumentów lub informacji potwierdzających dane, o których mowa w § 2;
7) imienną pieczęć i podpis właściwego pracownika, funkcjonariusza lub żołnierza upoważnionego przez szefa uprawnionej służby lub organu, kierującego wniosek.

§ 4. 1. Przekazanie informacji oraz udostępnianie dokumentów, o których mowa w § 3 pkt 6, polega na:
1) niezwłocznym przesłaniu, nie później jednak niż w terminie 14 dni od dnia otrzymania wniosku, odpisu, wypisu, wyciągu lub uwierzytelnionej kopii niezbędnych dokumentów albo informacji określonych we wniosku;
2) udostępnieniu do wglądu, upoważnionemu pracownikowi, funkcjonariuszowi lub żołnierzowi uprawnionej służby lub organu, niezbędnych dokumentów w siedzibie jednostki organizacyjnej.
2. W celu uzyskania dostępu do dokumentów, o których mowa w ust. 1 pkt 2, upoważniony pracownik, funkcjonariusz lub żołnierz uprawnionej służby lub organu jest obowiązany okazać:
1) imienne upoważnienie, wydane przez szefa uprawnionej służby lub organu, którego wzór stanowi załącznik do rozporządzenia;
2) legitymację służbową.

§ 5. Upoważnienie, o którym mowa w § 4 ust. 2 pkt 1, sporządza się w dwóch egzemplarzach, z których jeden przekazuje się kierownikowi jednostki organizacyjnej, drugi włącza się do akt postępowania.

§ 6. W szczególnie uzasadnionych przypadkach, uprawnione służby lub organy mogą zwrócić się, w ramach prowadzonego postępowania, do służb współdziałających z pisemnym wnioskiem o udzielenie niezbędnej pomocy w zakresie przeprowadzenia czynności określonych w art. 26 ust. 1 pkt 2, art. 27 ust. 1 pkt 1-3 oraz art. 27 ust. 5 ustawy.

§ 7. Wniosek, o którym mowa w § 6 ust. 1, powinien zawierać:
1) określenie uprawnionej służby lub organu, prowadzącego postępowanie i występującego z wnioskiem;
2) datę i miejsce sporządzenia wniosku;
3) podstawę prawną;

4) niezbędne dane identyfikacyjne osoby, której wniosek dotyczy, o których mowa w § 3 pkt 4 i 5;
5) określenie rodzaju i zakresu pomocy;
6) imienną pieczęć i podpis właściwego pracownika, funkcjonariusza lub żołnierza upoważnionego przez szefa uprawnionej służby lub organu kierującego wniosek.

§ 8. 1. Służba współdziałająca, w terminie 30 dni od dnia otrzymania wniosku określonego w § 7, jest obowiązana przeprowadzić czynności, których wniosek dotyczy, i udzielić pisemnej odpowiedzi uprawnionej służbie lub organowi.
2. W przypadku niemożności dotrzymania terminu, o którym mowa w ust. 1, służba współdziałająca informuje o tym niezwłocznie uprawnioną służbę lub organ, określając termin, w którym czynności objęte wnioskiem mogą być przeprowadzone.

§ 9. Do składania, przekazywania i udostępniania odpowiednio wniosków informacji i dokumentów, w zakresie i trybie określonym w rozporządzeniu, mogą być wykorzystywane systemy teleinformatyczne służące do przetwarzania informacji niejawnych.

§ 10. Korespondencję i dokumentację uzyskaną przez uprawnione służby lub organ od kierownika jednostki organizacyjnej oraz służb współdziałających w toku postępowania sprawdzającego włącza się do akt postępowania.

§ 11. Rozporządzenie wchodzi w życie _____.

Prezes Rady Ministrów

ZAŁĄCZNIK

WZÓR IMIENNEGO UPOWAŻNIENIA

(pieczęć nagłówkowa organu prowadzącego postępowanie) (miejscowość, data)

UPOWAŻNIENIE Nr _____

Na podstawie art. 13 ust. 4 ustawy z dnia _____ r. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. z _____ r. Nr ____, poz. ____) upoważniam

(imię i nazwisko pracownika, funkcjonariusza lub żołnierza organu prowadzącego postępowanie sprawdzające)

do wglądu w:

(określenie dokumentu)

znajdujące się w:

(nazwa jednostki organizacyjnej)

w związku z prowadzonym postępowaniem sprawdzającym wobec:

(imię i nazwisko, data i miejsce urodzenia osoby sprawdzanej)

Upoważnienie jest ważne jedynie przy jednoczesnym okazaniu legitymacji służbowej.

m.p. (podpis i imienna pieczęć upoważnionej osoby)

UZASADNIENIE

Rozporządzenie stanowi wykonanie delegacji ustawowej wyrażonej w art. 13 ust. 4 ustawy z dnia …….. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. ……..), zwanej dalej „ustawą”.

Konieczność wydania nowego rozporządzenia Prezesa Rady Ministrów w sprawie szczegółowego zakresu, warunków i trybu współdziałania organów, służb i jednostek organizacyjnych ze służbami i organami uprawnionymi do prowadzenia poszerzonych postępowań sprawdzających albo postępowań bezpieczeństwa przemysłowego wynika z niezbędności dostosowania przepisów aktu wykonawczego do zmian wprowadzonych do systemu ochrony informacji niejawnych wraz z ustawą.

Podstawą przygotowania projektu było bazowanie na stosowanych dotychczas rozwiązaniach (w myśl zasady niezmieniania czegoś, co dobrze funkcjonuje), jednakże z dostosowaniem niektórych rozwiązań do zmienionych przepisów ustawy.

W § 1 zawarto ogólne informacje na temat podmiotów uprawnionych do zwracania się o przekazywanie informacji i udostępniania dokumentów oraz udzielenia pomocy w ramach postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego. Z uwagi na ten sam cel postępowań sprawdzających, prowadzonych zarówno przez ABW i SKW, jak i inne organy uprawnione do prowadzenia poszerzonych postępowań sprawdzających, przede wszystkim z uwagi na dbałość o skuteczne przeprowadzenie postępowania sprawdzającego (możliwość pełniejszej weryfikacji informacji), nie ma powodu do nienadania dotychczasowych uprawnień ABW i SKW innym służbom. Z tego względu zarówno w nazwie rozporządzenia, jak i w treści, dotychczasowe sformułowanie „służby ochrony państwa”, należało zastąpić sformułowaniem „służby i organy uprawnione do prowadzenia poszerzonych postępowań sprawdzających albo postępowań bezpieczeństwa przemysłowego” (dalej w treści jako „uprawnione służby lub organy”).

Takie sformułowanie pozwala także na korzystanie z rozporządzenia przy prowadzeniu przez te służby zwykłych postępowań sprawdzających wobec własnych pracowników lub kandydatów do pracy, ponieważ jego nazwa i treść odnosi się nie do rodzaju prowadzonego postępowania, ale do podmiotu uprawnionego do prowadzenia określonego rodzaju postępowań (niezależnie od rodzaju postępowania prowadzonego w danym momencie).

W całym tekście rozporządzenia wskazano, że dotyczy ono także postępowań bezpieczeństwa przemysłowego, wskazując wprost, że ma zastosowanie do postępowań prowadzonych wobec podmiotów ubiegających się o wydanie świadectwa bezpieczeństwa przemysłowego.

W § 2 zawarto określenie celu zwrócenia się o przekazanie informacji i udostępnienie materiałów w celu weryfikacji danych zawartych w ankiecie bezpieczeństwa osobowego albo kwestionariuszu bezpieczeństwa przemysłowego (wcześniej było to zwracanie się o „potwierdzenie danych o osobie sprawdzanej wskazanych w pkt. 1 ankiety i w zależności od potrzeb, pozostałych danych z ankiety”).

W § 3 zawarto wskazanie wymogów dotyczących treści wniosku o przekazanie informacji i udostępnienie materiałów w celu weryfikacji danych zawartych w ankiecie bezpieczeństwa osobowego albo kwestionariuszu bezpieczeństwa przemysłowego.

W § 4 określono tryb przekazywania informacji i udostępniania materiałów. W trosce o dotrzymanie terminu realizacji postępowań skrócono z 21 do 14 dni termin realizacji tych czynności (ust. 1 pkt 1), a do grupy osób zatrudnionych w służbach i organach prowadzących postępowania sprawdzające, którym mogą zostać udostępnione do wglądu materiały i dokumenty, dołączono – obok żołnierzy i funkcjonariuszy – także pracowników, pozostawiając służbom i organom dowolność doboru osób do realizacji tych czynności (ust. 1 pkt 2, ust. 2).

W § 5 dotyczy sporządzania i przekazywania upoważnienia do wglądu w dokumenty i materiały.

W § 6 udzielenie pomocy w ramach prowadzonego postępowania sprawdzającego ograniczono tylko do szczególnie uzasadnionych przypadków (ust. 1). Z uwagi na znaczące rozszerzenie kręgu podmiotów, uprawnionych do korzystania z rozporządzenia, zasadna jest konieczność ograniczenia obowiązku udzielania pomocy przez CBA, Policję, SG, ŻW oraz organy kontroli skarbowej wszystkim służbom i organom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających albo postępowań bezpieczeństwa przemysłowego, ponieważ „udzielana pomoc" ma mniejszy wymiar informacyjny, niż weryfikacja danych, a czynności te (rozmowy z osobami polecającymi, wywiad w miejscu zamieszkania, rozmowa z przełożonym lub innymi osobami) mogą przeprowadzić same organy w ramach prowadzonych postępowań.

Ponadto do czynności, przy których może być udzielona pomoc, dodano rozmowę z przełożonym lub innymi osobami.

Usunięto natomiast i tak dotychczasowej w praktyce martwego i *de facto* nic niewnoszącego do procedury przepisu o konieczności potwierdzania przyjęcia wniosku o udzielenie pomocy oraz informowania o terminie i zakresie pomocy.

W § 7 zawarto wskazanie wymogów dotyczących treści wniosku o udzielenie pomocy w ramach postępowań sprawdzających, a w § 8-11 – przepisy regulujące tryb udzielania pomocy i jej dokumentowanie.

Ocena Skutków Regulacji

1. **Podmioty, na które oddziałuje rozporządzenie**

Zakres oddziaływania znowelizowanych przepisów rozporządzenia jest ograniczony do podmiotów wymienionych w art. 1 ust. 2 ustawy o ochronie informacji niejawnych.

2. **Wpływ regulacji na sektor finansów publicznych, w tym na budżet państwa i budżety jednostek samorządu terytorialnego**

Wejście w życie rozporządzenia nie wywoła zwiększenia wydatków z budżetu państwa i budżetu jednostek samorządu terytorialnego.

3. **Wpływ regulacji na rynek pracy**

Wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy.

4. **Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw**

Wejście w życie rozporządzenia nie wpłynie na konkurencyjność gospodarki i przedsiębiorczość.

5. **Wpływ regulacji na sytuację i rozwój regionalny**

Wejście w życie rozporządzenia pozostanie bez wpływu na sytuację i rozwój regionalny.

6. **Zgodność z przepisami prawa Unii Europejskiej**

Przedmiotowe rozporządzenie pozostaje poza zakresem prawa Unii Europejskiej. Projekt rozporządzenia nie zawiera przepisów technicznych i w związku z tym nie podlega procedurze notyfikacji aktów prawnych, określonej w rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz.U. Nr 239, poz. 2039 i z 2004 r. Nr 65, poz. 597).

PROJEKT

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia

w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych

Na podstawie art. 18 ust. 1 ustawy z dnia o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. Nr ….., poz. ……) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) szczegółowe zadania pełnomocników ochrony w jednostkach organizacyjnych podległych i nadzorowanych przez Ministra Obrony Narodowej, zwanych dalej „jednostkami organizacyjnymi”, w tym dotyczące koordynowania oraz nadzorowania działalności pionów ochrony przez pełnomocników ochrony bezpośrednio nadrzędnych jednostek organizacyjnych;
2) sposób współdziałania, w zakresie ochrony informacji niejawnych, z właściwymi jednostkami organizacyjnymi Służby Kontrwywiadu Wojskowego;
3) organizowanie szkoleń w zakresie ochrony informacji niejawnych;
4) szczególne wymagania w zakresie stosowania środków bezpieczeństwa fizycznego ochrony informacji niejawnych w jednostkach organizacyjnych;

§ 2 Użyte w rozporządzeniu określenia oznaczają:

1) ustawa – ustawę z dnia …….. o ochronie informacji niejawnych oraz o zmianie niektórych innych ustaw;
2) komórka organizacyjna Ministerstwa Obrony Narodowej – Sekretariat Ministra Obrony Narodowej, departament, zarząd, biuro;
3) system ochrony informacji niejawnych w jednostce organizacyjnej – zespół przedsięwzięć organizacyjno-technicznych obejmujących ochronę fizyczną i techniczną informacji niejawnych w jednostce organizacyjnej.

Rozdział 2

Szczegółowe zadania pełnomocników ochrony kierowników jednostek organizacyjnych

§ 3. 1. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych realizuje w Ministerstwie Obrony Narodowej zadania wymienione w § 4 oraz koordynuje realizację zadań w zakresie ochrony informacji niejawnych przez piony ochrony jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska Ministerstwa oraz kierownikom komórek organizacyjnych Ministerstwa Obrony Narodowej i jest zobowiązany do:

1) określania, w porozumieniu z Szefem Służby Kontrwywiadu Wojskowego, propozycji dotyczących zasadniczych zadań i kierunków działania dla pionów ochrony jednostek organizacyjnych oraz przedkładania ich do akceptacji Ministrowi Obrony Narodowej;
2) kierowania pracami związanymi z opracowaniem projektów dokumentów prawnych regulujących problematykę ochrony informacji niejawnych w Ministerstwie Obrony Narodowej oraz jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej;
3) opiniowania i uzgadniania projektów dokumentów decyzyjnych (rozkazodawczych) wydawanych przez kierowników jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej przez osoby

zajmujące kierownicze stanowiska ministerstwa, regulujących problematykę ochrony informacji niejawnych w tych jednostkach;

4) wykonywania zadań związanych z realizacją funkcji gestora specjalistycznego sprzętu ochrony informacji niejawnych, w tym określanie potrzeb modernizacji i kierunków rozwoju tego sprzętu;
5) opracowywania, w porozumieniu z Szefem Służby Kontrwywiadu Wojskowego, programów szkolenia specjalistycznego dla kierowników i pracowników kancelarii tajnych, tajnych – zagranicznych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywane, obieg i udostępnianie materiałów niejawnych;
6) organizowania szkolenia:
   a) o którym mowa w art. 19 ust. 2 pkt 1 i 2 ustawy, prowadzonego przez Służbę Kontrwywiadu Wojskowego, wobec osób z jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska Ministerstwa oraz kierownikom komórek organizacyjnych Ministerstwa Obrony Narodowej,
   b) specjalistycznego z zakresu bezpieczeństwa teleinformatycznego, prowadzonego przez Służbę Kontrwywiadu Wojskowego, dla inspektorów bezpieczeństwa teleinformatycznego i administratorów systemu pełniących służbę oraz zatrudnionych w jednostkach organizacyjnych, o których mowa w lit. a,
   c) specjalistycznego dla osób pełniących służbę lub zatrudnionych w kancelariach tajnych oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych jednostek organizacyjnych, o których mowa w lit. a, z wyłączeniem dowództw rodzajów sił zbrojnych Inspektoratu Wsparcia Sił Zbrojnych, Dowództwa Garnizonu Warszawa oraz Komendy Głównej Żandarmerii Wojskowej;
7) nadzorowania działalności merytorycznej pionów ochrony, a także realizowania, kontroli stanu ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
8) uzgadniania rocznych planów zasadniczych przedsięwzięć pionów ochrony jednostek organizacyjnych, o których mowa w pkt. 6 lit. a;

9) sporządzania i przedkładania Ministrowi Obrony Narodowej okresowych analiz, sprawozdań, meldunków i wniosków dotyczących przestrzegania przepisów o ochronie informacji niejawnych w komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz jednostkach organizacyjnych, o których mowa w pkt. 7;
10) wydawania opinii w sprawach dotyczących ochrony informacji niejawnych

2. Pełnomocnicy ochrony dowódców rodzajów sił zbrojnych, Dowódcy Operacyjnego Sił Zbrojnych, Szefa Inspektoratu Wsparcia Sił Zbrojnych, Dowódcy Garnizonu Warszawa, Komendanta Głównego Żandarmerii Wojskowej, Szefa Inspektoratu Wojskowej Służby Zdrowia, dowódców okręgów wojskowych, dowódców związków taktycznych i innych osób funkcyjnych, którym podporządkowano jednostki organizacyjne realizują zadania wymienione w § 4 oraz koordynują realizację zadań w zakresie ochrony informacji niejawnych przez piony ochrony jednostek organizacyjnych podległych tym osobom, sprawują nadzór nad ich działalnością merytoryczną i są zobowiązani do:
   1) określania propozycji dotyczących zasadniczych zadań dla pionów ochrony podległych jednostek organizacyjnych oraz przedkładania ich do akceptacji swoim przełożonym;
   2) kierowania pracami związanymi z opracowaniem projektów dokumentów prawnych regulujących problematykę ochrony informacji niejawnych w podległych jednostkach organizacyjnych;
   3) uzgadniania rocznych planów zasadniczych przedsięwzięć pionów ochrony podległych jednostek organizacyjnych;
   4) nadzorowania działalności merytorycznej pionów ochrony podległych jednostek organizacyjnych, zgodnie z rocznym planem kontroli zatwierdzonym przez swojego przełożonego;
   5) sporządzania i przedkładania swoim przełożonym okresowych analiz, ocen, sprawozdań oraz wniosków dotyczących przestrzegania przepisów o ochronie informacji niejawnych i obiektów wojskowych w podległych jednostkach organizacyjnych.
3. Pełnomocnicy ochrony dowódców rodzajów sił zbrojnych, Inspektoratu Wsparcia Sił Zbrojnych, Dowódcy Garnizonu Warszawa, Komendanta Głównego Żandarmerii Wojskowej, niezależnie od przedsięwzięć wyszczególnionych w ust. 2, organizują szkolenie:

1) o którym mowa w art. 19 ust. 2 pkt 1 i 2 ustawy, prowadzone przez Służbę Kontrwywiadu Wojskowego, wobec osób z podległych jednostek organizacyjnych,
2) specjalistyczne z zakresu bezpieczeństwa teleinformatycznego, prowadzonego przez Służbę Kontrwywiadu Wojskowego dla inspektorów bezpieczeństwa teleinformatycznego i administratorów systemu pełniących służbę lub zatrudnionych w jednostkach organizacyjnych, o których mowa pkt. 1,
3) specjalistyczne dla osób pełniących służbę lub zatrudnionych w kancelariach tajnych oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przechowywanie, rejestrowanie, obieg i udostępnianie materiałów niejawnych jednostek organizacyjnych, o których mowa w pkt. 1.

§ 4. Do szczegółowych zadań pełnomocnika ochrony należy zapewnienie ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji w jednostce organizacyjnej, a zwłaszcza:

1) opracowywanie projektów dokumentów normujących ochronę informacji niejawnych w jednostce organizacyjnej, a w tym:
   a) zasady obiegu informacji niejawnych oznaczonych klauzulą „poufne”,
   b) planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego i jego uaktualnianie;
2) zapewnienie ochrony systemów i sieci teleinformatycznych funkcjonujących w jednostce organizacyjnej, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne;
3) realizacja czynności związanych z akredytacją systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”;
4) prowadzenie kontroli stanu ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji w jednostce organizacyjnej;
5) zgłaszanie potrzeb do planu ochrony jednostki organizacyjnej w zakresie ochrony fizycznej i technicznej informacji niejawnych oraz nadzorowanie realizacji zadań w tym względzie;
6) organizowanie kontroli rocznych stanu ochrony informacji niejawnych oraz szkolenie członków komisji biorących udział w tych kontrolach;
7) prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających, podejmowanie decyzji dotyczących wydania lub odmowy

wydania poświadczenia bezpieczeństwa, cofnięcia poświadczenia bezpieczeństwa, a także postanowień o umorzeniu lub zawieszeniu postępowania sprawdzającego;

8) opracowywanie programów szkolenia oraz organizacja szkolenia z zakresu ochrony informacji niejawnych dla osób pełniących służbę wojskową oraz zatrudnionych w jednostce organizacyjnej;
9) szacowanie ryzyka dla bezpieczeństwa przetwarzanych w jednostce organizacyjnej informacji niejawnych oraz zarządzanie ryzykiem;
10) zapewnienie obsługi kancelaryjnej w jednostce organizacyjnej;
11) sprawowanie nadzoru nad funkcjonowaniem kancelarii tajnej, tajnej - zagranicznej oraz innych komórek organizacyjnych, przechowujących, przetwarzających, wytwarzających, przekazujących i prowadzących ewidencję materiałów niejawnych;
12) prowadzenie wykazu stanowisk w jednostce organizacyjnej i prac zleconych, z którymi może się wiązać dostęp do informacji niejawnych;
13) prowadzenie wykazu osób zatrudnionych w jednostce organizacyjnej albo wykonujących prace zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, którym odmówiono wydania lub cofnięto poświadczenia bezpieczeństwa;
14) prowadzenie wykazu przedsiębiorców realizujących na rzecz jednostki organizacyjnej umowy lub zadania związane z dostępem do informacji niejawnych;
15) powiadamianie o tym osób upoważnionych do obsady stanowiska służbowego, Służby Kontrwywiadu Wojskowego oraz osób sprawdzanych;
16) informowanie kierownika jednostki organizacyjnej oraz pełnomocnika ochrony bezpośrednio nadrzędnej jednostki organizacyjnej o naruszeniu przepisów o ochronie informacji niejawnych, a także kierownika właściwej jednostki organizacyjnej Służby Kontrwywiadu Wojskowego w przypadku naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą „poufne” lub wyższą;
17) prowadzenie postępowań wyjaśniających okoliczności naruszenia przepisów o ochronie informacji niejawnych oraz przedstawianie wyników tych postępowań i wynikających z nich wniosków kierownikowi jednostki organizacyjnej;

18) zapewnienie ochrony fizycznej informacji niejawnych w jednostce organizacyjnej, a w tym:
    a) opracowanie planu ochrony informacji niejawnych jednostki organizacyjnej i jego bieżąca aktualizacja,
    b) sprawowanie nadzoru nad funkcjonowaniem systemu ochrony informacji niejawnych w jednostce organizacyjnej,
    c) nadawanie uprawnień do wstępu do stref ochronnych,
    d) współudział w opracowywaniu Minimalnych Wojskowych Wymagań Organizacyjno - Użytkowych oraz Programów Organizacyjno – Użytkowych dotyczących zabezpieczenia kancelarii tajnych oraz innych pomieszczeń, w których są wytwarzane, przetwarzane, przekazywane lub przechowywane materiały niejawne;
19) zapewnienie ochrony informacji niejawnych podczas ćwiczeń, treningów sztabowych, narad, odpraw i szkoleń oraz ochrona pomieszczeń, w których są one prowadzone;
20) współudział w opracowywaniu umów i instrukcji bezpieczeństwa przemysłowego dotyczących zlecenia przedsiębiorcy wykonania zadań związanych z dostępem do informacji niejawnych;
21) nadzorowanie, szkolenie i doradztwo w zakresie wykonywania przez przedsiębiorców, z którymi jednostka organizacyjna zawarła umowę, obowiązku ochrony przekazanych im informacji;
22) przedstawianie kierownikowi jednostki organizacyjnej propozycji dotyczących wyznaczenia osoby odpowiedzialnej za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę obowiązku ochrony przekazanych mu informacji niejawnych w związku z wykonywanymi umowami albo zadaniami związanymi z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą.

Rozdział 3

Zasady współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych z właściwymi jednostkami organizacyjnymi Służby Kontrwywiadu Wojskowego

§ 5. Pełnomocnicy ochrony realizując zadania w zakresie ochrony informacji niejawnych, wymienione w rozdziale 2, współdziałają na bieżąco z właściwymi jednostkami organizacyjnymi Służby Kontrwywiadu Wojskowego i informują kierowników jednostek organizacyjnych o przebiegu tego współdziałania; współdziałanie pełnomocników ochrony z SKW polega w szczególności na:

1) wymianie doświadczeń i informacji,
2) udostępnianiu pełnomocnikom ochrony przez Służbę Kontrwywiadu Wojskowego dokumentów regulujących problematykę ochrony informacji niejawnych w Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej, a także tłumaczeń tych dokumentów;
3) przekazywaniu przez Służbę Kontrwywiadu Wojskowego Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji niejawnych wyników inspekcji przeprowadzonych przez przedstawicieli organów bezpieczeństwa NATO i UE w kancelariach tajnych zagranicznych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
4) wzajemnym udostępnianiu ocen, materiałów analitycznych oraz wyników kontroli stanu ochrony informacji niejawnych przeprowadzonych w jednostkach organizacyjnych;
5) wspólnym opracowywaniu programów szkolenia i materiałów szkoleniowych;
6) zapraszaniu przedstawicieli Służby Kontrwywiadu Wojskowego do udziału w prowadzonych przez pełnomocników ochrony odprawach, szkoleniach i konferencjach,
7) udostępnianiu pełnomocnikom ochrony przez właściwe jednostki Służby Kontrwywiadu Wojskowego informacji o zagrożeniach mogących mieć wpływ na bezpieczeństwo informacji niejawnych przetwarzanych w jednostkach organizacyjnych,

8) przekazywaniu przez pełnomocników ochrony właściwym jednostkom organizacyjnym Służby Kontrwywiadu Wojskowego danych dotyczących osób uprawnionych do dostępu informacji niejawnych, osób którym odmówiono wydania poświadczenia bezpieczeństwa, lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa,
9) informowaniu właściwej jednostki organizacyjnej Służby Kontrwywiadu Wojskowego o utworzeniu lub likwidacji w jednostce organizacyjnej kancelarii tajnej,
10) informowaniu Służby Kontrwywiadu Wojskowego przez pełnomocników ochrony o zawieranych przez jednostkę organizacyjną umowach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą, zakończeniu wykonania umowy, a także przypadkach naruszenia przez przedsiębiorcę, z którym zawarto umowę przepisów o ochronie informacji niejawnych,
11) uzgadnianiu przez pełnomocników ochrony z właściwymi jednostkami organizacyjnymi Służby Kontrwywiadu Wojskowego projektów dokumentów regulujących problematykę ochrony informacji niejawnych.

Rozdział 4

Szkolenie w zakresie ochrony informacji niejawnych

§ 6. W zakresie ochrony informacji niejawnych w komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, prowadzi się następujące rodzaje szkolenia:

1) podstawowe;
2) uzupełniające;
3) specjalistyczne.

§ 7.1. Celem szkolenia podstawowego jest zapoznanie żołnierzy zawodowych, członków korpusu służby cywilnej oraz pracowników wojska z tematyką określoną w art. 19 ust. 1

ustawy, oraz ze szczegółowymi wymaganiami w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone” i „poufne” w jednostce organizacyjnej.

2. Szkolenie podstawowe organizuje i przeprowadza pełnomocnik ochrony.

3. Pełnomocnik ochrony potwierdza odbycie szkolenia podstawowego wydaniem zaświadczenia według wzoru określonego w załączniku nr ……. do rozporządzenia Prezesa Rady Ministrów z dnia ……. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych (Dz. U. Nr ……, poz. ……).

4. Osoby, które uzyskały certyfikat Unii Europejskiej (EU PERSONNEL SECURITY CLEARANCE CERTIFICATE), certyfikat Unii Zachodnioeuropejskiej (WEU SECURITY CERTIFICATE), certyfikat bezpieczeństwa NATO (NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE), certyfikat potwierdzający sprawdzenie osoby (CERTIFICATE OF SECURITY CLEARANCE), poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych Unii Europejskiej, Unii Zachodnioeuropejskiej lub NATO, podlegają przeszkoleniu z przepisów bezpieczeństwa odpowiednio Unii Europejskiej, Unii Zachodnioeuropejskiej i NATO przez Służbę Kontrwywiadu Wojskowego.

5. Służba Kontrwywiadu Wojskowego potwierdza odbycie szkolenia, o którym mowa w ust. 4, wydaniem stosownego zaświadczenia odpowiednio według wzorów określonych w załącznikach do rozporządzenia Prezesa Rady Ministrów z dnia ……. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych (Dz. U. Nr ……, poz. ……).

§ 8. Celem szkolenia uzupełniającego jest podtrzymanie i uaktualnianie wiedzy uzyskanej podczas szkolenia podstawowego w zakresie ochrony informacji niejawnych.

§ 9. Za opracowanie planu szkolenia podstawowego i uzupełniającego oraz prowadzenie dokumentacji szkoleniowej odpowiada pełnomocnik ochrony.

§ 10.1. Szkoleniem specjalistycznym obejmuje się osoby przewidziane do objęcia stanowiska lub pełnienia funkcji:

1) pełnomocnika ochrony i zastępcy pełnomocnika ochrony;
2) administratora systemu teleinformatycznego;
3) pracownika pionu ochrony pełniącego funkcję inspektora bezpieczeństwa teleinformatycznego;

4) kierownika, zastępcy kierownika i kancelisty kancelarii tajnej, tajnej – zagranicznej oraz innych niż kancelaria tajna komórek wewnętrznych lub organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych.

2. Celem szkolenia specjalistycznego jest przygotowanie osób, o których mowa w ust. 1, do wykonywania obowiązków służbowych.
3. Programy szkolenia specjalistycznego osób, o których mowa w ust.1 pkt 1- 3 opracowuje Służba Kontrwywiadu Wojskowego.
4. Program szkolenia specjalistycznego osób, o których mowa w ust.1 pkt 4, opracowuje Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych w porozumieniu ze Służbą Kontrwywiadu Wojskowego i przekazuje go odpowiednio osobom, o których mowa w § 3 ust. 3.
5. Szkolenie osób wymienionych w ust. 1 pkt 1- 3 prowadzą wyłącznie żołnierze lub funkcjonariusze Służby Kontrwywiadu Wojskowego;
6. Służba Kontrwywiadu Wojskowego potwierdza odbycie szkolenia specjalistycznego przez osoby, o których mowa w ust. 1 pkt 1- 3 wydaniem zaświadczenia według właściwego wzoru określonego w załącznikach do rozporządzenia Prezesa Rady Ministrów z dnia ……. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych (Dz. U. Nr ……, poz. ……).
7. Ukończenie szkolenia specjalistycznego przez osoby, o których mowa w ust. 1 pkt 4, pełnomocnicy ochrony dokumentują odpowiednio wydaniem zaświadczenia, według wzoru określonego w załączniku Nr …. do rozporządzenia.

Rozdział 5

Szczególne wymagania w zakresie stosowania środków bezpieczeństwa fizycznego ochrony informacji niejawnych

§ 11. W celu zapewnienia skutecznej ochrony informacji niejawnych, w jednostce organizacyjnej stosuje się środki bezpieczeństwa fizycznego oraz wydziela strefy ochronne, w tym także określa pomieszczenia, w których są przetwarzane informacje niejawne i obiekty (rejony) podlegające szczególnej ochronie.

§ 12. System ochrony informacji niejawnych w jednostce organizacyjnej realizuje się przez ochronę fizyczną oraz przy wykorzystaniu technicznych środków ją wspomagających.

§ 13.1. Zakres stosowania środków bezpieczeństwa fizycznego powinien być dostosowany do poziomu zagrożenia nieuprawnionego dostępu do informacji niejawnych, wynikającego z przeprowadzonej analizy.

2. Zastosowane w ochronie informacji niejawnych systemy powinny posiadać deklarację zgodności ich wykonania w odpowiedniej klasie, natomiast urządzenia wykorzystane do ich budowy odpowiednie certyfikaty lub świadectwa kwalifikacyjne. Systemy i urządzenia powinny spełniać parametry określone w normie obronnej NO-04-A004 – Obiekty wojskowe. Systemy alarmowe.
3. Zainstalowane systemy i urządzenia alarmowe powinny być remontowane, konserwowane i poddawane przeglądom technicznym zgodnie z normą obronną NO-04-A004-8 Obiekty wojskowe. Systemy alarmowe. Eksploatacja.

§ 14.1. W jednostce organizacyjnej, w której są przetwarzane materiały niejawne, wydziela się strefy ochronne: administracyjną, klasy I i klasy II, a także określa pomieszczenia i obiekty (rejony) podlegające szczególnej ochronie.

2. Strefę ochronną - administracyjną stanowi obszar przylegający do stref ochronnych, o których mowa w ust. 1, w którym jest zapewniona kontrola ruchu osób i pojazdów.
3. Strefę ochronną klasy I – stanowi oznaczony i chroniony obszar, obiekt, kompleks, budynek, a także fragment budynku, w którym informacje niejawne o klauzuli „poufne” lub wyższej są przetwarzane w taki sposób, że wejście do niego może wiązać się z bezpośrednim dostępem do tych informacji; w strefie tej mogą pracować lub pełnić służbę osoby posiadające poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli odpowiadającej co najmniej klauzuli najwyżej sklasyfikowanej informacji przetwarzanej w tym obszarze; wstęp osób nie będących żołnierzami albo pracownikami komórki organizacyjnej objętej strefą (interesantów) może nastąpić po uzyskaniu zgody kierownika tej komórki i pod nadzorem upoważnionego przez niego żołnierza lub pracownika, pod warunkiem zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie;
4. Strefę ochronną klasy II – stanowi oznaczony i chroniony obszar, obiekt, kompleks, budynek, a także fragment budynku, w którym informacje niejawne o klauzuli „poufne” lub wyższej są przetwarzane w taki sposób, że wejście do strefy nie wiąże się z bezpośrednim dostępem do tych informacji; w strefie tej mogą pracować lub pełnić

służbę osoby posiadające poświadczenie bezpieczeństwa uprawniające co najmniej do dostępu do informacji niejawnych oznaczonych klauzulą „poufne”; wstęp osób nie będących żołnierzami albo pracownikami komórki organizacyjnej objętej strefą (interesantów) może nastąpić po uzyskaniu zgody kierownika tej komórki lub uprawnionej przez niego osoby i pod nadzorem upoważnionego żołnierza lub pracownika, pod warunkiem zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie.

5. Na czas sprzątania i wykonywania prac remontowych użytkownicy pomieszczeń objętych strefą ochronną mają obowiązek zabezpieczenia dokumentów niejawnych w sposób uniemożliwiający przypadkowe ujawnienie ich treści osobom nieuprawnionym; sprzątanie oraz wykonywanie prac remontowych w pomieszczeniach objętych strefą ochronną może odbywać się jedynie w obecności użytkowników tych pomieszczeń.
6. W przypadku, gdy prace, których mowa w ust. 5, wiążą się z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej, personel sprzątający lub techniczny powinien posiadać poświadczenia bezpieczeństwa odpowiednie do klauzuli tych informacji; jeżeli prace porządkowe lub remontowe wykonuje podmiot zewnętrzny, powinien on posiadać stosowne świadectwo bezpieczeństwa przemysłowego.
7. W stosunku do osób pełniących służby wewnątrz strefy ochronnej klasy I, przepis ust. 3 stosuje się odpowiednio, natomiast osoby pełniące służbę ochronną w strefie ochronnej klasy II powinny posiadać poświadczenia bezpieczeństwa uprawniające co najmniej do informacji niejawnych oznaczonych klauzulą „poufne”.
8. Pomieszczenia i obiekty znajdujące się w strefie ochronnej klasy I zalicza się do pomieszczeń i obiektów podlegających szczególnej ochronie.

§ 15.1. Dokumentami uprawniającymi do wejścia do strefy ochronnej - administracyjnej są: przepustki stałe, okresowe, jednorazowe, elektroniczne karty dostępu lub inne identyfikatory, imienne upoważnienia do wykonywania czynności kontrolnych, legitymacje służbowe pracowników Najwyższej Izby Kontroli, Państwowej Inspekcji Pracy, legitymacje poselskie lub senatorskie oraz zezwolenia stałe i jednorazowe wydawane przedstawicielom placówek dyplomatycznych państw obcych.

2. Dokumentami uprawniającymi do wjazdu na teren strefy ochronnej - administracyjnej są przepustki samochodowe lub rozkazy wyjazdu w odniesieniu do pojazdów pozostających na wyposażeniu danej jednostki organizacyjnej.

3. Dokumenty, o których mowa w ust. 1, uprawniają również do wejścia do stref ochronnych bezpieczeństwa klasy I i II, na zasadach określonych przez kierownika jednostki organizacyjnej.
4. Wejścia do strefy ochronnej oraz wyjścia z niej osób nie będących żołnierzami lub pracownikami jednostki albo komórki organizacyjnej (interesantów) powinny być rejestrowane, a ewidencja przechowywana przez co najmniej jeden rok.

§ 16. 1. Strefy ochronne oznacza się w następujący sposób:

1) strefę ochronną klasy I:
   a) w przypadku pojedynczych pomieszczeń – tablicą w kształcie prostokąta o podstawie 19 cm i wysokości 13 cm z napisem koloru czarnego „Strefa ochronna klasy I” o wysokości liter 1 cm na czerwonym tle,
   b) w pozostałych przypadkach (obszar, obiekt, fragment budynku, kilka pomieszczeń) – linią ciągłą koloru czerwonego szerokości 10 cm oraz tablicą w kształcie prostokąta o podstawie 29,5 cm i wysokości 21 cm z napisem koloru czarnego „Strefa ochronna klasy I” o wysokości liter 1,7 cm na czerwonym tle;
2) strefę ochronną klasy II:
   a) w przypadku pojedynczych pomieszczeń – tablicą w kształcie prostokąta o podstawie 19 cm i wysokości 13 cm z napisem koloru czarnego „Strefa ochronna klasy II” o wysokości liter 1 cm na żółtym tle,
   b) w pozostałych przypadkach (obszar, obiekt, fragment budynku, kilka pomieszczeń) – linią ciągłą koloru żółtego szerokości 10 cm oraz tablicą w kształcie prostokąta o podstawie 29,5 cm i wysokości 21 cm z napisem koloru czarnego „Strefa ochronna klasy II” o wysokości liter 1,7 cm na żółtym tle.

2. Tablice, o których mowa w ust. 1, umieszcza się:
   1) w przypadku pojedynczych pomieszczeń – na drzwiach wejściowych do pomieszczeń lub na ścianie przy drzwiach wejściowych;
   2) w pozostałych przypadkach (obszar, obiekt, fragment budynku, kilka pomieszczeń) - na drzwiach wejściowych do stref, na ścianach przy wejściu do stref lub na specjalnych stojakach.
3. Linie, o których mowa w ust. 1, maluje się przed wejściem do obszaru, obiektu lub fragmentu budynku na całej jego szerokości.

Rozdział 5

Planowanie ochrony informacji niejawnych. Elementy planu ochrony informacji niejawnych.

§ 17. 1. Ochrona informacji niejawnych w jednostce organizacyjnej jest organizowana i realizowana na podstawie planu ochrony informacji niejawnych.

2. Plan ochrony informacji niejawnych w jednostce organizacyjnej opracowuje w 2 egzemplarzach pełnomocnik ochrony, w porozumieniu z kierownikami komórek organizacyjnych, a zatwierdza kierownik jednostki organizacyjnej. Planowi ochrony przyznaje się klauzulę tajności stosowną do treści zawartych w nim informacji.

§ 18. 1. Plan ochrony informacji niejawnych składa się z części graficznej i opisowej.

2. W części graficznej przedstawia się rozmieszczenie:
   1) budynków (pomieszczeń), z wyróżnieniem tych, w których są przetwarzane materiały niejawne. Wszystkie budynki przedstawia się w formie rzutu płaskiego z góry i opisuje się je;
   2) technicznych środków wspomagających ochronę fizyczną informacji niejawnych,
   3) stref ochronnych oraz pomieszczeń i obiektów (rejonów) podlegających szczególnej ochronie, a ponadto w formie tabeli przedstawia się podział sił i środków wydzielanych do ochrony jednostki organizacyjnej;
   4) dróg oraz rejonów ewakuacji materiałów niejawnych przechowywanych w kancelariach tajnych, kancelariach tajnych - zagranicznych, kancelariach kryptograficznych, stacjach łączności kryptograficznej oraz pomieszczeniach wydzielonych.
3. Zestawienie podstawowych znaków umownych stosowanych w części graficznej planów ochrony informacji niejawnych zawiera załącznik do rozporządzenia.
4. Część graficzną planu ochrony informacji niejawnych wykonuje się w skali umożliwiającej naniesienie wszystkich elementów ochrony i urządzeń ją wspomagających. Z części graficznej musi jasno wynikać sposób ochrony informacji niejawnych w jednostce organizacyjnej.
5. W części opisowej zawiera się:
   1) charakterystykę jednostki organizacyjnej, a w niej:

a) pełną nazwę jednostki organizacyjnej i jej rodzaj,

b) opis jakiego rodzaju materiały niejawne są przetwarzane w jednostce organizacyjnej;

2) analizę bezpieczeństwa i zagrożeń jednostki organizacyjnej związaną z ochroną przetwarzanych informacji niejawnych, z uwzględnieniem:

a) zagrożeń zewnętrznych takich jak wywiadowcze, terrorystyczne, dywersyjne i sabotażowe oraz kryminalne – na podstawie informacji uzyskanych od właściwych jednostek Służby Kontrwywiadu Wojskowego, Żandarmerii Wojskowej i Policji,

b) zagrożeń wewnętrznych wraz z podaniem ujawnionych negatywnych zjawisk w tym względzie;

3) ocenę aktualnego stanu ochrony informacji niejawnych w jednostce organizacyjnej;

4) rodzaje zabezpieczeń technicznych wykorzystywanych w ochronie materiałów niejawnych;

5) określenie stref ochronnych, sposobu ich ochrony, w tym organizację systemu przepustkowego lub kontroli dostępu;

6) sposób przechowywania i zabezpieczenia kluczy użytku bieżącego i zapasowych, kodów do zamków szyfrowych oraz kodów systemów alarmowych do stref i pomieszczeń, w których są przetwarzane informacje niejawne, a także znajdujących się w nich urządzeń do przechowywania dokumentów niejawnych;

7) organizację systemu ochrony informacji niejawnych w godzinach służbowych, po godzinach służbowych oraz w dniach wolnych od zajęć służbowych;

8) sposób postępowania z materiałami niejawnymi w sytuacjach kryzysowych;

9) siły i środki wydzielone do ewakuacji i zabezpieczenia dróg ewakuacji materiałów niejawnych przechowywanych w kancelariach tajnych, tajnych - zagranicznych, kryptograficznych, stacjach łączności kryptograficznej oraz pomieszczeniach wydzielonych;

10) inne ustalenia związane z ochroną materiałów niejawnych.

§ 19. 1. Plan ochrony informacji niejawnych przechowują pełnomocnik ochrony i oficer dyżurny jednostki organizacyjnej.

2. Plan ochrony informacji niejawnych może być udostępniony, w niezbędnym zakresie (w postaci wyciągów), siłom ochronnym i osobom realizującym zadania przewidziane dla nich w tym planie, a także osobom kontrolującym.

§ 20. Pełnomocnik ochrony nadzoruje realizację planu ochrony informacji niejawnych oraz na bieżąco go aktualizuje, stosownie do pojawiających się zagrożeń lub potrzeb.

§ 21. Bieżący nadzór nad ochroną informacji niejawnych w jednostce organizacyjnej sprawuje pion ochrony informacji niejawnych jednostki organizacyjnej.

Rozdział 6

Postępowanie z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne" w razie wprowadzenia stanu nadzwyczajnego

§ 22.1. Pełnomocnik ochrony opracowuje i aktualizuje na bieżąco, w porozumieniu z kierownikami komórek organizacyjnych jednostki organizacyjnej, plan postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne" w razie wprowadzenia stanu nadzwyczajnego.

2. Plan, o którym mowa w ust. 1 podlega zatwierdzeniu przez kierownika jednostki organizacyjnej.

§ 23. 1. Plan postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne" składa się z części opisowej i graficznej.

2. W części opisowej przedstawia się następujące informacje:

1) nazwy komórek organizacyjnych, z wyszczególnieniem numerów budynków oraz pomieszczeń, w których przetwarzane są informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne" w stanie stałej gotowości bojowej, przebieg stref ochronnych, a także sposób ich ochrony, rodzaj, ilość i skład sił ochronnych oraz rodzaje zabezpieczeń technicznych wykorzystywanych w ochronie wyżej wymienionych informacji niejawnych, organizacja systemu kontroli dostępu do stref ochronnych oraz sposób przechowywania i zabezpieczenia kluczy oraz kodów do zamków szyfrowych i systemów alarmowych;
2) działanie sił ochronnych, kierowników komórek organizacyjnych, pionu ochrony oraz wykonawców w czasie podwyższonej gotowości bojowej, gotowości bojowej zagrożenia wojennego, pełnej gotowości bojowej, a także

w sytuacjach awaryjnych (klęska żywiołowa, katastrofa naturalna, awaria techniczna), a w tym:

a) sposób postępowania sił ochronnych w poszczególnych stanach,

b) sposób i organizację wzmocnienia systemu ochrony informacji niejawnych w poszczególnych stanach, w tym sposób współdziałania sił ochronnych z Żandarmerią Wojskową, Policją oraz innymi organami porządkowymi,

c) przyjmowanie materiałów niejawnych od wykonawców przez kancelarie tajne, przygotowanie materiałów do zniszczenia, przekazania do archiwów oraz ewakuacji;

3) ewakuacja materiałów zawierających informacje oznaczone klauzulą „tajne" lub „ściśle tajne". Określenie rejonów ewakuacji, sił i środków wydzielonych do ewakuacji i zabezpieczenia dróg ewakuacji materiałów niejawnych. Współpraca z wojskowymi i cywilnymi służbami podczas ewakuacji materiałów niejawnych.

4) postępowanie z materiałami niejawnymi pozostawionymi w miejscu stałej dyslokacji oraz przeznaczonymi do zniszczenia.

3. W części graficznej przedstawia się:

1) rozmieszczenie budynków i pomieszczeń, z wyróżnieniem tych, w których są przetwarzane materiały niejawne, w postaci rzutu płaskiego z góry z opisem;

2) rozmieszczenie stref ochronnych;

3) rozmieszczenie technicznych środków wspomagających ochronę informacji niejawnych oraz posterunków wartowniczych, patroli i służb dyżurnych realizujących zadania w zakresie ochrony informacji niejawnych oznaczonych klauzulą „tajne" lub „ściśle tajne";

4) drogi oraz rejony ewakuacji materiałów niejawnych przechowywanych w kancelariach tajnych i innych niż kancelaria tajna komórkach wewnętrznych odpowiedzialnych za rejestrowanie, przechowywanie i obieg materiałów niejawnych.

§ 24.1 Plan postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne" w razie wprowadzenia stanu nadzwyczajnego przechowuje pełnomocnik ochrony.

2. Plan udostępnia się, w niezbędnym zakresie, kierownikom komórek organizacyjnych, siłom ochronnym oraz osobom realizującym zadania przewidziane dla nich w tym dokumencie.

§ 25. Pełnomocnik ochrony, w zakresie realizacji zadań wynikających z planu postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne" w razie wprowadzenia stanu nadzwyczajnego, ma prawo żądać od kierowników komórek organizacyjnych udzielenia natychmiastowej pomocy.

Rozdział 7

Przepis końcowy

§ 26. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER OBRONY NARODOWEJ

UZASADNIENIE

Konieczność zmiany dotychczasowych przepisów jest konsekwencją wejścia w życie ustawy z dnia……..2010 r. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. Nr ……, poz…..).

Projekt rozporządzenia stanowi wykonanie przez Ministra Obrony Narodowej delegacji zawartej w art. 18 ust. 1 powołanej powyżej ustawy.

Zgodnie z art. 18 ust. 1 ustawy w przedłożonym projekcie uregulowano następującą problematykę:

1) w § 3 określono:

   a) zadania Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych związane z koordynowaniem i nadzorowaniem realizacji przedsięwzięć dotyczących ochrony informacji niejawnych przez piony ochrony jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska Ministerstwa oraz kierownikom komórek organizacyjnych Ministerstwa Obrony Narodowej,

   b) zadania pełnomocników ochrony dowódców rodzajów sił zbrojnych (równorzędnych) i innych osób funkcyjnych, którym podporządkowano jednostki organizacyjne dotyczące koordynowania i nadzorowania realizacji przedsięwzięć w zakresie ochrony informacji niejawnych przez piony ochrony jednostek organizacyjnych podległych tym osobom.

2) w § 4 sprecyzowano szczegółowe zadania pełnomocników ochrony dowódców jednostek organizacyjnych związane z zapewnieniem w jednostkach organizacyjnych właściwej ochrony informacji niejawnych oraz przestrzegania przepisów w tym zakresie;

3) w § 5 sprecyzowano zasady współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych w właściwymi jednostkami organizacyjnymi Służby Kontrwywiadu Wojskowego;

4) w § 6 określono rodzaje szkolenia w zakresie ochrony informacji niejawnych, a także zasady jego organizowania i prowadzenia przez pełnomocników ochrony dowódców jednostek organizacyjnych;

5) w § 11-16 sprecyzowano szczególne wymagania w zakresie stosowania środków bezpieczeństwa fizycznego ochrony informacji niejawnych. Określono definicje stref ochronnych, sposoby oznaczania stref ochronnych, a także zasady wchodzenia i wjazdu na teren tych stref;

6) w §17-21 określono zasady opracowywania planów ochrony informacji niejawnych w jednostkach organizacyjnych oraz sprecyzowano elementy z jakich powinien się składać plan ochrony;

7) w § 22-25 określono zasady postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „ściśle tajne" i „tajne" w razie wprowadzenia stanu nadzwyczajnego oraz elementy, które powinien zawierać plan postępowania z materiałami zwierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne".

W projekcie rozporządzenia, niezależnie od zmian wynikających z wprowadzenia przepisów nowej ustawy o ochronie informacji niejawnych, uwzględniono zmiany, które zaszły w ostatnim czasie w przepisach o ochronie obiektów wojskowych, a także przekształcenia wynikające z profesjonalizacji i restrukturyzacji Sił Zbrojnych.

Projekt rozporządzenia nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych, ponieważ nie zawiera przepisów technicznych.

Przepisy przedmiotowego rozporządzenia pozostają poza zakresem prawa Unii Europejskiej.

Ocena skutków regulacji (OSR)

1) przedmiotowy projekt był konsultowany z kierownikami komórek organizacyjnych Ministerstwa Obrony Narodowej oraz Służbą Kontrwywiadu Wojskowego. Ponadto będzie podlegał uzgodnieniom zgodnie z postanowieniami uchwały Nr 49 Rady Ministrów z dnia 19 marca 2002 r. – Regulamin pracy Rady Ministrów (M.P. Nr 13, poz. 221, z późn. zm.);

2) projekt oddziaływuje wyłącznie na jednostki organizacyjne, o których mowa w art. 1 ust. 2 pkt 2 ustawy z dnia…….o ochronie informacji niejawnych;

3) przepisy prawa nie obligują projektodawców do przeprowadzenia dodatkowych konsultacji, o których mowa w § 10 ust. 6 pkt 2 uchwały Nr 49 Rady Ministrów z dnia 19 marca 2002 r. – Regulamin pracy Rady Ministrów, ze względu na przedmiot regulacji i wąski zakres oddziaływania przedmiotowego rozporządzenia;

4) wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy, konkurencyjność wewnętrzną i zewnętrzną gospodarki, sytuację i rozwój regionalny; nie wywrze negatywnych skutków prawnych w dziedzinie uznaniowości działania organów administracji państwowej oraz stosowanych przez te organy procedur;

5) wejście w życie rozporządzenia nie spowoduje dodatkowych skutków finansowych dla budżetu państwa;

6) projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

43-02-aa

Projekt

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia ……

w sprawie sposobu przeprowadzania i podstawowych kryteriach określania poziomu zagrożeń oraz doboru środków bezpieczeństwa fizycznego, a także wymagań w zakresie organizacji i funkcjonowania kancelarii tajnych oraz obiegu informacji niejawnych

(Dz. U. z dnia ……..)

Na podstawie art. 47 ust. 1 ustawy z dnia …… o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U…….) zarządza się, co następuje:

§ 1. 1. Rozporządzenie określa:

1) rodzaje zagrożeń, które należy uwzględnić w określaniu poziomu zagrożeń;
2) środki ochrony fizycznej;
3) kryteria tworzenia stref ochronnych;
4) strukturę organizacyjną kancelarii, z uwzględnieniem możliwości tworzenia jej oddziałów;
5) podstawowe zadania kierownika kancelarii;
6) tryb obiegu informacji niejawnych;
7) wzór dziennika ewidencji;
8) wzór karty zapoznania z dokumentem;

2. Postanowień, o których mowa w ust. 1 pkt 1-6, nie stosuje się w jednostkach organizacyjnych organów wymienionych w art. _____ustawy z dnia _____o ochronie informacji niejawnych oraz o zmianie niektórych ustaw.

§ 2.1. Przy organizacji kancelarii tajnej, zwanej dalej „kancelarią” oraz zabezpieczaniu pomieszczeń, w których przetwarzane są lub będą informacje niejawne oznaczone klauzulą „ściśle tajne”, „tajne” i „poufne” należy określić poziom zagrożenia nieuprawnionego ujawnienia lub ich utraty, zwany dalej „poziomem zagrożenia”, uwzględniający:

1) zagrożenia związane z zasobami ludzkimi;
2) zagrożenia związane z lokalizacją;
3) zagrożenia związane z organizacją i środkami ochrony fizycznej;
4) zagrożenia związane z działaniem sił natury.

2. Czynniki mające wpływ na określenie poziomu zagrożenia informacji niejawnych oraz sposób jego oceny określa załącznik nr 1 do rozporządzenia.

§ 3. Dokumentacja w zakresie bezpieczeństwa fizycznego, o której mowa w art. 42 ust. 3 Ustawy określa skalę zagrożeń dla nieuprawnionego ujawnienia lub utraty informacji niejawnych na poziomie: wysokim, średnim lub niskim.

§ 4. 1. Tworzy się strefy ochronne:

1) Strefę I, w której przebywanie wiąże się z możliwością bezpośredniego dostępu do informacji niejawnych. W strefie I dokumenty niejawne oznaczone klauzulą „ściśle tajne" lub „tajne" można przechowywać poza szafami metalowymi w pomieszczeniach odpowiadających co najmniej klasie I odporności na włamanie według Polskiej Normy PN-EN- 1143-1 z zastrzeżeniem § 5 ust. 1 pkt 1;
2) Strefę II, w której przebywanie nie wiąże się z bezpośrednim dostępem do informacji niejawnych. W strefie II dokumenty niejawne oznaczone klauzulą „ściśle tajne" lub „tajne" muszą być przechowywane w szafach metalowych w odpowiedniej klasie.
3) Strefę III służącą do kontroli osób, w której przebywanie nie wiąże się z dostępem do informacji niejawnych oznaczonych klauzulą „ściśle tajne" lub „tajne".

2. Wejście i wyjście ze strefy I lub II następuje wyłącznie ze strefy III.

3. Kryteria tworzenia stref ochronnych określa załącznik nr 2 do rozporządzenia.

§ 5.1. Informacje niejawne oznaczone klauzulą „ściśle tajne" lub „tajne" przetwarzane są w strefach ochronnych odpowiednio:

1) przy wysokim poziomie zagrożenia w strefie I, dodatkowo powinny być przechowywane w szafie metalowej określonej w § 6 ust. 1 pkt 1-2;

2) przy średnim poziomie zagrożenia w strefie I;

3) przy niskim poziomie zagrożenia mogą być przetwarzane w strefie II.

2. Informacje niejawne oznaczone klauzulą „poufne" przetwarzane są w III strefie ochronnej odpowiednio:

1) przy wysokim poziomie zagrożenia w odpowiedniej szafie metalowej, w pomieszczeniu zabezpieczonym w drzwi o zwiększonej odporności na włamanie z zamkiem wielopunktowym i blokadami przeciwwyważeniowymi, z oknami zabezpieczonymi przed podglądem i włamaniem;

2) przy średnim poziomie zagrożenia w odpowiedniej szafie metalowej, w pomieszczeniu zabezpieczonym w drzwi z zamkiem wielopunktowym;
3) przy niskim poziomie zagrożenia w odpowiedniej szafie metalowej.

§ 6. 1. W zależności od nadanej klauzuli tajności, dokumenty niejawne lub materiały, z zastrzeżeniem § 5 ust. 1 pkt 1, przechowywane są:
1) „ściśle tajne" - w szafach metalowych klasy C;
2) „tajne" - w szafach metalowych klasy B;
3) „poufne" - w szafach metalowych klasy A.

2. Klasyfikację szaf oraz rodzaje środków ochrony fizycznej określa załącznik nr 3 do rozporządzenia.

§ 7. 1. Do ochrony informacji niejawnych oznaczonych klauzulą „ściśle tajne" i „tajne" stosuje się elektroniczne systemy zabezpieczeń:

1) Systemy sygnalizacji włamania i napadu wyposażony w urządzenia transmisji alarmu;

2) Systemy telewizji dozorowej stosowane w zabezpieczeniach;

3) Systemy kontroli dostępu stosowane w zabezpieczeniach;

4) Systemy sygnalizacji pożarowej.

2. Elektroniczne systemy zabezpieczeń wykorzystywane do ochrony informacji niejawnych mogą funkcjonować jako podsystem innego elektronicznego systemu zabezpieczeń.

3. W elektronicznych systemach zabezpieczeń stosuje się wyłącznie urządzenia elektroniczne posiadające certyfikaty wydane przez akredytowaną jednostkę certyfikującą lub deklaracje zgodności producenta potwierdzające zgodność tych urządzeń z obowiązującymi dokumentami normatywnymi.

4. Instalację, konserwacje i naprawy elektronicznych systemów zabezpieczeń może wykonywać osoba posiadająca licencję pracownika zabezpieczenia technicznego drugiego stopnia.

5. Systemy wykonane przed wejściem w życie rozporządzenia wykonane według Polskiej Normy PN-93/E-08390 w klasie SA3 i SA4 mogą być wykorzystywane nadal do zabezpieczenia informacji niejawnych oznaczonych

klauzulą „ściśle tajne” i „tajne”, pod warunkiem, że system określa rodzaje czynności przewidziane dla drugiego stopnia zabezpieczenia według Polskiej Normy PN-EN-50133-1.

§ 8. W przypadku gdy kancelaria obsługuje więcej niż jedną jednostkę organizacyjną, informacje niejawne tych jednostek muszą być fizycznie od siebie oddzielone.

§ 9. 1. Kancelaria, ze względów organizacyjnych, może mieć swoje oddziały tworzone i funkcjonujące zgodnie z zasadami i na warunkach przewidzianych dla kancelarii.

2. Kancelarią kieruje kierownik kancelarii, wyznaczony przez kierownika jednostki organizacyjnej na wniosek pełnomocnika ochrony.

3. Kierownik jednostki organizacyjnej, na wniosek pełnomocnika ochrony, może wyznaczyć zastępcę kierownika kancelarii.

4. Oddziałem kancelarii kieruje zastępca kierownika kancelarii lub inny wyznaczony przez pełnomocnika ochrony pracownik pionu ochrony.

§ 10. Pełnomocnik ochrony sprawuje nadzór nad pracownikami wykonującymi czynności kancelaryjne związane z obsługą dokumentów niejawnych, w zakresie realizacji tych czynności.

§ 11. 1. Do podstawowych zadań kierownika kancelarii należy:

1) bezpośredni nadzór nad obiegiem dokumentów;
2) udostępnianie lub wydawanie dokumentów osobom do tego uprawnionym;
3) egzekwowanie zwrotu dokumentów;
4) kontrola przestrzegania właściwego oznaczania i rejestrowania dokumentów w kancelarii oraz jednostce organizacyjnej;
5) prowadzenie bieżącej kontroli postępowania z dokumentami;
6) wykonywanie poleceń pełnomocnika ochrony;
7) nadzór nad pracą oddziałów kancelarii.

2. Osoby, o których mowa w § 8 ust. 4 i 5, wykonują obowiązki kierownika kancelarii określone w ust. 1 pkt 1-6.

§ 12. 1. W przypadku zmiany na stanowisku kierownika kancelarii lub osoby, o której mowa w § 8 ust. 4 i 5 sporządza się protokół zdawczo-odbiorczy.

2. Protokół, o którym mowa w ust. 1, sporządza się w obecności osoby zdającej obowiązki, osoby przejmującej oraz pełnomocnika ochrony. Protokół sporządza się w dwóch egzemplarzach; pierwszy egzemplarz przechowywany jest w kancelarii, drugi u pełnomocnika ochrony.

3. W sytuacji czasowej nieobecności osób, o których mowa w § 8 ust. 3-5 ich obowiązki przejmuje upoważniony pracownik kancelarii lub inny pracownik pionu ochrony. W razie ich braku kancelarię przejmuje protokolarnie inny pracownik wyznaczony przez kierownika jednostki organizacyjnej, na wniosek pełnomocnika ochrony.

§ 13. 1. W pomieszczeniach kancelarii można wydzielić miejsce, w którym osoby upoważnione mogą zapoznawać się z dokumentami - czytelnię.

2. Czytelnia powinna być zorganizowana w sposób umożliwiający stały nadzór nad dokumentami ze strony pracowników kancelarii.

3. W czytelni dopuszcza się możliwość instalowania systemu nadzoru wizyjnego wyłącznie do obserwacji osób zapoznających się z treścią dokument.

§ 14. 1. Dokumenty i materiały oznaczone różnymi klauzulami tajności są przechowywane w odrębnych szafach metalowych lub pomieszczeniach, chyba że wchodzą one w skład zbioru dokumentów.

2. Dokumenty i materiały, o których mowa w ust. 1, mogą być przechowywane w jednej szafie metalowej lub pomieszczeniu pod warunkiem ich fizycznego oddzielenia. W takim przypadku szafa musi spełniać wymagania odpowiednie dla najwyższej klauzuli tajności przechowywanych w nich dokumentów lub materiałów.

§ 15. Kierownik jednostki organizacyjnej zatwierdza plan ochrony informacji niejawnych, który powinien zawierać w szczególności:

1. Opis granic stref ochronnych.
2. Zastosowane środki ochrony fizycznej.
3. Zasady i sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do pomieszczeń oraz szaf, w których przechowane są informacje niejawne a także zasady ustalania, zmiany i deponowania haseł lub szyfrów, w przypadku stosowania zamków szyfrowych.

4. Procedury przyznawania uprawnień do wejścia, wyjścia i przebywania w strefach ochronnych I i II, w tym dla pracowników obsługi technicznej (np. personel sprzątający), oraz interesantów/gości;
5. Sposób interwencji osób odpowiedzialnych za ochronę fizyczną w przypadkach wywołania alarmu.
6. Procedury ewakuacji i niszczenia informacji niejawnych (w tym w razie wprowadzenia stanu nadzwyczajnego).

§ 16. 1. Po zakończeniu pracy kierownik kancelarii, zastępca kierownika kancelarii lub upoważniony pracownik kancelarii jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczeń.

2. Wszelkie nieprawidłowości związane z naruszeniem zasad, o których mowa w § 14 należy niezwłocznie zgłaszać pełnomocnikowi ochrony.

§ 17. 1. W kancelarii przyjmuje się, rejestruje, przechowuje, przekazuje i wysyła dokumenty i materiały oraz prowadzi:
1) rejestr dzienników, książek ewidencyjnych i teczek, którego wzór określa załącznik nr 4 do rozporządzenia;
2) dziennik ewidencji, którego wzór określa załącznik nr 5 do rozporządzenia;
3) karty zapoznania się z dokumentem zawierającym tajemnicę państwową, którego wzór określa załącznik nr 6 do rozporządzenia;
4) książkę doręczeń przesyłek miejscowych, której wzór określa załącznik nr 7 do rozporządzenia;
5) wykaz przesyłek nadanych, którego wzór określa załącznik nr 8 do rozporządzenia.

2. W kancelarii dodatkowo prowadzi się rejestr wydanych przedmiotów, którego wzór określa załącznik nr 9 do rozporządzenia, do ewidencjonowania wydanych nośników do zapisów informacji w postaci cyfrowej, dysków optycznych i taśm elektromagnetycznych oraz innych przedmiotów.

3. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych kancelaria może prowadzić także inne rejestry niż wymienione w ust. 1 i 2, w tym odrębne rejestry dla dokumentów oznaczonych różnymi klauzulami tajności.

4. Za zgodą kierownika jednostki organizacyjnej, w porozumieniu z pełnomocnikiem ochrony, w kancelarii mogą być przyjmowane, rejestrowane, przechowywane i wysyłane dokumenty i materiały oznaczone klauzulą „poufne” lub „zastrzeżone".

5. W przypadku określonym w § 7 kancelaria prowadzi urządzenia wymienione w ust. 1 i 2 odrębnie dla każdej jednostki organizacyjnej.

§ 18. 1. Kierownik kancelarii, zastępca kierownika kancelarii, pracownik kancelarii lub biura podawczego przyjmuje przesyłki lub dokumenty za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do jednostki organizacyjnej.

2. Przyjmując przesyłkę, sprawdza się:

1) prawidłowość adresu;
2) całość pieczęci i opakowania;
3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy;
4) zgodność numeru na przesyłce z numerem tej przesyłki w wykazie lub w książce doręczeń.

3. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania osoba kwitująca odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi pełnomocnikowi ochrony w jednostce organizacyjnej odbiorcy, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik - kolejny egzemplarz protokołu przekazuje się także jemu.

4. Przesyłki lub dokumenty przyjęte przez biuro podawcze jednostki organizacyjnej niezwłocznie przekazuje się do kancelarii.

5. Po otwarciu przesyłki kierownik kancelarii, zastępca kierownika kancelarii lub pracownik kancelarii:

1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
2) ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.

6. W przypadku stwierdzenia nieprawidłowości w wyniku czynności, o których mowa w ust. 5, kierownik kancelarii, zastępca kierownika kancelarii lub pracownik kancelarii sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy.

7. Kierownik kancelarii, zastępca kierownika kancelarii lub pracownik kancelarii odnotowuje fakt sporządzenia protokołu, o którym mowa w ust. 3 i 6, w odpowiednim dzienniku lub rejestrze w rubryce „Informacje uzupełniające/Uwagi".

§ 19. 1. Kierownik kancelarii lub zastępca kierownika kancelarii albo pracownik kancelarii rejestruje przyjęte dokumenty w odpowiednim dzienniku lub rejestrze.

2. Dla każdego dokumentu oznaczonego klauzulą „ściśle tajne” lub „tajne” z chwilą zarejestrowania, zakłada się kartę zapoznania się z dokumentem, którą dołącza się do dokumentu. Kartę zapoznania się z dokumentem można załączyć do dokumentu zawierającego informacje niejawne oznaczone klauzulą „poufne".

3. Do zbioru dokumentów załącza się jedną kartę zapoznania się z dokumentem.

4. Zarejestrowane dokumenty kierownik kancelarii, zastępca kierownika kancelarii lub pracownik kancelarii przekazuje albo udostępnia adresatowi lub upoważnionej osobie za pokwitowaniem.

§ 20. 1. W kancelarii nie otwiera się przesyłek oznaczonych „do rąk własnych". W odpowiednim dzienniku lub rejestrze wpisuje się nadawcę, numer i datę wpływu dokumentu; w rubryce „Informacje uzupełniające/Uwagi" odnotowuje się, że przesyłka była oznaczona „do rąk własnych".

2. Na opakowaniu przesyłek, o których mowa w ust. 1, wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę. Przesyłkę przekazuje się - za pokwitowaniem - bezpośrednio adresatowi, a w razie jego nieobecności - osobie przez niego upoważnionej do odbioru.

3. Zatrzymanie przez adresata dokumentu, adresowanego „do rąk własnych", odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".

4. Czynności, o których mowa w § 17 ust. 5, w stosunku do przesyłek, o których mowa w ust. 1, dokonuje adresat przesyłki.

5. W przypadku zwrotu do kancelarii przesyłki, o której mowa w ust. 1, kierownik kancelarii, zastępca kierownika kancelarii lub pracownik kancelarii uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.

6. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki „do rąk własnych" w kancelarii w stanie zamkniętym, kierownik kancelarii, zastępca kierownika kancelarii lub pracownik kancelarii dokonuje czynności, o których mowa w ust. 5, przy udziale adresata. Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".

§ 21. Pilne przesyłki, telegramy i szyfrogramy doręcza się niezwłocznie adresatom. Przy kwitowaniu odbioru tych przesyłek odnotowuje się godzinę doręczenia.

§ 22. 1. Otrzymaną i wysyłaną przesyłkę, bądź wytworzony dokument lub materiał rejestruje się we właściwej ewidencji odpowiednio w kolejności wytworzenia lub otrzymania.

2. Rejestracji, o których mowa w ust. 1, dokonuje się atramentem lub tuszem. Zmian we właściwej rejestracji dokonuje się kolorem czerwonym, umieszczając datę i czytelny podpis osoby dokonującej zmiany.

3. W przypadku anulowania pozycji we właściwej ewidencji, należy podać powód anulowania, umieszczając datę i czytelny podpis osoby dokonującej anulowania. Anulowania pozycji we właściwej ewidencji dokonuje się kolorem czerwonym.

4. Zabrania się wycierania i zamazywania rejestracji, o których mowa w ust. 1.

§ 23. 1. Środki ochrony fizycznej wynikające z oceny poziomu zagrożenia należy dostosować w terminie 1 roku od dnia wejścia w życie rozporządzenia.

2. W jednostkach organizacyjnych nadal stosuje się rejestry, książki i wykazy, o których mowa w § 10 ust. 1 pkt 1 i 4-6 oraz ust. 2 i 3 rozporządzenia Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. Nr 208, poz. 1741).

3. Dziennik, o którym mowa § 10 ust. 1 pkt 2 rozporządzenia wymienionego w ust. 2, stosuje się do dnia 31 grudnia 2010 r.

§ 24. Traci moc rozporządzenie Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. Nr 208, poz. 1741).

§ 25. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezes Rady Ministrów

Załącznik nr 1 do rozporządzenia

Sposób przeprowadzania i podstawowe kryteria określania poziomu zagrożenia oraz dobór środków bezpieczeństwa fizycznego właściwych do wskazanego poziomu zagrożenia.

W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków ochrony fizycznej należy w szczególności określić poziom zagrożenia nieuprawnionego ujawnienia lub utraty informacji niejawnych, zwanego dalej „poziomem zagrożenia". Określając poziom zagrożenia należy ustalić realne zagrożenia mogące mieć wpływ na bezpieczeństwo informacji niejawnych i ocenić je według proponowanej poniżej matrycy.

Przed wypełnianiem matrycy proszę szczegółowo zapoznać się z założeniami oraz postępować zgodnie z instrukcją.

Założenia:

1. Poziom zagrożenia określa jednostka organizacyjna (np. pełnomocnik ochrony).
2. Dokumentację (matrycę) wskazującą poziom zagrożenia zatwierdza kierownik jednostki organizacyjnej.
3. Czynniki od I do VI wpływające na określenie poziomu zagrożenia zostały przedstawione w tabeli z podziałem na warianty (A, B, C, D, E). Przy ocenie dokonuje się wyboru tylko jednego wariantu mającego odniesienie do jednostki organizacyjnej lub zbliżonego do niego.
4. Punkty przypisane dla każdego wariantu nie podlegają zmianom.
5. W przypadku wystąpienia innych czynników mogących mieć wpływ na ochronę informacji niejawnych należy je dodatkowo uwzględnić (VII. Inne czynniki) a wartość punktową wpisać w matrycę. Dodatkowo w tabeli należy zamieścić uzasadnienie dla każdego wskazanego czynnika.
6. Wskazane czynniki powinny być poddane wnikliwej analizie pod kątem ich realnego wpływu na bezpieczeństwo informacji niejawnych przetwarzanych w jednostce organizacyjnej.

7. Punkty z matrycy należy podsumować. Uzyskany wynik wskaże poziom zagrożenia zgodnie ze skalą: poziom niski do 15 pkt, poziom średni od 16 do 28 pkt, poziom wysoki powyżej 28 pkt.
8. Określenie poziomu zagrożenia powinno mieć zastosowanie do jednostki organizacyjnej lub do jej poszczególnych obiektów, w których są lub będą przetwarzane informacje niejawne.
9. Określanie poziomu zagrożenia dokonuje się przy każdej zmianie istotnych czynników mogących mieć wpływ na poziom zagrożenia.

MATRYCA
DO OKREŚLENIA POZIOMU ZAGROŻENIA

I. LOKALIZACJA

	Warianty	Punktacja	Ocena jednostki
A	Budynek wolnostojący i ogrodzony	0	_____ pkt
B	Budynek wolnostojący nie ogrodzony	2	
C	Budynek w zabudowie zwartej	4	
D	Budynek użytkowany wspólnie z innymi podmiotami	8	

A. Budynek, w najbliższym sąsiedztwie którego nie ma innych obiektów. Ogrodzenie budynku stanowi barierę chroniącą przed bezpośrednim wejściem do środka. Budynek częściowo ogrodzony, ale w taki sposób, że wejście jest możliwe tylko po wcześniejszym pokonaniu ogrodzenia.

B. Budynek bez ogrodzenia. Budynek częściowo ogrodzony, ale wejście do budynku nie wymaga pokonania ogrodzenia.

C. Budynek, którego ściany przylegają do budynku innej jednostki organizacyjnej.

D. Budynek użytkowany przez więcej niż jedną jednostkę organizacyjną, ze wspólnym wejściem.

II. OCHRONA FIZYCZNA

	Warianty	Punktacja	Ocena jednostki
A	Całodobowa ochrona osobowa z wykorzystaniem systemów elektronicznych	0	_____ pkt
B	Całodobowa ochrona osobowa	2	
C	Całodobowa ochrona przy zastosowaniu systemów elektronicznych	4	
D	Ochrona sprawowana tylko po godzinach pracy	6	
E	Brak ochrony	8	

A. Budynek jest chroniony całodobowo przez przedsiębiorcę wykonującego zadania w zakresie ochrony osób i mienia lub wewnętrzną służbę ochrony i jednocześnie wykorzystuje się elektroniczne systemy wspomagające (system nadzoru wizyjnego, system sygnalizacji włamania i napadu).

B. Budynek jest chroniony całodobowo przez przedsiębiorcę wykonującego zadania w zakresie ochrony osób i mienia lub wewnętrzną służbę ochrony bez wykorzystania elektronicznych systemów wspomagających.

C. Budynek jest chroniony przez całą dobę tylko systemami elektronicznymi (systemem sygnalizacji włamania i napadu lub systemem nadzoru wizyjnego). Działanie systemów musi powodować reakcję osób w sytuacjach alarmowych.

D. Ochrona budynku sprawowana jest tylko po godzinach pracy przez osoby lub systemy elektroniczne.

III. LICZBA OSÓB MAJĄCYCH DOSTĘP DO INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ŚCIŚLE TAJNE", „TAJNE" I „POUFNE" (ŁĄCZNIE)

	Warianty	Punktacja	Ocena jednostki
A	do 20 % ogólnej liczby pracowników	2	_____ pkt
B	od 21% do 30%	4	
C	od 31% do 50%	6	
D	powyżej 51%	10	

Przy określeniu liczby osób mających dostęp do informacji niejawnych należy uwzględnić wszystkich pracowników jednostki organizacyjnej uprawnionych do dostępu do informacji od klauzuli „poufne" wzwyż na podstawie przepisów ustawy o ochronie informacji niejawnych lub na podstawie innych przepisów (o ustroju sądów powszechnych, ustroju sądów wojskowych oraz o prokuraturze).

W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

IV. ILOŚĆ INFORMACJI NIEJAWNYCH PRZETWARZANYCH W JEDNOSTCE ORGANIZACYJNEJ OZNACZONYCH KLAUZULĄ „ŚCIŚLE TAJNE", „TAJNE" I „POUFNE" (ŁĄCZNIE)

	Warianty	Punktacja	Ocena jednostki
A	do 100 dokumentów niejawnych	2	_____ pkt
B	101 – 200 dokumentów niejawnych	3	
C	201 – 500 dokumentów niejawnych	6	
D	501 – 1000 dokumentów niejawnych	8	
E	powyżej 1000 dokumentów niejawnych	10	

Przy określeniu ilości dokumentów przetwarzanych w jednostce organizacyjnej należy brać pod uwagę wszystkie dokumenty niejawne od klauzuli „poufne" wzwyż zarejestrowane w urządzeniach ewidencyjnych w minionym roku kalendarzowym oraz pozostające w faktycznej dyspozycji jednostki, zarejestrowane w latach poprzednich (suma dokumentów będzie opowiadała wskazanemu wyżej wariantowi).

W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

V. ZAGROŻENIE POŻAREM

	Warianty	Punktacja	Ocena jednostki
A	Automatyczne systemy gaszenia	0	_____ pkt
B	Wyposażenie budynku w stałe instalacje gaśnicze	1	
C	Wyposażenie budynku w podręczne środki gaśnicze	2	
D	Brak ochrony przeciwpożarowej	4	

A. Zabezpieczenie budynku będą stanowić systemy sygnalizacji pożarowej wraz z samoczynnymi systemami gaszenia.

B. Budynek wyposażony w instalacje gaśnicze, nie umożliwiające samoczynnego gaszenia pożaru (np. zraszacze, hydranty).

C. W budynku znajdują się jedynie podręczne środki gaśnicze (np. gaśnice, koce).

VI. KONSTRUKCJA BUDYNKU

	Warianty	Punktacja	Ocena jednostki
A	Budynek o konstrukcji zapewniającej wysoki stopień odporności na włamanie	0	_____ pkt
B	Budynek o konstrukcji odpornej na siłowe wtargnięcie	4	
C	Budynek o konstrukcji szkieletowej	8	

A. Konstrukcja budynku wykonana z betonu lub porównywalnego materiału z drzwiami antywłamaniowymi i oknami zabezpieczonymi przed włamaniem.

B. Budynek wykonany z cegieł lub materiałów o podobnych właściwościach, z oknami i drzwiami zabezpieczonymi przed wtargnięciem.

C. Szkieletowa konstrukcja budynku z wypełnieniem wykonanym z materiałów o niskiej odporności na włamanie (np. pojedynczej cegły, pustaka, aluminium, drewna lub elementów szklanych).

VII. INNE CZYNNIKI

	Czynniki mogące wpływać na poziom bezpieczeństwa informacji niejawnych	Punktacja 1-10	Ocena jednostki	Uzasadnienie
A				
B				
C				
D				
		SUMA		

Analiza zagrożeń powinna uwzględniać inne czynniki wynikające ze specyfiki jednostki organizacyjnej, nie uwzględnione w tabelach powyżej a mogące mieć wpływ na ochronę informacji niejawnych np.:

A. Najbliższe sąsiedztwo:

- obiekty przedstawicielstw i podmiotów zagranicznych,
- obiekty sportowe i hale widowiskowe,
- ogólnodostępne parkingi i garaże,
- zakłady przemysłowe i instalacje stanowiące zagrożenie dla życia i zdrowia.

B. Lokalizacja jednostki organizacyjnej na obszarach zagrożonych powodzią, szkodami górniczymi itp.

W przypadku uwzględnienia dodatkowego czynnika należy go ocenić według zaproponowanej skali i uzasadnić ocenę. Punkty należy podsumować.

WYNIK		
Czynnik		**Punktacja**
I	Lokalizacja	
II	Ochrona fizyczna	
III	Liczba osób mających dostęp do informacji niejawnych	
IV	Ilość informacji niejawnych przetwarzanych w jednostce organizacyjnej	
V	Zagrożenie pożarem	
VI	Konstrukcja budynku	
VII	Inne	
	SUMA	

POZIOM ZAGROŻENIA		
NISKI	ŚREDNI	WYSOKI
1 pkt - 15 pkt	16 pkt - 28 pkt	powyżej 28 pkt
[ ]*	[ ]	[ ]

*) wstawić „X” przy odpowiednim poziomie

Załącznik nr 2 do rozporządzenia
Kryteria tworzenia stref ochronnych

STREFA I	STREFA II	STREFA III
1. obustronny system kontroli dostępu rejestrujący wejścia, wyjścia i przebywanie, umożliwiający identyfikację personalną osób; 2. system nadzoru wizyjnego rejestrujący wejścia do strefy (dla informacji oznaczonych klauzulą „ściśle tajne”); 3. zapis danych zarejestrowanych przez system nadzoru wizyjnego i system kontroli dostępu musi być możliwy do odtworzenia po upływie, co najmniej 30 dni od zarejestrowania; 4. system sygnalizacji włamania i napadu co najmniej w klasie SA3; 5. system sygnalizacji pożarowej; 6. zabezpieczenie przed podglądem i włamaniem; 7. ściany i stropy stanowiące granicę strefy powinny być wykonane z materiałów niepalnych o nośności granicznej odpowiadającej co najmniej konstrukcji murowanej z cegły pełnej o grubości 250 mm; dopuszcza się zastosowanie innych zabezpieczeń posiadające właściwości nie mniejsze niż ściana o ww. konstrukcji; 8. drzwi wejściowe do strefy powinny być w klasie C według Polskiej Normy PN-90/B-92270 lub klasy 3-4 wg PN-ENV 1627	1. obustronny system kontroli dostępu rejestrujący wejścia, wyjścia i przebywanie, umożliwiający identyfikację personalną osób; 2. system sygnalizacji włamania i napadu co najmniej w klasie SA 3; 3. system sygnalizacji pożarowej; 4. zabezpieczenie przed podglądem i włamaniem 5. drzwi wejściowe o zwiększonej odporności na włamanie wyposażone w zamek wielopunktowy i blokady przeciwwyważeniowe.	kontrola osób wchodzących i wychodzących.

Załącznik nr 3 do rozporządzenia

Środki ochrony fizycznej

NAZWA	Klasyfikacja
Szafy	**Szafa metalowa klasy C (dla dokumentów oznaczonych klauzulą „ściśle tajne")** 1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane ze stali konstrukcyjnej wyższej jakości, o grubości minimum 5 mm, a w przypadku konstrukcji wielopłaszczowej grubość płaszcza zewnętrznego powinna wynosić minimum 3 mm. Połączenia korpusu szafy powinny zapewnić dostateczną sztywność. 2. Szafa może być wyposażona w zamykane skrytki. 3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe wyposażone w mechanizm dźwigniowy, blokujący je co najmniej na czterech krawędziach. 4. Mechanizm dźwigniowy rygli w drzwiach powinien być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglujący, w tym: a) zamek mechaniczny kluczowy wielozastawkowy z możliwością wyjęcia klucza tylko w pozycji zamkniętej, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem, b) zamek mechaniczny szyfrowy o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skoku nastawień nie większym niż jedna działka i posiadający minimum 100 podziałek na pokrętle (minimum 1.000.000 kombinacji). Czas otwarcia zamka przez osobę nieuprawnioną drogą wybierania kolejnych kombinacji powinien wynosić nie mniej niż 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem radiologicznym (promieniowanie co najmniej 10 curie, Co-60 z odległości 760 mm). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Szafa powinna być wyposażona w dwa komplety kluczy do ustawiania szyfru. Dopuszcza się również stosowanie zamka elektronicznego szyfrowego, pod warunkiem spełnienia przez niego takich samych wymagań odporności na włamanie co zamek mechaniczny szyfrowy. 5. Podstawa szafy musi posiadać te same rozmiary co wierzch. Konstrukcja dna szafy powinna wytrzymać siły minimum 50 kN. 6. Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą, potwierdzający zgodność wyrobu z wymaganiami klasy C. 7. Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane: a) nazwę wyrobu, b) nazwę i kod identyfikacyjny producenta, typ i numer modelu, c) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu, d) masę. **Szafa metalowa klasy B (dla dokumentów oznaczonych klauzulą „tajne")** 1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 3 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność. 2. Szafa może być wyposażona w zamykane skrytki. 3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe wyposażone w mechanizm dźwigniowy, blokujący je co najmniej na czterech krawędziach. 4. Mechanizm dźwigniowy rygli w drzwiach musi być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglujący, w tym: a) zamek mechaniczny kluczowy wielozastawkowy z możliwością wyjęcia klucza tylko w pozycji zamkniętej, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem, b) zamek mechaniczny szyfrowy o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skali nastawień nie większej niż półtorej działki i posiadający minimum 100 podziałek na pokrętle (minimum 1.000.000 kombinacji). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem. Z szafą powinny być dostarczone dwa komplety kluczy do zmiany

Załącznik nr 4 do rozporządzania

WZÓR

REJESTR DZIENNIKÓW, KSIĄŻEK EWIDENCYJNYCH I TECZEK

Oznaczenie klauzuli tajności dziennika, rejestru, książki ewidencyjnej itp.	Numer kolejny dziennika, rejestru, książki ewidencyjnej itp.	Adnotacje dot. przedłużenia okresu ochrony, zniesienia bądź zmiany klauzuli tajności	Data rejestracji dziennika, rejestru, książki ewidencyjnej itp.	Nazwa teczki, dziennika, rejestru, książki ewidencyjnej itp.	Data		Liczba stron dziennika, rejestru, książki ewidencyjnej itp.	Komórka organizacyjna, odpowiedzialna za prowadzenie dziennika, rejestru, książki ewidencyjnej itp.	Pokwitowanie odbioru dziennika, rejestru, książki ewidencyjnej itp.			Informacje uzupełniające / Uwagi
					rozpoczęcia dziennika, rejestru, książki ewidencyjnej itp.	zakończenia dziennika, rejestru, książki ewidencyjnej itp.			imię i nazwisko	data oraz podpis osoby prowadzącej dziennik, rejestr, książkę ewidencyjną itp.	potwierdzenie zwrotu data i podpis	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**

...../.....

.....
(klauzula tajności) ...../.....

Załącznik nr 5 do rozporządzenia

WZÓR

DZIENNIK EWIDENCJI
strona lewa

Oznaczenie klauzuli tajności	Numer kolejny zapisu	Adnotacje dot. przedłużenia okresu ochrony, zniesienia bądź zmiany klauzuli tajności	Data rejestracji dokumentu	Rodzaj dokumentu W-wychodzący P-przychodzący X-inne[1]	Nazwa nadawcy/ adresata	Numer i data dokumentu otrzymanego	Nazwa dokumentu lub czego dotyczy	Liczba egzemplarzy	Liczba (dotyczy jednego egzemplarza)		
									stron dokumentu z załącznikami lub innych jednostek miary	załączników	stron załączników lub innych jednostek miary
1	2	3	4	5	6	7	8	9	10	11	12

[1] np. notatki, kopie, wyciągi, tłumaczenia itp.

strona prawa

Numer kopiowanego dokumentu	Imię i nazwisko osoby sporządzającej/wykonującej dokument	Imię i nazwisko osoby otrzymującej dokument, data i podpis	Potwierdzenie zwrotu dokumentu do kancelarii, data i podpis	Adnotacje o wysłaniu dokumentu lub załącznika (poz. ks. dor. przesyłek miejscowych/poz. wykazu przesyłek nadanych)	Informacje uzupełniające/Uwagi
13	14	15	16	17	18

Załącznik nr 6 do rozporządzenia

WZÓR

**KARTA ZAPOZNANIA SIĘ Z DOKUMENTEM OZNACZONYM KLAUZULĄ "ŚCIŚLE TAJNE"* / "TAJNE" *
nr .....**

	UDOSTĘPNIENIE DOKUMENTU			ZWROT DOKUMENTU			
Lp.	**imię i nazwisko osoby, której dokument udostępniono**	**data**	**podpis**	**imię i nazwisko osoby, której dokument zwrócono**	**data**	**podpis**	**Uwagi**

* Niepotrzebne skreślić.

. . . . . / . . . . .

Załącznik nr 7 do rozporządzenia

WZÓR

KSIĄŻKA DORĘCZEŃ PRZESYŁEK MIEJSCOWYCH

Numer kolejny zapisu	Data	Adresat	Numer pisma (rodzaj przesyłki)	Potwierdzenie odbioru podpis, pieczęć i data
1	2	3	4	5

strona ..... / .....

Załącznik nr 8 do rozporządzenia

WZÓR

...., dnia ...-...-... r.
(pieczęć nagłówkowa jednostki organizacyjnej) (miejscowość)

WYKAZ Nr .....
PRZESYŁEK NADANYCH

przekazanych przez .....
(nazwa i adres jednostki organizacyjnej wysyłającego)

do wysłania ..... w .....
(nazwa przewoźnika lub nazwisko doręczyciela)

Lp.	Numer przesyłki	Rodzaj przesyłki (list, paczka itp.)	Do kogo adresowany	Uwagi
1	2	3	4	5

Ogółem przesyłek: ....
(liczbowo) (słownie)

.....
(podpis sporządzającego wykaz)
.....
(podpis doręczającego)
.....
(podpis przyjmującego)
.....
(data i godzina przyjęcia)

mp.

(pieczęć przewoźnika)

Załącznik nr 9 do rozporządzenia

WZÓR

REJESTR WYDANYCH PRZEDMIOTÓW

Oznaczenie klauzuli	Nr kolejny zapisu	Data rejestracji	Rodzaj przedmiotu, pojemność (dysku, taśmy, itp.)	Imię i nazwisko pobierającego, data i podpis	Potwierdzenie zwrotu do kancelarii, data i podpis	Adnotacje o wysłaniu dokumentu (nr z Dziennika Ewidencji) lub zniszczeniu przedmiotu (nr protokołu zniszczenia)	Informacje uzupełniające/ Uwagi
1	2	3	4	5	6	7	8

UZASADNIENIE

Rozporządzenie Rady Ministrów w sprawie sposobu przeprowadzania i podstawowych kryteriów określania poziomu zagrożenia oraz doboru środków bezpieczeństwa fizycznego stanowi realizację upoważnienia ustawowego zawartego w art. 47 ust. 1 ustawy z dnia …….. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. ……).

Konieczność wydania nowego rozporządzenia w przedmiotowej sprawie jest następstwem nowelizacji ustawy o ochronie informacji niejawnych. Zmiana tej ustawy spowodowała, iż niezbędnym stało się opracowanie nowych zasad dotyczących stosowania środków ochrony fizycznej – zbliżonych do przepisów obowiązujących w innych krajach Unii Europejskiej. Zmiany zmierzają przede wszystkim w kierunku racjonalności stosowania metod i środków służących ochronie informacji niejawnych oraz adekwatności rozwiązań odpowiednich do klauzul tajności informacji, które przetwarzane są w jednostkach organizacyjnych. W projekcie rozporządzania przy doborze środków bezpieczeństwa fizycznej bierze się pod uwagę dwa elementy: klauzulę tajności informacji niejawnych oraz poziom zagrożenia ich nieuprawnionego ujawnienia lub utraty.

W porównaniu z obowiązującym rozporządzeniem wprowadzono do niego nowe rozwiązania, które pozwolą na stosowanie środków bezpieczeństwa fizycznego uwzględniających specyfikę jednostki.

W projekcie nowego rozporządzenia zobligowano kierowników jednostek organizacyjnych (dot. podmiotów dysponujących informacjami o klauzulach „ściśle tajne", „tajne" lub „poufne") do ustalenia poziomu zagrożenia nieuprawnionego ujawnienia lub utraty informacji niejawnych. W celu ujednolicenia zasad ustalania poziomu zagrożenia opracowana została tzw. matryca, tj. przedstawiono katalog zagrożeń mających wpływ na ochronę informacji niejawnych (załącznik nr 1 do rozporządzenia). W katalogu tym zostały ujęte czynniki, które decydują o poziomie zagrożenia takie jak: lokalizacja budynku, jego struktura, liczba osób mających dostęp do informacji niejawnych, ilość informacji niejawnych przetwarzanych w danej jednostce organizacyjnej.

Informacje niejawne przetwarzane będą w tzw. strefach ochronnych, które tworzy się uwzględniając poziom zagrożenia (wysoki, średni lub niski) oraz klauzule tajności informacji (§ 4 rozporządzenia). W projekcie rozporządzenia zostały zdefiniowane strefy ochronne (§ 5 rozporządzenia) oraz określone zostały kryteria tworzenia tych stref (załącznik nr 2 do rozporządzenia). Dotychczasowe przepisy obligowały jednostki organizacyjne dysponujące informacjami oznaczonymi klauzulą „poufne" lub stanowiącymi tajemnicę państwową do utworzenia strefy bezpieczeństwa, a wokół niej strefy administracyjnej. Zaproponowane rozwiązania odchodzą od konieczności tworzenia „strefy w strefie" - w projekcie rozporządzenia strefa ochronna może obejmować zarówno jedno pomieszczenie jak też szereg pomieszczeń czy też wydzielony obszar. Klasa strefy (I, II lub III) zależy od klauzuli tajności przetwarzanych informacji oraz zagrożenia ich ujawniania lub utraty.

Strefy ochronne, w których przetwarzane są informacje niejawne powinny być odpowiednio zabezpieczone w środki bezpieczeństwa fizycznego. W projekcie rozporządzenia zostały wskazane (opisane) środki ochrony fizycznej jakie należy zastosować przy zabezpieczaniu informacji niejawnych (załącznik nr 3 do rozporządzenia). Środki te stosuje się zgodnie ze wskazaniami określonymi w rozporządzeniu (§ 4 i 6 zarządzenia). Zgodnie z nowym projektem rozporządzenia więcej środków należy zastosować dla zabezpieczenia informacji niejawnych oznaczonych klauzulą „ściśle tajne" przy wysokim poziomie zagrożenia niż dla zabezpieczenia informacji niejawnych oznaczonych tą samą klauzulą tajności, ale przy niskim poziomie zagrożenia. Liczba i rodzaj środków ochrony fizycznej zależy od poziomu zagrożenia i klauzuli tajności informacji niejawnych (im mniejsze zagrożenie i niższa klauzula, tym mniej środków bezpieczeństwa fizycznego).

Przy opracowywaniu zmian w stosowaniu środków ochrony fizycznej zadbano o wprowadzenie nowych, aktualnie obowiązujących polskich normy m.in. w zakresie systemów alarmowych (załącznik nr 3 do rozporządzenia), określono m.in. rodzaje czynności, jakie powinien wykrywać system sygnalizacji włamania i napadu w zależności od stopnia zabezpieczenia.

W projekcie rozporządzania (§ 14), po raz pierwszy, wskazano elementy jakie powinien zawierać plan ochrony informacji niejawnych, o którym mowa w ustawie o ochronie informacji niejawnych. Z punktu widzenia bezpieczeństwa informacji niejawnych ma to istotne znaczenie, albowiem z jednej strony eliminuje wątpliwości dot. zawartości merytorycznej takiego dokumentu z drugiej zaś obliguje do wprowadzenia i stosowania

procedur mających wpływ na bezpieczeństwo informacji niejawnych (np. procedury przyznawania uprawnień do poruszania się w strefach ochronnych).

Istotną zmianą merytoryczną jest zrezygnowanie z prowadzenia dziennika ewidencji wykonanych dokumentów. Zmianie ulegnie także dotychczasowy wzór dziennika korespondencyjnego, który zostanie uzupełniony o dodatkowe rubryki umożliwiające m.in. rejestrowanie kopii dokumentów niejawnych. Zmianie ulegnie również nazwa tego urządzenia ewidencyjnego z „dziennika korespondencyjnego" na „dziennik ewidencji". Powodem tej zmiany było ograniczenie prowadzenia urządzeń ewidencyjnych, w których rejestrowane są dokumenty niejawne. Dokumentowi niejawnemu powinno nadawać się jeden numer ewidencyjnych – umożliwiający jego identyfikację, na potrzeby obiegu korespondencyjnego.

W § 16 ust. 2 wprowadzono urządzenie ewidencyjne „rejestr wydanych przedmiotów", którego wzór określa załącznik nr 9 do projektu rozporządzenia. Rejestr będzie służył ewidencjonowaniu wydanych nośników do zapisów informacji w postaci cyfrowej, dysków optycznych i taśm elektromagnetycznych oraz innych przedmiotów.

Ocena Skutków Regulacji

1. Podmioty, na które oddziałuje rozporządzenie

Rozwiązania prawne przyjęte w projekcie rozporządzenia dotyczą podmiotów wymienionych w art. 1 ust. 2 ustawy z dnia … o ochronie informacji niejawnych oraz o zmianie niektórych ustaw.

2. Wpływ regulacji na sektor finansów publicznych, w tym na budżet państwa i budżety jednostek samorządu terytorialnego

Wejście w życie rozporządzenia nie wywoła zwiększenia wydatków z budżetu jednostek samorządu terytorialnego, a także nie wpłynie na zwiększenie wydatków z budżetu państwa.

3. Wpływ regulacji na rynek pracy

Wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy.

4. **Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw**

Wejście w życie rozporządzenia nie wpłynie na konkurencyjność, zarówno wewnętrzną, jak i zewnętrzną gospodarki.

5. **Wpływ regulacji na sytuację i rozwój regionalny**

Wejście w życie rozporządzenia pozostanie bez wpływu na sytuację i rozwój regionalny.

6. **Zgodność z przepisami prawa Unii Europejskiej**

Przedmiotowe rozporządzenie nie jest objęte zakresem Unii Europejskiej. Projekt rozporządzenia nie zawiera przepisów technicznych i w związku z tym nie podlega procedurze notyfikacji aktów prawnych, określonej w rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039 i z 2004 r. Nr 65, poz. 597).

Projekt

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia …… r.

w sprawie trybu i sposobu nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne

Na podstawie art. 47 ust. 4 ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. …….), zwanej dalej „ustawą”, zarządza się, co następuje:

§ 1.

Rozporządzenie określa tryb i sposób przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne w celu ich zabezpieczenia przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem.

§ 2.

1. Czynności, o których mowa w § 1 na zlecenie jednostek organizacyjnych wymienionych w art. 1 ust. 2 ustawy, zwanych dalej „nadawcami”, realizują podmioty zwane dalej „przewoźnikami”:
   1) poczta specjalna podlegająca ministrowi właściwemu do spraw wewnętrznych, działająca w jednostkach organizacyjnych Policji, zapewniająca przewóz materiałów zawierających informacje niejawne do adresatów zamiejscowych na terenie kraju;
   2) właściwa komórka organizacyjna Ministerstwa Spraw Zagranicznych zapewniająca przewóz materiałów zawierających informacje niejawne poza granicami Rzeczypospolitej Polskiej;
   3) właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej;
   4) podmioty prowadzące działalność w zakresie usług pocztowych;
   5) przedsiębiorcy prowadzący działalność w zakresie ochrony osób i mienia;
   6) przedsiębiorcy prowadzący działalność w zakresie usług transportowych.
2. Przewoźnicy muszą spełniać wymagania w zakresie ochrony informacji niejawnych.

§ 3.

1. Materiały zawierające informacje niejawne oznaczone klauzulą „ściśle tajne” i „tajne” są przewożone przez przewoźników określonych w § 2 ust. 1 pkt 1-3, z zastrzeżeniem § 4.
2. W szczególnie uzasadnionych przypadkach kierownik jednostki organizacyjnej może podjąć decyzję o zleceniu przewiezienia materiałów oznaczonych klauzulą „ściśle tajne” i „tajne” przez przewoźników, o których mowa w § 2 ust. 1 pkt 4 i 5.

§ 4.

Materiały zawierające informacje niejawne, których przewóz, w szczególności z uwagi na ich znaczne rozmiary lub fakt bycia towarem niebezpiecznym w przewozie, nie może być zrealizowany przez przewoźników określonych w § 2 ust. 1 pkt 1-5, mogą być przewożone przez przewoźników, o których mowa w § 2 ust. 1 pkt 6.

§ 5.

Materiały zawierające informacje niejawne mogą być przekazywane także bez pośrednictwa przewoźników, jeżeli są zabezpieczone przed zniszczeniem oraz dostępem osób nieuprawnionych, a przewóz dokonywany jest przez nadawców lub odbiorców zgodnie z § 8 ust. 1-3 oraz § 11.

§ 6.

Nadawcy przekazują przewoźnikom materiały zawierające informacje niejawne w postaci przesyłek listowych lub paczek, zwanych dalej przesyłkami, zaadresowanych, zabezpieczonych, opakowanych i oznaczonych zgodnie z wymaganiami określonymi w § 8.

§ 7.

1. Przewoźnicy przyjmują przesyłki na podstawie wykazu przesyłek nadanych, wykonanego przez nadawcę lub na podstawie dokumentów stosowanych przez operatora pocztowego.
2. Wykaz przesyłek nadanych wykonywany jest w dwóch egzemplarzach, po jednym egzemplarzu dla nadawcy przesyłki i przewoźnika.
3. Przyjęcie przesyłki potwierdza się podpisem, zapisem liczbowym i słownym liczby przyjętych przesyłek oraz odciskiem pieczęci przewoźnika na obu egzemplarzach wykazu przesyłek nadanych.
4. Przewoźnik nie przyjmuje przesyłki nieodpowiadającej wymaganiom określonym w § 9 ust. 3 lub może odmówić przyjęcia przesyłki nieodpowiadającej wymaganiom określonym w § 8.
5. W przypadku odmowy przyjęcia przesyłki, o której mowa w ust. 4, przewoźnik wykreśla ją na obu egzemplarzach wykazu przesyłek nadanych, potwierdzając to podpisem osoby odmawiającej przyjęcia przesyłki i odciskiem pieczęci przewoźnika.

§ 8.

1. Materiały zawierające informacje niejawne, nadawane za pośrednictwem przewoźników, jako przesyłki listowe, powinny być opakowane w dwie nieprzezroczyste i mocne koperty, przy czym na kopertach muszą być umieszczone:
   1) na wewnętrznej:
      a) klauzula tajności i ewentualne dodatkowe oznaczenie;
      b) imienne określenie adresata;
      c) imię, nazwisko i podpis osoby pakującej;
      d) numer, pod którym dokument został zarejestrowany w odpowiedniej ewidencji;
   2) na zewnętrznej:
      a) nazwa jednostki organizacyjnej adresata;
      b) adres siedziby adresata;
      c) numer wykazu i pozycji w wykazie przesyłek nadanych;
      d) nazwa jednostki organizacyjnej nadawcy.
2. Miejsca sklejenia każdej koperty zabezpiecza się przez odciśnięcie pieczęci "do pakietów" oraz za pomocą przezroczystej taśmy samoprzylepnej, przy czym na kopercie zewnętrznej, zamiast tej taśmy, może być stosowana pieczęć odciśnięta w substancji zapewniającej jej trwały odcisk.
3. Materiały zawierające informacje niejawne, nadawane za pośrednictwem przewoźników w postaci paczek, muszą być opakowane w dwie nieprzezroczyste warstwy mocnego papieru, oznaczone i zabezpieczone jak w ust. 1 i 2.

4. W przypadku przekazywania materiałów zawierających informacje niejawne przez przewoźników, o których mowa w § 2 ust. 1 pkt 4, przekazuje się je, jako przesyłki polecone lub z zadeklarowaną wartością.

§ 9.

1. Przesyłki przewożone są w zamkniętych oraz zaplombowanych paczkach, workach lub innego rodzaju pojemnikach, zwanych dalej pojemnikami.
2. Na każdym pojemniku umieszcza się informację zawierającą nazwę i adres nadawcy i odbiorcy oraz pouczenie o postępowaniu ze znalezionym pojemnikiem o następującej treści: "Znalazca niniejszego pojemnika proszony jest o niezwłoczne przekazanie go najbliższej jednostce Policji. Pojemnika nie rozplombowywać i nie otwierać".
3. Przesyłki przyjmowane przez przewoźników, o których mowa w § 2 ust. 1 pkt 1-3, nie powinny przekraczać następujących wymiarów i masy:
   1) przesyłki listowe - wymiarów od 10 cm x 15 cm do 25 cm x 35 cm i masy do 0,5 kg;
   2) paczki - wymiarów od 5 cm x 10 cm x 15 cm do 35 cm x 35 cm x 35 cm i masy do 5 kg.

§ 10.

1. Przesyłki za pośrednictwem przewoźników przewozi się:
   1) środkami publicznego transportu lądowego, pod warunkiem zarezerwowania pomieszczenia na potrzeby konwoju lub zarezerwowania miejsc w sposób gwarantujący ciągły dozór przesyłki;
   2) specjalnie przystosowanymi samochodami przewoźnika, które w przypadku przewożenia materiałów niejawnych oznaczonych klauzulą „ściśle tajne” i „tajne” muszą spełniać wymagania, o których mowa w załączniku nr 3 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 14 października 1998 r. w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne (Dz. U. Nr 129, poz. 858 oraz z 2000 r. Nr 17, poz. 221);
   3) statkami powietrznymi, przy zapewnieniu wydzielonego miejsca ograniczającego dostęp osób nieuprawnionych do przesyłek lub wydzielenia miejsc gwarantujących ciągły dozór przesyłki przez konwojentów;
   4) środkami transportu wodnego, przy zapewnieniu wydzielonego miejsca, ograniczającego dostęp osób nieuprawnionych do przesyłek i konwojentów.
2. Przewóz przesyłek bez pośrednictwa przewoźników odbywa się za pomocą środków transportu drogowego, kolejowego, lotniczego lub wodnego, pod warunkiem zabezpieczenia przesyłek przed dostępem osób nieuprawnionych.
3. Od warunków, o których mowa w ust. 1 pkt 2, można odstąpić wówczas, gdy przesyłka przekazywana jest bezpośrednio od nadawcy do odbiorcy własnymi środkami transportu nadawcy lub odbiorcy.

§ 11.

1. Przesyłki zawierające informacje niejawne oznaczone klauzulą „ściśle tajne” przewożą i ochraniają konwoje złożone, co najmniej z dwóch uzbrojonych w broń palną konwojentów posiadających odpowiednie poświadczenia bezpieczeństwa, z zastrzeżeniem § 12.

2. Przesyłki zawierające informacje niejawne oznaczone klauzulą „tajne” przewozi i ochrania, co najmniej jeden uzbrojony w broń palną konwojent posiadający odpowiednie poświadczenie bezpieczeństwa.
3. Przesyłki zawierające informacje niejawne oznaczone klauzulą „poufne” i „zastrzeżone” przewozi i ochrania, co najmniej jeden konwojent posiadający stosowne dopuszczenie do informacji niejawnych.
4. Od warunku posiadania broni palnej można odstąpić w czasie przewozu przesyłek poza granicami lub za granicę Rzeczypospolitej Polskiej, a także wówczas, gdy przesyłki przekazywane są bezpośrednio od nadawcy do odbiorcy na terenie tej samej miejscowości.
5. Konwojentów wyposaża się w środki łączności umożliwiające kontakt z nimi podczas przewozu oraz w instrukcję postępowania z ochranianymi i przewożonymi przesyłkami.

§ 12.

Przesyłki zawierające informacje niejawne o klauzuli „ściśle tajne” przewożone poza granicami lub za granicę Rzeczypospolitej Polskiej mogą być przewożone i ochraniane przez jednego konwojenta po dokonaniu analizy ryzyka przez pełnomocnika do spraw ochrony informacji niejawnych w jednostce nadającej przesyłkę, jeżeli podróż odbywa się transportem lotniczym na bezpośredniej trasie przewozu, a konwojentowi do momentu wejścia na podkład statku powietrznego oraz od momentu jego opuszczenia towarzyszy inna osoba posiadająca odpowiednie poświadczenie bezpieczeństwa.

§ 13.

Materiały zawierające informacje niejawne oznaczone klauzulą „ściśle tajne” i „tajne” nie mogą być przewożone łącznie z przesyłkami niebezpiecznymi oraz stwarzającymi zagrożenie ich kradzieży, bądź uszkodzenia.

§ 14.

1. Przewóz przesyłek planuje się w taki sposób, aby dostarczane były w możliwie najkrótszym czasie do adresata.
2. Trasa przewozu przesyłki zawierającej informacje niejawne może być uzgadniana z nadawcą.

§ 15.

1. W czasie przewożenia przesyłki niedopuszczalne jest pozostawienie jej bez nadzoru konwojentów.
2. Przesyłki czasowo przechowywane powinny znajdować się w zamkniętych, chronionych miejscach, do których dostęp mogą mieć tylko osoby posiadające odpowiednie poświadczenie bezpieczeństwa lub inne przewidziane przepisami ustawy dopuszczenie do informacji niejawnych.
3. Każdy przypadek przechowywania, o którym mowa w ust. 2, należy odnotować w wykazie przesyłek nadanych w rubryce "Uwagi".
4. Załadunek, przeładunek i wyładunek przesyłki musi odbywać się pod kontrolą konwojentów, przewoźnika lub pracowników nadawcy lub adresata przesyłki.

§ 16.

1. W przypadku uszkodzenia przesyłki przewoźnik zabezpiecza ją w celu niedopuszczenia do dalszych uszkodzeń i ujawnienia jej zawartości oraz wykonuje protokół w trzech egzemplarzach, z których pierwszy wydaje się adresatowi, drugi wysyła do nadawcy, a trzeci pozostawia u przewoźnika.

2. Przesyłkę, o której mowa w ust. 1, wraz z wykonanym protokołem dotyczącym uszkodzenia przesyłki wydaje się adresatowi.
3. W przypadku odmowy przyjęcia przez adresata uszkodzonej przesyłki przewoźnik zwraca ją nadawcy wraz z protokołem, o którym mowa w ust. 1 i naniesioną na nim adnotacją o przyczynie odmowy przyjęcia przesyłki.
4. Zasady określone w ust. 1-3 stosuje się odpowiednio, w przypadkach, gdy mogło dojść do ujawnienia lub doszło do ujawnienia treści przesyłki, wyjaśniając w protokole, komu i w jakich okolicznościach jej treść mogła zostać lub została ujawniona.
5. Wzór protokołu w sprawie uszkodzenia przesyłki określa załącznik nr 1 do rozporządzenia.

§ 17.

1. Przewoźnik wydaje przesyłki upoważnionemu przedstawicielowi adresata na podstawie wykazu przesyłek wydanych, wykonanego przez przewoźnika.
2. Wzór wykazu przesyłek wydanych określa załącznik nr 2 do rozporządzenia.
3. Przedstawiciel adresata, przed odebraniem przesyłki, obowiązany jest przedstawić upoważnienie do jej odbioru.
4. Wzór upoważnienia do nadawania i odbioru przesyłek określa załącznik nr 3 do rozporządzenia.
5. W przypadku przekazania przesyłki bez pośrednictwa przewoźników, adresat przesyłki potwierdza pisemnie nadawcy ich odbiór.

§ 18.

Przesyłkę nieodebraną w terminie trzech dni roboczych od daty zawiadomienia adresata o jej nadejściu odsyła się do nadawcy.

§ 19.

1. W przypadku nieotrzymania przez adresata od przewoźnika przesyłki ujętej w wykazie przesyłek nadanych, zawiadamia on niezwłocznie o tym nadawcę.
2. Nadawca występuje do przewoźnika z żądaniem podjęcia czynności wyjaśniających, których celem jest ustalenie osób odpowiedzialnych za utratę przesyłki, oraz okoliczności, w jakich to nastąpiło, informując o tym jednocześnie – w przypadku utraty materiałów o klauzuli „poufne” i wyższej - Agencję Bezpieczeństwa Wewnętrznego, bądź - w przypadku jednostek organizacyjnych, o których mowa w art. 10 ust. 2 ustawy - Służbę Kontrwywiadu Wojskowego.
3. Przewoźnik po dokonaniu ustaleń, o których mowa w ust. 2, udziela nadawcy odpowiedzi na piśmie, nie później niż w terminie 2 tygodni od otrzymania od nadawcy żądania, informując równocześnie zgodnie z właściwością Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego.

§ 20.

1. Jeżeli zawarte umowy międzynarodowe nie stanowią inaczej, materiały zawierające informacje niejawne oznaczone klauzulą „ściśle tajne” i „tajne” przekazywane są poza granice Rzeczypospolitej Polskiej za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 1 pkt 2.
2. Materiały niejawne oznaczone klauzulą „poufne” i „zastrzeżone” mogą być przesyłane poza granice Rzeczypospolitej Polskiej za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 1 pkt 4, z uwzględnieniem zasad zabezpieczenia i pakowania określonych w § 8.

3. Materiały niejawne określone w § 4 mogą być przesyłane poza granice Rzeczypospolitej Polskiej za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 1 pkt 6, z uwzględnieniem zasad zabezpieczenia i pakowania określonych w § 9 ust. 1-2.

§ 21.

1. W przypadku, gdy zachodzi konieczność pilnego wywozu za granicę materiałów w ramach wynikających z umów międzynarodowych rozmów, konferencji lub innych kontaktów i nie istnieje możliwość przekazania materiałów za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 1 pkt 2 i 4, kierownik jednostki delegującej może zezwolić na wywóz tych materiałów, jeżeli osoba wywożąca:
   1) legitymuje się odpowiednim poświadczeniem bezpieczeństwa;
   2) zapewnia stałą osobistą ochronę i bezpośredni nadzór w czasie podróży nad przewożonym materiałem;
   3) ma zapewniony środek transportu umożliwiający bezpieczny przewóz materiałów do miejsca, w którym materiały będą wykorzystywane;
   4) posiada środek łączności umożliwiający szybki kontakt z jednostką delegującą;
   5) ma zapewnione miejsce gwarantujące bezpieczne przechowywanie tych materiałów.
2. Przed wydaniem zezwolenia, o którym mowa w ust. 1, kierownik jednostki delegującej, z wyjątkiem służb i organów, o których mowa w art. 24 ust. 5 ustawy, jest obowiązany powiadomić o potrzebie wywozu materiałów oznaczonych klauzulą „ściśle tajne" i „tajne" zgodnie z właściwością Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego. W przypadku konieczności zdeponowania tych materiałów informuje się Ministerstwo Spraw Zagranicznych lub właściwe polskie przedstawicielstwo dyplomatyczne.
3. Osobie wywożącej za granicę materiały oznaczone klauzulą „ściśle tajne" i „tajne" wydaje się paszport dyplomatyczny oraz list kurierski.
4. Osoba wywożąca za granicę materiały musi być wyposażona w instrukcję określającą zasady postępowania z tymi materiałami, wydaną przez kierownika jednostki delegujacej.
5. Osoba, która po wykorzystaniu wywiezionych materiałów oznaczonych klauzulą „ściśle tajne" i „tajne" nie powraca z nimi bezpośrednio do kraju, jest obowiązana zdeponować je w kancelarii tajnej najbliższego polskiego przedstawicielstwa lub wskazanej przez Ministerstwo Spraw Zagranicznych placówce celem przesłania ich do kraju przy wykorzystaniu przewoźnika, o którym mowa w § 2 ust. 1 pkt 2.

§ 22.

Traci moc rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. Nr 200, poz. 1650).

§ 23.

Rozporządzenie wchodzi w życie z dniem ……...

Prezes Rady Ministrów

Załączniki do rozporządzenia Prezesa Rady Ministrów
w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne

Załącznik nr 1

WZÓR

..... (pieczęć nagłówkowa przewoźnika)

....., dnia ...-...-..... r. (miejscowość)

Egz. nr .....

PROTOKÓŁ Nr .....
W SPRAWIE USZKODZENIA PRZESYŁKI

My niżej podpisani oświadczamy, że w dniu ...-...-.....r., o godz. ..., przy rozpakowaniu pakietu, pojemnika* nr ..... nadanego przez ..... w ..... stwierdzono uszkodzenie .... nr ..... adresowanego do ..... (określenie rodzaju przesyłki)

Uszkodzenie przesyłki nastąpiło w wyniku .... (rodzaj i przyczyna uszkodzenia)

Wyżej wymieniona przesyłka została przepakowana i zabezpieczona celem niedopuszczenia do dalszych uszkodzeń i doręczona adresatowi wraz z egzemplarzem nr 1 niniejszego protokołu.

Uszkodzenie przesyłki wskazuje (nie wskazuje) na możliwość ujawnienia jej treści.

Podpis przewoźnika:
.....
.....

Przyczyny odmowy przyjęcia przesyłki przez adresata:
.....
.....
.....
.....
(imię i nazwisko)

Wyk. w 3 egz.
Egz. nr 1 - adresat przesyłki
Egz. nr 2 - nadawca
Egz. nr 3 - a/a

* Niepotrzebne skreślić.

Załącznik nr 2

WZÓR

..., dnia ...-...-.....r.
(miejscowość)

.....
(pieczęć nagłówkowa placówki przewoźnika)

WYKAZ Nr ...
PRZESYŁEK WYDANYCH

.....
(nazwa jednostki organizacyjnej odbierającej przesyłki)
.....
(nazwa przewoźnika)

Lp.	Numer i rodzaj przesyłki	Nadawca	Uwagi
1	2	3	4

Ogółem przesyłek .....
(liczbowo)
.....
(słownie)

.....
(podpis sporządzającego wykaz)
.....
(podpis wydającego przesyłki)
.....
(podpis przyjmującego przesyłki)
.....
(data przyjęcia)

.....
(pieczęć do pokwitowań adresata)

Pouczenie: Wykaz wypełnić maszynowo lub odręcznie w sposób czytelny. W kolumnie 2 wpisać literę symbolizującą rodzaj przesyłki: L - dla listu, P - dla paczki, I - inne.

Załącznik nr 3
WZÓR

WZÓR UPOWAŻNIENIA
DO NADAWANIA I ODBIORU PRZESYŁEK

	..... Nr ..... **UPOWAŻNIENIE** **do nadawania i odbioru przesyłek**

Upoważniam Pana(ią) .... (imię i nazwisko) rodzaj i nr dowodu tożsamości .... wydanego przez .... do nadawania i odbioru przesyłek zawierających materiały niejawne w .... w ..... Upoważnienie ważne jest na rok ..... przy okazaniu dowodu tożsamości. pieczęć ..... (podpis wystawcy)	UWAGA Po wypełnieniu upoważnienie stanowi druk ścisłego zarachowania. W przypadku utraty upoważnienia kierownik jednostki organizacyjnej: 1) powiadamia natychmiast przewoźnika; 2) przeprowadza postępowanie wyjaśniające na okoliczność utraty upoważnienia. Ważność upoważnienia przedłuża się na rok: mp. mp. mp. mp. 20..... r. 20..... r. 20..... r. 20..... r.

UZASADNIENIE

Rozporządzenie Prezesa Rady Ministrów w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne stanowi realizację upoważnienia ustawowego zawartego w art. 47 ust. 5 ustawy z dnia …….. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. ……..).

Konieczność wydania nowego rozporządzenia w przedmiotowej sprawie jest następstwem nowelizacji ustawy o ochronie informacji niejawnych. Zmiana tej ustawy spowodowała, iż niezbędnym stało się dokonanie następujących korekt w omawianym akcie wykonawczym:

- w związku ze zmianą definicji informacji niejawnych, polegającą na rezygnacji z podziału informacji niejawnych na stanowiące tajemnicę państwową i służbową – wszystkie zwroty „tajemnica państwowa" i „tajemnica służbowa" zostały zastąpione zwrotem „informacje niejawne",
- w związku z tym, że Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego przestały być służbami ochrony państwa (w aktualnym systemie ochrony informacji niejawnych nie ma już służb ochrony państwa) – wszystkie zwroty „właściwa służba ochrony państwa" zostały zastąpione zwrotem „zgodnie z właściwością Agencja Bezpieczeństwa Wewnętrznego lub Służba Kontrwywiadu Wojskowego".

Projekt nowego rozporządzenia Prezesa Rady Ministrów w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne, poza wprowadzeniem zmian będących następstwem wejścia w życie nowej ustawy, ma również na celu usystematyzowanie regulowanej problematyki oraz wyeliminowanie jednostek redakcyjnych dublujących de facto te same treści. W tym celu zmieniona została kolejność kilku dotychczasowych paragrafów (tak by kwestie nimi regulowane stanowiły logiczną całość), a niektóre z nich zostały skreślone.

Istotną zmianą merytoryczną, w stosunku do dotychczasowych przepisów w tym zakresie, jest rezygnacja z wyszczególnienia „Poczty Polskiej" wśród przewoźników

prowadzących działalność w zakresie usług pocztowych. Ma to związek z komercjalizacją tego przedsiębiorstwa oraz postępująca demonopolizacją rynku usług pocztowych.

Konsekwencją uproszczenia nazewnictwa w systemie ochrony informacji niejawnych polegającego na zastąpieniu stosowanego wcześniej rozróżnienia „wykonujący" oraz „sporządzający" pojęciem „wykonawca" (w związku z uznaniem, że pojęcie „wykonawca" jest szersze od „sporządzającego") stało się uaktualnienie terminologii również w nowelizowanym rozporządzeniu. Nowe pojęcie zastosowano co do wskazania osoby przygotowującej dokument lub materiał jako „wykonawcy" i co do podejmowanych przez nią czynności, czyli przygotowania dokumentacji jako „wykonania".

W § 8 ujednolicono sposób opakowywania i oznaczenia przesyłek listowych i paczek zawierających informacje niejawne; obecnie klauzula tajności nie determinuje sposobu opakowania i oznaczenia materiału zawierającego informację niejawną.

Kierując się względami racjonalności w § 11 zmienione zostały także zasady konwojowania materiałów zawierających informacje niejawne w ten sposób, że:

a) rozróżniono zasady przewożenia materiałów zawierających informacje niejawne oznaczone klauzulą „ściśle tajne" i „tajne"; dotychczas oba rodzaje tych informacji przewoziły konwoje złożone z co najmniej dwóch uzbrojonych w broń palną konwojentów, obecnie ten sposób pozostał aktualny tylko dla informacji niejawnych oznaczonych klauzulą „ściśle tajne", a informacje niejawne oznaczone klauzulą „tajne" będzie mógł przewozić i ochraniać co najmniej jeden uzbrojony w broń palną konwojent posiadający odpowiednie poświadczenie bezpieczeństwa,

b) zmienione zostały zasady konwojowania materiałów zawierających informacje niejawne oznaczonych klauzulą „poufne" i „zastrzeżone"; zarówno jedne, jak i drugie (a nie jak dotychczas tylko o klauzuli „poufne"), będzie przewoził i ochraniał co najmniej jeden konwojent posiadający stosowne dopuszczenie do informacji niejawnych; zrezygnowano natomiast z konieczności posiadania przez niego broni palnej,

c) scalone zostały ust. 3 i 5, dotyczące odstępstw od posiadania broni palnej przez konwojentów.

Treść proponowanego § 12 wynika z propozycji Ministerstwa Spraw Zagranicznych. Rozwiązanie ograniczające liczbę konwojentów na trasach zagranicznych (zarówno za granicę jak i za granicą) pozwoli przede wszystkim na znaczne zmniejszenie kosztów przewożenia i ochraniania przesyłek zawierających informacje niejawne, o ile taka podróż odbywa się transportem lotniczym na bezpośredniej trasie przewozu. Jednoczesne

wprowadzenie ograniczeń w postaci obowiązku towarzyszenia konwojentowi do chwili wejścia na pokład samolotu oraz jego opuszczenia wprowadza dodatkowe gwarancje należytej ochrony przesyłek. Nałożenie na pełnomocnika ochrony obowiązku każdorazowego badania ryzyka związanego z konkretną podróżą umożliwi odrębne traktowanie każdego przypadku przewożenia takich przesyłek.

W dotychczasowym § 14 (obecnie § 15) z ust. 1 został wykreślony zwrot uszczegóławiający miejsca, w których przewożone przesyłki nie mogą pozostać bez nadzoru; zdaniem projektodawcy to doprecyzowanie było zbędne, gdyż w ustępie tym wyrażony został ogólny zakaz pozostawiania bez nadzoru przesyłki zawierającej informacje niejawne,

Zmianie - w stosunku do Rozporządzenia Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. Nr 200, poz. 1650) - nie ulegają wzory: Protokołu w sprawie uszkodzenia przesyłki, Wykazu przesyłek wydanych oraz Wzór upoważnienia do nadania i odbioru przesyłek stanowiące załączniki do rozporządzenia.

Ocena Skutków Regulacji

1. **Podmioty, na które oddziałuje rozporządzenie**

Zakres oddziaływania znowelizowanych przepisów rozporządzenia jest ograniczony do przewoźników przesyłek zawierających informacje niejawne (wymienionych w § 2 rozporządzenia) oraz podmiotów wymienionych w art. 1 ust. 2 ustawy o ochronie informacji niejawnych

2. **Wpływ regulacji na sektor finansów publicznych, w tym na budżet państwa i budżety jednostek samorządu terytorialnego**

Przewidywana zmiana rozporządzenia zmniejszy koszty podróży kurierskich co w konsekwencji pociągnie za sobą oszczędności dla budżetu państwa w kwocie……

3. **Wpływ regulacji na rynek pracy**

Wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy.

4. **Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw**

Wejście w życie rozporządzenia nie wpłynie na konkurencyjność, zarówno wewnętrzną, jak i zewnętrzną gospodarki.

5. **Wpływ regulacji na sytuację i rozwój regionalny**

Wejście w życie rozporządzenia pozostanie bez wpływu na sytuację i rozwój regionalny.

6. **Zgodność z przepisami prawa Unii Europejskiej**

Przedmiotowe rozporządzenie nie jest objęte zakresem Unii Europejskiej. Projekt rozporządzenia nie zawiera przepisów technicznych i w związku z tym nie podlega procedurze notyfikacji aktów prawnych, określonej w rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz.U. Nr 239, poz. 2039 i z 2004 r. Nr 65, poz. 597).

40-02-aa

Projekt

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW

z dnia ……

w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

Na podstawie art. 49 ust. 10 ustawy z dnia … o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. z … r., Nr …, poz. …), zwanej dalej ustawą, zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne służące do przetwarzania informacji niejawnych;
2) sposób opracowywania dokumentacji bezpieczeństwa systemów teleinformatycznych.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

1) ABW — należy przez to rozumieć Agencję Bezpieczeństwa Wewnętrznego;
2) autentyczności — należy przez to rozumieć właściwość określającą, że tożsamość podmiotu lub zasobu jest taka jak deklarowana;
3) dedykowanym trybie bezpieczeństwa pracy — należy przez to rozumieć tryb bezpieczeństwa pracy, w którym wszyscy użytkownicy systemu teleinformatycznego posiadają poświadczenia bezpieczeństwa o klauzuli nie mniejszej niż maksymalna klauzula tajności informacji przetwarzanych w systemie, formalną zgodę na dostęp do wszystkich kategorii informacji przetwarzanych w systemie oraz jednakową potrzebę dostępu do wszystkich informacji przetwarzanych w systemie;
4) dostępności — należy przez to rozumieć właściwość określającą, że zasób jest możliwy do wykorzystania na żądanie, w założonym czasie, przez uprawniony podmiot;
5) incydencie bezpieczeństwa teleinformatycznego — należy przez to rozumieć każde zdarzenie, które może mieć negatywny wpływ na bezpieczeństwo zasobów systemu teleinformatycznego, spowodowane w szczególności awarią systemu teleinformatycznego, działaniem osób uprawnionych lub nieuprawnionych do pracy w tym systemie albo zaniechaniem osób uprawnionych;
6) informatycznym nośniku danych — należy przez to rozumieć informatyczny nośnik danych w rozumieniu art. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r., nr 64, poz. 565);
7) integralności — należy przez to rozumieć właściwość określającą, że zasób nie został zmodyfikowany w sposób nieuprawniony;

8) kategorii informacji — należy przez to rozumieć grupę informacji niejawnych, dla których, poza wymogiem posiadania stosownego poświadczenia bezpieczeństwa, wymagana jest formalna (udokumentowana) zgoda na dostęp;

9) niezaprzeczalności — należy przez to rozumieć właściwość określającą, że podmioty uczestniczące w wymianie informacji nie mogą zanegować swego uczestnictwa w całości lub części tej wymiany;

10) podatności — należy przez to rozumieć słabość zasobu lub zabezpieczenia, która może zostać wykorzystana przez zagrożenie;

11) połączeniu międzysystemowym — należy przez to rozumieć techniczne lub organizacyjne połączenie dwóch lub więcej zarządzanych przez różne podmioty systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;

12) poufności — należy przez to rozumieć właściwość określającą, że informacja nie jest udostępniana lub ujawniana nieuprawnionym do tego podmiotom;

13) przedziałowym trybie bezpieczeństwa pracy — należy przez to rozumieć tryb bezpieczeństwa pracy, w którym wszyscy użytkownicy systemu teleinformatycznego posiadają poświadczenia bezpieczeństwa o klauzuli nie mniejszej niż maksymalna klauzula tajności informacji przetwarzanych w systemie, ale nie wszyscy użytkownicy posiadają formalną zgodę na dostęp do wszystkich kategorii informacji przetwarzanych w systemie oraz nie wszyscy użytkownicy posiadają jednakową potrzebę dostępu do wszystkich informacji przetwarzanych w systemie;

14) przekazywaniu informacji — należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone;

15) rozliczalności — należy przez to rozumieć właściwość określającą, że działania podmiotu mogą być jednoznacznie przypisane tylko temu podmiotowi;

16) ryzyku — należy przez to rozumieć kombinację prawdopodobieństwa zdarzenia i jego konsekwencji;

17) SKW — należy przez to rozumieć Służbę Kontrwywiadu Wojskowego;

18) strefie kontrolowanego dostępu — należy przez to rozumieć obszar, do którego możliwość wstępu mają jedynie osoby uprawnione;

19) systemowym trybie bezpieczeństwa pracy — należy przez to rozumieć tryb bezpieczeństwa pracy, w którym wszyscy użytkownicy systemu teleinformatycznego posiadają poświadczenia bezpieczeństwa o klauzuli nie mniejszej niż maksymalna klauzula tajności informacji przetwarzanych w systemie oraz formalną zgodę na dostęp do wszystkich kategorii informacji przetwarzanych w systemie, ale nie wszyscy użytkownicy posiadają jednakową potrzebę dostępu do wszystkich informacji przetwarzanych w systemie;

20) testach bezpieczeństwa — należy przez to rozumieć testy poprawności funkcjonowania zabezpieczeń w systemie teleinformatycznym;

21) trybie bezpieczeństwa pracy — należy przez to rozumieć tryb pracy systemu teleinformatycznego określający rodzaj użytkowników systemu pod względem posiadanego poświadczenia bezpieczeństwa, posiadanej formalnej zgody na dostęp do kategorii informacji przetwarzanych w systemie oraz posiadanej po-

trzeby dostępu do informacji przetwarzanych w systemie (wyróżnia się cztery tryby bezpieczeństwa pracy: dedykowany, systemowy, przedziałowy i wielopoziomowy);

22) wielopoziomowym trybie bezpieczeństwa pracy — należy przez to rozumieć tryb bezpieczeństwa pracy, w którym nie wszyscy użytkownicy systemu teleinformatycznego posiadają poświadczenia bezpieczeństwa o klauzuli co najmniej równej maksymalnej klauzuli tajności informacji przetwarzanych w systemie, nie wszyscy użytkownicy posiadają formalną zgodę na dostęp do wszystkich kategorii informacji przetwarzanych w systemie oraz nie wszyscy użytkownicy posiadają jednakową potrzebę dostępu do wszystkich informacji przetwarzanych w systemie;

23) zabezpieczeniu — należy przez to rozumieć środki o charakterze fizycznym, technicznym lub administracyjnym zmniejszające ryzyko;

24) zagrożeniu — należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w systemie teleinformatycznym lub organizacji;

25) zasobach systemu teleinformatycznego — należy przez to rozumieć przetwarzane w systemie teleinformatycznym informacje niejawne, jak również usługi, oprogramowanie, dane i sprzęt mające wpływ na bezpieczeństwo tych informacji.

Rozdział 2

Podstawowe wymagania bezpieczeństwa teleinformatycznego

§ 3. 1. Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym zapewnia się przez wdrożenie spójnego zbioru zabezpieczeń z zakresu bezpieczeństwa fizycznego, osobowego i teleinformatycznego, w celu stworzenia bezpiecznego środowiska pracy systemu teleinformatycznego oraz realizacji następujących celów bezpieczeństwa:

1) zapewnienia poufności informacji niejawnych;

2) zapewnienia integralności informacji niejawnych;

3) zapewnienia dostępności informacji niejawnych.

2. Aby zrealizować cele bezpieczeństwa, o których mowa w ust. 1, w systemie teleinformatycznym stosuje się:

1) zasadę zarządzania ryzykiem, polegającą na objęciu systemu teleinformatycznego procesem zarządzania ryzykiem, o którym mowa w rozdziale 3;

2) zasadę minimalnej funkcjonalności, polegającą na instalowaniu i wykorzystywaniu w systemie teleinformatycznym wyłącznie funkcji, protokołów i usług niezbędnych dla prawidłowej realizacji zadań, do których system został przeznaczony;

3) zasadę ograniczania przywilejów, polegającą na nadawaniu użytkownikom systemu teleinformatycznego jedynie takich przywilejów i uprawnień, jakie są im niezbędne do wykonywania zadań służbowych;

4) zasadę wielopoziomowej ochrony systemu, polegającą na stosowaniu zabezpieczeń na możliwie wielu różnych poziomach organizacji ochrony systemu te-

leinformatycznego, w celu ograniczenia występowania przypadków, w których przełamanie pojedynczego zabezpieczenia skutkuje naruszeniem celów bezpieczeństwa;

5) zasadę ograniczonego zaufania, polegającą na tym, że system teleinformatyczny powinien traktować pozostałe systemy teleinformatyczne jak niezaufane i posiadać zabezpieczenia kontrolujące wymianę informacji z tymi systemami;

6) zasadę weryfikacji sposobu realizacji ochrony systemu teleinformatycznego, polegającą na potwierdzeniu zastosowania zasad określonych w pkt 1–5 oraz okresowym sprawdzaniu poprawności działania zabezpieczeń wdrożonych w systemie teleinformatycznym.

3. Projektując zbiór zabezpieczeń, o których mowa w ust. 1, uwzględnia się, odpowiednio do zadań realizowanych przez system teleinformatyczny:

1) środki realizujące identyfikację i uwierzytelnienie osób uprawnionych do korzystania z systemu teleinformatycznego;

2) środki realizujące nadzór nad zapoznawaniem się z informacjami oraz zapewniające kontrolę dostępu do zasobów systemu teleinformatycznego, z uwzględnieniem porzeby dostępu do informacji;

3) środki weryfikacji źródła pochodzenia oraz integralności zasobów systemu teleinformatycznego;

4) środki zapewniające integralność zasobów systemu teleinformatycznego;

5) środki zapewniające dostępność zasobów systemu teleinformatycznego;

6) środki kontroli połączeń międzysystemowych;

7) środki oceny i weryfikacji poprawności działania poszczególnych zabezpieczeń w całym cyklu życia systemu;

8) środki rejestrujące działania użytkowników oraz systemu teleinformatycznego;

9) środki zapewniające autentyczność i niezaprzeczalność;

10) środki ochrony informacji niejawnych zapisanych na informatycznych nośnikach danych, w przypadku nie zapewnienia właściwego bezpieczeństwa fizycznego.

4. Zabezpieczenia, o których mowa w ust. 1, wdraża się na podstawie wyników szacowania ryzyka dla systemu teleinformatycznego, z uwzględnieniem klauzul informacji przewarzanych w systemie, trybu bezpieczeństwa pracy systemu oraz zaleceń, o których mowa w art. 48 ust. 3 ustawy.

§ 4. 1. Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym uwzględnia się w całym cyklu życia systemu teleinformatycznego, składającym się z etapów:

1) planowania;

2) projektowania;

3) wdrażania;

4) eksploatacji;

5) wycofywania.

2. Na etapie planowania ustala się potrzeby w zakresie przetwarzania informa-

cji niejawnych w systemie teleinformatycznym, a w szczególności określa się:

1) przeznaczenie systemu teleinformatycznego;
2) maksymalną klauzulę tajności oraz ilość informacji planowanych do przetwarzania w systemie;
3) tryb bezpieczeństwa pracy systemu;
4) liczbę użytkowników;
5) rozległość i planowane obciążenie systemu;
6) planowaną lokalizację.

3. Na etapie projektowania:

1) przeprowadza się wstępne szacowanie ryzyka dla projektowanego systemu teleinformatycznego w celu określenia wymagań dla zabezpieczeń;
2) dokonuje się wyboru zabezpieczeń dla systemu teleinformatycznego, z uwzględnieniem wyników wstępnego szacowania ryzyka;
3) opracowuje się dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego.

4. Na etapie wdrażania:

1) pozyskuje i wdraża się urządzenia lub narzędzia realizujące zabezpieczenia w systemie teleinformatycznym;
2) przeprowadza się testy bezpieczeństwa systemu teleinformatycznego;
3) przeprowadza się szacowanie ryzyka dla systemu teleinformatycznego z uwzględnieniem wprowadzonych zabezpieczeń;
4) opracowuje się dokument procedur bezpiecznej eksploatacji oraz uzupełnienia dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego;
5) system teleinformatyczny poddaje się akredytacji bezpieczeństwa teleinformatycznego.

5. Na etapie eksploatacji:

1) utrzymuje się zgodność systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu teleinformatycznego;
2) zapewnia się ciągłość procesu zarządzania ryzykiem w systemie teleinformatycznym;
3) okresowo przeprowadza się testy bezpieczeństwa w celu weryfikacji poprawności działania poszczególnych zabezpieczeń oraz usuwa stwierdzone nieprawidłowości;
4) w zależności od potrzeb wprowadza się modyfikacje do systemu teleinformatycznego oraz, jeśli jest to właściwe, wykonuje testy bezpieczeństwa, a także uaktualnia dokumentację bezpieczeństwa systemu teleinformatycznego. Modyfikacje systemu teleinformatycznego mające wpływ na jego bezpieczeństwo wymagają zgody podmiotu, który udzielił akredytacji bezpieczeństwa teleinformatycznego oraz mogą wymagać ponownego udzielenia akredytacji bezpieczeństwa teleinformatycznego.

6. Na etapie wycofywania systemu teleinformatycznego z eksploatacji, bezpieczeństwo informacji niejawnych, które były przetwarzane w tym systemie, zapewnia się poprzez właściwe zniszczenie lub archiwizację tych informacji.

§ 5. 1. System teleinformatyczny obsługiwany jest przez wyspecjalizowany personel zgodnie z procedurami zawartymi w dokumentacji bezpieczeństwa systemu teleinformatycznego.

2. Przed dopuszczeniem osób do pracy w systemie teleinformatycznym zapewnia się ich przeszkolenie z zakresu bezpieczeństwa teleinformatycznego oraz zaznajamia z procedurami bezpiecznej eksploatacji w zakresie jaki ich dotyczy.

§ 6. Inspektor bezpieczeństwa teleinformatycznego bierze udział w szacowaniu ryzyka dla bezpieczeństwa informacji przetwarzanych w systemie teleinformatycznym, a w ramach bieżącej kontroli zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji prowadzi kontrolę:

1) poprawności realizacji zadań przez administratora, a w szczególności właściwą eksploatację zabezpieczeń, zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom;
2) znajomości i przestrzegania przez użytkowników zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie teleinformatycznym, w szczególności w zakresie wykorzystywania urządzeń i narzędzi służących do ochrony informacji niejawnych;
3) stanu zabezpieczeń systemu teleinformatycznego, w szczególności analizując rejestry zdarzeń systemu teleinformatycznego.

§ 7. W ramach odpowiedzialności za funkcjonowanie systemu teleinformatycznego oraz przestrzeganie zasad i wymagań bezpieczeństwa dla systemu teleinformatycznego administrator w szczególności:

1) wdraża zabezpieczenia w systemie teleinformatycznym;
2) prowadzi szkolenia użytkowników systemu z zakresu jego eksploatacji oraz wykorzystania zabezpieczeń;
3) utrzymuje zgodność systemu z jego dokumentacją bezpieczeństwa;
4) udziela wsparcia w procesie zarządzania ryzykiem w systemie teleinformatycznym, w szczególności przez:
   a) informowanie o stwierdzonych naruszeniach bezpieczeństwa,
   b) informowanie o zmianach poziomu istniejących lub pojawieniu się nowych zagrożeń bądź podatności w systemie,
   c) systematyczne kontrolowanie funkcjonowania zabezpieczeń w systemie oraz poprawności działania systemu.

§ 8. 1. Informacje niejawne przetwarzane w systemie teleinformatycznym chroni się przed nieuprawnionym dostępem, a w tym przed podglądem i podsłuchem.

2. W celu zapewnienia kontroli dostępu do systemu teleinformatycznego:

1) ustala się warunki i sposób przydzielania uprawnień do pracy w systemie;

2) chroni się informacje i materiały umożliwiające dostęp do systemu teleinformatycznego, odpowiednio do klauzuli informacji, do których dostęp umożliwiają;

3) elementy systemu teleinformatycznego, istotne dla jego bezpieczeństwa, instaluje się w sposób zapewniający możliwość wykrycia prób fizycznego dostępu lub wprowadzenia nieuprawnionych zmian.

3. W systemie teleinformatycznym przetwarzającym informacje niejawne oznaczone klauzulą „poufne" lub wyższą wprowadza się, odpowiednio do wyników szacowania ryzyka dla informacji niejawnych, środki zapobiegawcze ograniczające elektromagnetyczną emisję ujawniającą pochodzącą z elementów systemu teleinformatycznego, przez umieszczanie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej lub stosowanie urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.

4. Podczas przekazywania informacji niejawnych w formie transmisji poza strefę kontrolowanego dostępu stosuje się urządzenia lub narzędzia kryptograficzne zapewniające poufność tych informacji, a jeśli to właściwe również integralność, niezaprzeczalność lub autentyczność.

§ 9. Urządzenie lub narzędzie przeznaczone do ochrony informacji niejawnych, dla którego został wydany przez ABW lub SKW certyfikat ochrony kryptograficznej lub elektromagnetycznej, podlega ochronie do momentu jego zniszczenia. Sposób niszczenia danego typu urządzenia lub narzędzia ustala się z ABW lub SKW.

§ 10. W systemie teleinformatycznym przetwarzającym informacje niejawne należy tworzyć, zabezpieczać integralność i przechowywać rejestry zdarzeń w zakresie niezbędnym do zapewnienia przeglądu, analizy oraz dostarczania dowodów działań naruszających bezpieczeństwo informacji, jak również w celu rozliczania działań indywidualnych użytkowników.

§ 11. System teleinformatyczny zabezpiecza się przed działaniem oprogramowania złośliwego.

§ 12. 1. W celu zapewnienia dostępności zasobów, w systemie teleinformatycznym wprowadza się w szczególności:

1) zasady tworzenia i przechowywania kopii zapasowych;

2) procedury postępowania w sytuacjach kryzysowych, w tym w przypadkach awarii elementów systemu;

3) monitorowanie stanu technicznego i wydajności systemu.

2. W zależności od potrzeb oraz wyników szacowania ryzyka, w celu zapewnienia dostępności zasobów systemu teleinformatycznego stosuje się redundancję sprzętu i łączy komunikacyjnych oraz zasilanie awaryjne.

3. W zależności od potrzeb oraz wyników szacowania ryzyka, transmisję danych w systemie teleinformatycznym chroni się przed wykryciem, przechwyceniem lub zakłócaniem, stosując w szczególności:

1) maskowanie ruchu;

2) zmianę parametrów transmisji.

§ 13. 1. W przypadku organizacji połączenia międzysystemowego uwzględnia się zasadę ograniczonego zaufania, o której mowa w § 3 ust. 2 pkt 5.

2. Organizując połączenie międzysystemowe dla systemów teleinformatycznych przetwarzających informacje niejawne o różnych klauzulach tajności, wdraża się zabezpieczenia uniemożliwiające przekazywanie informacji o wyższej klauzuli tajności do systemu przetwarzającego informacje o klauzuli niższej.

3. Połączenie międzysystemowe narodowych systemów teleinformatycznych z systemami teleinformatycznymi innych państw lub organizacji międzynarodowych musi spełniać zarówno wymagania narodowe, jak również wymagania tych państw bądź organizacji.

§ 14. 1. Informatyczne nośniki danych przeznaczone do przekazywania lub przechowywania informacji niejawnych obejmuje się ochroną od momentu oznaczenia klauzulą tajności aż do ich fizycznego zniszczenia lub zniesienia klauzuli tajności, o którym mowa w ust. 3.

2. Informacje niejawne przekazywane poza strefę kontrolowanego dostępu na informatycznych nośnikach danych chroni się:

1) z wykorzystaniem urządzeń lub narzędzi kryptograficznych, odpowiednich do klauzuli tajności przekazywanych informacji lub
2) przez spełnienie wymagań, o których mowa w przepisach w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów, w celu ich zabezpieczenia przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem.

3. Przed obniżeniem lub zniesieniem klauzuli tajności informatycznego nośnika danych przeprowadza się proces wymazywania danych z wykorzystaniem metod i narzędzi uzgodnionych z ABW lub SKW.

4. Możliwość obniżenia lub zniesienia klauzuli tajności oraz sposób fizycznego niszczenia informatycznych nośników danych i innych elementów systemu teleinformatycznego, które mogą przechowywać informacje niejawne, uzgadnia się z ABW lub SKW.

§ 15. System teleinformatyczny wyposaża się w mechanizmy i procedury umożliwiające wykrywanie incydentów bezpieczeństwa teleinformatycznego oraz zapewniające niezwłoczne informowanie o tym odpowiednich osób.

Rozdział 3

Zarządzanie ryzykiem w systemie teleinformatycznym

§ 16. 1. Zarządzanie ryzykiem w systemie teleinformatycznym polega na realizacji procesów:

1) szacowania ryzyka;
2) postępowania z ryzykiem;
3) akceptacji ryzyka;
4) komunikowania ryzyka;
5) przeglądu i monitorowania ryzyka.

2. Kierownik jednostki organizacyjnej organizującej system teleinformatyczny, odpowiada za zapewnienie ciągłości procesu zarządzania ryzykiem dla tego systemu.

3. W sytuacji, gdy system teleinformatyczny jest użytkowany przez kilka niezależnych jednostek organizacyjnych, każdy kierownik jednostki organizacyjnej użytkującej system teleinformatyczny, współdziała z osobą, o której mowa w ust. 2 w celu zapewnienia ciągłości procesu zarządzania ryzykiem dla tego systemu.

§ 17. 1. Szacowanie ryzyka obejmuje:

1) analizę ryzyka, na którą składają się:
   a) identyfikacja ryzyka,
   b) estymacja ryzyka,
2) ocenę ryzyka.

2. W ramach identyfikacji ryzyka określa się:

1) zasoby systemu teleinformatycznego;
2) zagrożenia;
3) podatności;
4) wdrożone zabezpieczenia;
5) konsekwencje wykorzystania przez poszczególne zagrożenia odpowiadających im podatności, a w szczególności naruszenia celów bezpieczeństwa.

3. W procesie estymacji ryzyka wyznacza się poziomy zidentyfikowanych ryzyk.

4. Ocena ryzyka polega na porównaniu wyznaczonych poziomów ryzyk z przyjętymi dla systemu teleinformatycznego kryteriami w celu określenia znaczenia poszczególnych ryzyk dla bezpieczeństwa systemu teleinformatycznego. Na podstawie oceny podejmuje się decyzję co do dalszego postępowania z ryzykami.

5. Wstępne szacowanie ryzyka przeprowadza się przed podjęciem decyzji o wprowadzeniu niezbędnych zabezpieczeń w systemie teleinformatycznym.

6. Wyniki wstępnego szacowania ryzyka, o którym mowa w ust. 5:

1) przedstawia się w dokumentacji bezpieczeństwa systemu teleinformatycznego;
2) wykorzystuje się w procesie projektowania zabezpieczeń dla danego systemu teleinformatycznego przeciwdziałających zidentyfikowanym zagrożeniom;
3) zachowuje się jako podstawę do przyszłych uaktualnień.

7. Szacowanie ryzyka przeprowadza się ponownie:

1) w przypadku wprowadzania zmian w systemie teleinformatycznym;
2) po wykryciu nowych zagrożeń lub zidentyfikowaniu nowych podatności, które nie były rozpatrywane podczas wcześniejszego szacowania ryzyka;
3) w przypadku zaistnienia poważnego incydentu bezpieczeństwa teleinformatycznego;

4) jeśli zmianie lub rozszerzeniu uległo przeznaczenie, zadania, funkcjonalność lub znaczenie systemu teleinformatycznego dla realizacji zadań statutowych jednostki organizacyjnej;

5) okresowo, w celu zachowania ciągłości procesu zarządzania ryzykiem.

8. Częstotliwość okresowego przeprowadzania szacowania ryzyka, o którym mowa w ust. 7 pkt. 5 określa się w dokumentacji bezpieczeństwa systemu teleinformatycznego.

§ 18. 1. Postępowanie z ryzykiem obejmuje:

1) obniżanie ryzyka poprzez wdrażanie zabezpieczeń;

2) pozostawienie ryzyka na poziomie określonym w trakcie estymacji ryzyka i zaniechanie dalszych działań;

3) unikanie ryzyka poprzez nie podejmowanie działań będących źródłem ryzyka;

4) przeniesienie ryzyka w całości lub części na inny podmiot.

2. Doboru zabezpieczeń dokonuje się z uwzględnieniem zaleceń, o których mowa w art. 48 ust. 3 ustawy.

3. Poziom ryzyka, pozostający po procesie postępowania z ryzykiem nosi nazwę ryzyka szczątkowego i podlega procesowi akceptacji ryzyka.

4. Dla ryzyk szczątkowych, które nie mogą być zaakceptowane ze względu na ich zbyt wysoki poziom, należy ponownie przeprowadzić proces postępowania z ryzykiem.

5. Przeprowadzenie procesu postępowania z ryzykiem może powodować konieczność powtórnego przeprowadzenia szacowania ryzyka.

§ 19. Proces akceptacji ryzyka polega na formalnym i świadomym zaakceptowaniu ryzyka szczątkowego, wraz z jego ewentualnymi konsekwencjami, przez kierownika jednostki organizacyjnej na podstawie przyjętych kryteriów akceptacji zawartych w dokumentacji bezpieczeństwa systemu teleinformatycznego.

§ 20. 1. Proces komunikowania ryzyka polega na wzajemnej wymianie informacji dotyczących ryzyka, między odpowiedzialnymi za zarządzanie ryzykiem, a innymi zainteresowanymi stronami.

2. Informacja wymieniana w procesie komunikowania ryzyka może dotyczyć występowania, natury, formy, prawdopodobieństwa, wagi, akceptowalności, kontroli, postępowania, wykrywalności oraz innych aspektów ryzyka.

3. Komunikowanie ryzyka przebiega na każdym etapie zarządzania ryzykiem.

§ 21. Proces przeglądu i monitorowania ryzyka polega na:

1) ciągłym monitorowaniu i regularnym przeglądzie czynników ryzyka w celu wykrycia zmian we wczesnym ich stadium i możliwie szybkim na nie reagowaniu;

2) ciągłym monitorowaniu, regularnym przeglądzie i udoskonalaniu procesu zarządzania ryzykiem w celu zapewnienia jego prawidłowości i skuteczności stosownie do zmieniających się okoliczności.

§ 22. W procesie zarządzania ryzykiem uwzględnia się zalecenia, o których mowa w art. 48 ust. 3 ustawy.

Rozdział 4

Dokumentacja bezpieczeństwa teleinformatycznego

§ 23. 1. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego opracowuje się po przeprowadzeniu szacowania ryzyka dla informacji niejawnych, które mają być przetwarzane w systemie teleinformatycznym, z uwzględnieniem warunków charakterystycznych dla jednostki organizacyjnej.

2. Pierwszym etapem formułowania dokumentu szczególnych wymagań bezpieczeństwa jest ustalenie wstępnej, zwięzłej i jednoznacznej definicji systemu obejmującej następujące aspekty:

1) rodzaje informacji, które będą przetwarzane, ich kategorie i klauzule tajności;
2) rodzaje użytkowników systemu uwzględniające posiadane poświadczenia bezpieczeństwa, formalną zgodę na dostęp do kategorii informacji przetwarzanych w systemie oraz posiadaną potrzebę dostępu do informacji przetwarzanych w systemie;
3) tryb bezpieczeństwa pracy systemu;
4) przeznaczenie i funkcjonalność systemu;
5) wymagania eksploatacyjne dla wymiany informacji i połączeń z innymi systemami;
6) opis środowiska systemu obejmujący dane dotyczące elementów wchodzących w skład systemu w zakresie:
   a) typu wykorzystywanych urządzeń oraz oprogramowania,
   b) lokalizacji,
   c) granic systemu, w tym sposobu realizowania połączeń wewnętrznych oraz zewnętrznych,
   d) funkcjonalności poszczególnych elementów systemu.

3. Dokument szczególnych wymagań bezpieczeństwa zawiera informację o metodologii użytej w procesie szacowania ryzyka, raport z tego procesu, opis zastosowanych zabezpieczeń, opis ryzyk szczątkowych oraz deklarację ich akceptacji.

§ 24. Opis zaproponowanych zabezpieczeń, który jest główną częścią dokumentu szczególnych wymagań bezpieczeństwa, odnosi się do następujących zagadnień:

1) w zakresie zarządzania:
   a) zarządzanie ryzykiem związane z komunikowaniem ryzyka, okresowym przeglądem i monitorowaniem ryzyka,
   b) planowanie zmian w systemie teleinformatycznym, w tym dotyczące aktualizacji dokumentacji bezpieczeństwa systemu,
   c) nabywanie elementów systemu i usług w poszczególnych etapach cyklu życia systemu,
   d) ocena bezpieczeństwa systemu;

2) w zakresie eksploatacji:

   a) zapewnienie bezpieczeństwa osobowego,

   b) zapewnienie bezpieczeństwa fizycznego, w tym granice i lokalizację stref ochronnych oraz środki ich ochrony, jak również ochrona przed ulotem elektromagnetycznym,

   c) zapewnienie ciągłości działania, w tym tworzenie kopii zapasowych, odzyskania systemu oraz, jeżeli to właściwe, zapewnienie alternatywnych łaczy telekomunikacyjnych,

   d) zarządzanie konfiguracją, w tym ustawienia konfiguracyjne z zapewnieniem niezbędnej funkcjonalności, kontrola zmian konfiguracji obejmująca testy bezpieczeństwa w celu określenia wpływu planowanej zmiany na funkcjonujące w systemie zabezpieczenia, weryfikację poprawności wdrożenia zmiany, stosownej aktualizacji dokumentacji bezpieczeństwa systemu teleinformatycznego oraz zapoznania użytkowników systemu teleinformatycznego z wprowadzonymi modyfikacjami lub przeprowadzenia uzupełniających szkoleń,

   e) utrzymanie systemu, w tym dokonywanie przeglądów diagnostycznych i napraw, zasad użycia narzędzi diagnostycznych i serwisowych,

   f) integralność systemu, w tym ochrona przed podejrzanym kodem, zasady wprowadzania poprawek lub uaktualnień oprogramowania, techniki i narzędzia identyfikacji intruzów,

   g) ochrona nośników, w tym oznaczanie, dostęp, transport, deklasyfikacja i niszczenie,

   h) reagowanie na incydenty, w tym tryb postępowania osób odpowiedzialnych za bezpieczeństwo teleinformatyczne oraz osób uprawnionych do pracy w systemie teleinformatycznym w sytuacji wystąpienia incydentu bezpieczeństwa teleinformatycznego,

   i) zasady szkolenia z zakresu bezpieczeństwa teleinformatycznego osób odpowiedzialnych za bezpieczeństwo teleinformatyczne oraz osób uprawnionych do pracy w systemie teleinformatycznym;

3) w zakresie zabezpieczeń technicznych:

   a) identyfikacja i uwierzytelnienie użytkowników i urządzeń, w tym zarządzanie identyfikatorami użytkowników oraz zarządzanie danymi uwierzytelnienia,

   b) kontrola dostępu, w tym zarządzanie kontami, kontrola dostępu do aplikacji, reakcja na nieudane próby logowania, separacja obowiązków, minimalne przywileje, blokowanie i zamykanie sesji, przegląd aktywności użytkowników,

   c) audyt, w tym zdarzenia podlegające audytowi, zawartość rekordu audytu, reakcja na błędy procesu audytu, monitorowanie i analizowanie, ochrona danych audytu,

   d) ochrona systemu i łączności, w tym zastosowane urządzenia zabezpieczeń brzegowych, poufność transmisji, mechanizmy ochrony kryptograficznej, dystrybucja kluczy kryptograficznych, uwierzytelnienie sesji, sposoby przeciwdziałania ujawnieniu informacji poprzez powtórne użycie obiektów,

oraz definiuje odpowiedzialność za wdrożenie zabezpieczeń.

§ 25. 1. Procedury bezpiecznej eksploatacji zawierają szczegółowy wykaz czynności wraz z dokładnym opisem sposobu ich wykonania, które powinny być realizowane przez osoby odpowiedzialne za bezpieczeństwo teleinformatyczne oraz osoby uprawnione do pracy w systemie teleinformatycznym.

2. Szczegółowy wykaz czynności powinien być ujęty w tematycznie wyodrębnione procedury bezpieczeństwa, obejmujące zagadnienia wymienione w § 24.

Rozdział 5

Przepisy końcowe

§ 26. Traci moc rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2005 r., nr 171, poz. 1433).

§ 27. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezes Rady Ministrów

UZASADNIENIE

do Projektu rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.

Projekt rozporządzenia realizuje dyspozycję art. 50 ust. 1 ustawy z dnia … o ochronie informacji niejawnych oraz o zmianie niektórych ustaw, zgodnie z którą Prezes Rady Ministrów został upoważniony do określenia podstawowych wymagań bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne służące do przetwarzania informacji niejawnych oraz sposobu opracowywania dokumentacji bezpieczeństwa systemów teleinformatycznych.

Powyższa problematyka jest aktualnie uregulowana w *Rozporządzeniu Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2005 r., nr 171, poz. 1433)*.

Proponowana zmiana rozporządzenia ma na celu określenie, ujednolicenie oraz doprecyzowanie podstawowych wymagań bezpieczeństwa dla systemów teleinformatycznych służących do przetwarzania informacji niejawnych, przez co ułatwi oraz usprawni organizację systemu teleinformatycznego i tworzenie dokumentacji bezpieczeństwa teleinformatycznego. Obejmuje ona stosowanie spójnego zbioru zabezpieczeń w celu zapewnienia ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych przed utratą poufności, integralności i dostępności, powstałych w wyniku przypadku lub celowych działań.

W powyższym projekcie uszczegółowiono podstawowe wymagania bezpieczeństwa teleinformatycznego oraz zapisy dotyczące dokumentacji bezpieczeństwa teleinformatycznego.

Wymagania bezpieczństwa oparto o dokumenty UE i NATO, jak również wzięto pod uwagę wytyczne amerykańskiego National Institute of Standards and Technology (NIST) odnoszące się do bezpieczeństwa systemów teleinformatycznych, w szczególności dokument „Special Publication 800-53”.

Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym musi być uwzględnione w całym cyklu życia systemu teleinformatycznego, którego szczegółowy opis zawiera § 4 projektu.

Istotnym *novum* tego projektu rozporządzenia jest rozdział 3, zawierający przepisy dotyczące zarządzania ryzykiem w systemie teleinformatycznym, określają-

ce jego poszczególne procesy oraz sposób ich realizacji. Zarządzanie ryzykiem oparto o normę ISO/IEC 27005:2008(E).

Szacownie ryzyka jest jednym z trzech najważniejszych, obok uwarunkowań wynikających z obowiązujących przepisów prawnych i zaleceń w zakresie bezpieczeństwa teleinformatycznego, środków ochrony systemu teleinformatycznego.

Wprowadzenie takiego uregulowania ma na celu zapewnienie doboru zabezpieczeń służących ochronie sytemu teleinformatycznego w sposób spójny i racjonalny.

Za zapewnienie ciągłości procesu zarządzania ryzykiem dla systemu teleinformatycznego, odpowiada kierownik jednostki organizacyjnej organizującej ten system, a w przypadku, gdy system teleinformatyczny jest użytkowany przez kilka niezależnych jednostek organizacyjnych – każdy kierownik jednostki organizacyjnej użytkującej system teleinformatyczny, współdziałając z innymi kierownikami jednostek organizacyjnych w celu zapewnienia ciągłości procesu zarządzania ryzykiem dla tego systemu.

W stosunku do poprzedniego stanu prawnego rozdział 4, regulujący zagadnienia związane z dokumentacją bezpieczeństwa teleinformatycznego został uszczegółowiony w części odnoszącej się do opisu wybranych dla systemu zabezpieczeń. Dla celów dokumentacji wymagania dotyczące zabezpieczeń są uporządkowane wg obszarów, których dotyczą, w hierarchię klas (zarządzanie, eksploatację oraz zabezpieczenia techniczne) i rodzin (zarządzanie ryzykiem, planowanie zmian, nabywanie elementów systemu i usług, ocena bezpieczeństwa systemu, bezpieczeństwa osobowego, bezpieczeństwa fizycznego, ciągłość działania, zarządzanie konfiguracją, utrzymanie systemu, integralność systemu, ochrona nośników, reagowanie na incydenty, szkolenia, identyfikacja i uwierzytelnienie, kontrola dostępu, audyt, ochrona systemu i łączności). Struktura ta ma służyć podkreśleniu faktu, że zapewnienie bezpieczeństwa teleinformatycznego wymaga doboru szerokiego spektrum zabezpieczeń. Głównym celem proponowanych zmian jest położenie nacisku na ochronę sytemu teleinformatycznego jako całości.

Projekt rozporządzenia stanowi rozwinięcie zawartej w nowej ustawie o ochronie informacji niejawnych zasady, zgodnie z którą szacowanie ryzyka stało się podstawą określenia niezbędnych elementów bezpieczeństwa teleinformatycznego. To właśnie na podstawie szacowania ryzyka będzie można określić, które elementy są niezbędne, a które będzie można zastąpić innym rozwiązaniem zakładając,

że ryzyko szczątkowe z nimi związane będzie mogło być zaakceptowane. Powyższe wpływa również korzystnie na kwestie związane z kosztami organizacji bezpieczeństwa teleinformatycznego dzięki zastosowaniu elastycznego i indywidualnego podejścia do każdego organizowanego systemu.

Ocena Skutków Regulacji (OSR)

1. **Podmioty, na które oddziałuje projekt rozporządzenia.**

Regulacja oddziałuje na podmioty działające w sferze ochrony informacji niejawnych, organizujące systemy teleinformatyczne, w których przetwarzane będą informacje niejawne.

2. **Konsultacje społeczne.**

3. **Wpływ regulacji na sektor finansów publicznych, w tym budżet państwa i budżet jednostek samorządu terytorialnego.**

Przewiduje się, że w świetle zaproponowanych przepisów wejście w życie projektowanego rozporządzenia nie będzie miało znaczącego wpływu na budżet państwa.

4. **Wpływ regulacji na rynek pracy.**

Rozporządzenie nie będzie miało wpływu na rynek pracy.

5. **Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw.**

Projektowany akt prawny nie będzie miał wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw.

6. **Wpływ regulacji na sytuację i rozwój regionalny.**

Rozporządzenie nie będzie miało wpływu na sytuację i rozwój regionalny.

7. **Zgodność regulacji z prawem Unii Europejskiej.**

Projekt porozumienia jest zgodny z dyrektywami Unii Europejskiej i NATO.

37-02-aa

Projekt

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW

z dnia ……

w sprawie wysokości opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego

Na podstawie art. 53 ust. 4 ustawy z dnia … o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. z … r., nr …, poz. …), zwanej dalej ustawą, zarządza się, co następuje:

§ 1. Rozporządzenie określa wysokość opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego, o których mowa w 48 ust. 3-6 oraz art. 50 ust. 1-4.

§ 2. 1. Opłaty za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego następujących czynności z zakresu bezpieczeństwa teleinformatycznego:

1) za badania i ocenę w ramach procesu certyfikacji urządzenia lub narzędzia kryptograficznego przeznaczonego do ochrony informacji niejawnych – równowartość 0,1 kwoty bazowej za godzinę pracy osoby wykonującej badania lub ocenę, ale w sumie nie więcej niż równowartość:
   a) 100-krotności kwoty bazowej, gdy urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli ściśle tajne,
   b) 75-krotności kwoty bazowej, gdy urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli tajne,
   c) 50-krotności kwoty bazowej, gdy urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli poufne,
   d) 25-krotności kwoty bazowej, gdy urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli zastrzeżone;
2) za badania i ocenę w ramach procesu certyfikacji środka ochrony elektromagnetycznej przeznaczonego do ochrony informacji niejawnych o klauzuli poufne lub wyższej – równowartość 0,1 kwoty bazowej za godzinę pracy osoby wykonującej badania lub ocenę, ale w sumie nie więcej niż równowartość 3-krotności kwoty bazowej;
3) za badania i ocenę w ramach procesu certyfikacji urządzenia lub narzędzia przeznaczonego do ochrony informacji niejawnych realizującego zabezpieczenia teleinformatyczne – równowartość 0,1 kwoty bazowej za godzinę pracy osoby wykonującej badania lub ocenę, ale w sumie nie więcej niż równowartość:
   a) 100-krotności kwoty bazowej, gdy urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli ściśle tajne,

b) 75-krotności kwoty bazowej, gdy urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli tajne,

c) 50-krotności kwoty bazowej, gdy urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli poufne,

d) 25-krotności kwoty bazowej, gdy urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli zastrzeżone;

4) za ocenę bezpieczeństwa systemu i audyt bezpieczeństwa teleinformatycznego w ramach akredytacji bezpieczeństwa teleinformatycznego systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych – równowartość 0,1 kwoty bazowej za godzinę pracy osoby dokonującej oceny lub audytu;

5) za wydanie certyfikatu ochrony kryptograficznej, certyfikatu ochrony elektromagnetycznej, certyfikatu bezpieczeństwa teleinformatycznego lub świadectwa akredytacji bezpieczeństwa teleinformatycznego – równowartość 0,25 kwoty bazowej;

6) za akredytację laboratorium badawczego, uprawniającą do wykonywania badań w ramach procesów certyfikacji prowadzonych przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego – równowartość 0,1 kwoty bazowej za godzinę pracy osoby dokonującej akredytacji;

2. Kwotę bazową stanowi kwota przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłoszonego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 7 ust. 1 ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich (Dz. U. z 1998 r., nr 108, poz. 685, z późn. zm.).

§ 3. Traci moc rozporządzenie Prezesa Rady Ministrów z dnia 30 września 2005 r. w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności z zakresu bezpieczeństwa teleinformatycznego (Dz. U. z 2005 r., nr 200, poz. 1652).

§ 4. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezes Rady Ministrów:

UZASADNIENIE

Projekt rozporządzenia realizuje dyspozycję art. 53 ust. 4 ustawy z dnia … o ochronie informacji niejawnych oraz o zmianie niektórych ustaw, zgodnie z którą Prezes Rady Ministrów został upoważniony do określenia wysokości opłat za przeprowadzenie czynności, o których mowa w art. 45 ust. 6-9 oraz art. 46 ust. 1-4, a także akredytacji, o której mowa w art. 46 ust. 7 w/w ustawy.

Powyższa problematyka jest aktualnie uregulowana w *Rozporządzeniu Prezesa Rady Ministrów z dnia 30 września 2005 r. w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności z zakresu bezpieczeństwa teleinformatycznego (Dz. U. z 2005 r., nr 200, poz. 1652).*

Proponowana zmiana rozporządzenia ma na celu ujednolicenie oraz uproszczenie zasad naliczania opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego, a także za akredytację laboratoriów badawczych.

Projekt nowego rozporządzenia wprowadza zmiany polegające na:

- Określeniu jednej wartości kwoty bazowej, właściwej dla wszystkich czynności wykonywanych w ramach procesu certyfikacji, określonej na 0,1 kwoty przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłoszonego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 7 ust. 1 ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich (Dz. U. z 1998 r., nr 108, poz. 685, z późn. zm.).

Jedynym odstępstwem od powyższej zasady jest § 2 ust. 1 pkt 5, gdzie wartość ta wynosi 0,25 powyższej kwoty.

- Określeniu równowartości kwoty bazowej za godzinę pracy osoby wykonującej badania lub ocenę, w przeciwieństwie do poprzednich zapisów stanowiących, że jest to równowartość kwoty bazowej za godzinę pracy zespołu badawczego, co rodziło duże trudności interpretacyjne.

- Ustaleniu górnej granicy opłaty za:

a) badania i ocenę w ramach procesu certyfikacji urządzenia lub narzędzia kryptograficznego przeznaczonego do ochrony informacji niejawnych;

b) badania i ocenę w ramach procesu certyfikacji środka ochrony elektromagnetycznej przeznaczonego do ochrony informacji niejawnych o klauzuli „poufne” lub wyższej;

c) badania i ocenę w ramach procesu certyfikacji urządzenia lub narzędzia przeznaczonego do ochrony informacji niejawnych realizującego zabezpieczenia teleinformatyczne.

Określenie jednolitej wartości kwoty bazowej oraz wskazanie górnej granicy opłat za czynności z zakresu bezpieczeństwa teleinformatycznego stwarza bardziej czytelne i jednoznaczne zasady uiszczania opłat za przedmiotowe czynności, nie zakłada natomiast zwiększenia kosztów z nimi związanych. Jest ponadto rozwiązaniem korzystniejszym dla podmiotów z nich korzystających, gdyż niezależnie od czasu trwania procedury wynagrodzenie za nią należne nie przekroczy określonej w rozporządzeniu wartości.

Ocena Skutków Regulacji (OSR)

1. **Podmioty, na które oddziałuje projekt rozporządzenia.**

Regulacja oddziałuje na podmioty działające w sferze ochrony informacji niejawnych, ubiegające się o uzyskanie świadectwa akredytacji bezpieczeństwa teleinformatycznego, certyfikatu ochrony elektromagnetycznej, certyfikatu ochrony kryptograficznej, certyfikatu bezpieczeństwa teleinformatycznego oraz podmioty, które chciałyby ubiegać się o certyfikat akredytacji laboratorium i brać udział w procesach certyfikacji uregulowanych w art. 46 ust. 1-3 ustawy z dnia … o ochronie informacji niejawnych oraz o zmianie niektórych ustaw.

2. **Konsultacje społeczne.**

3. **Wpływ regulacji na sektor finansów publicznych, w tym budżet państwa i budżet jednostek samorządu terytorialnego.**

Przewiduje się, że w świetle zaproponowanych przepisów wejście w życie projektowanego rozporządzenia nie będzie miało znaczącego wpływu na budżet państwa,

nie wiąże się również w żaden sposób z budżetem jednostek samorządu terytorialnego.

4. **Wpływ regulacji na rynek pracy.**

Rozporządzenie nie będzie miało znaczącego wpływu na rynek pracy.

5. **Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw.**

Projektowany akt prawny nie będzie miał wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw.

6. **Wpływ regulacji na sytuację i rozwój regionalny.**

Rozporządzenie nie będzie miało wpływu na sytuację i rozwój regionalny.

7. **Zgodność regulacji z prawem Unii Europejskiej.**

Tematyka projektu rozporządzenia nie jest regulowana w prawie Unii Europejskiej.

35-02-aa

PROJEKT

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia .....

w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego na przeprowadzenie sprawdzeń przedsiębiorcy oraz poszerzonych postępowań sprawdzających

Na podstawie art. 61 ust. 2 ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. Nr ……, poz……..) zarządza się, co następuje:

§ 1

Rozporządzenie określa:

1) wysokość zwrotu zryczałtowanych kosztów ponoszonych na przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego i Służbę Kontrwywiadu Wojskowego sprawdzeń przedsiębiorcy i poszerzonych postępowań sprawdzających,

2) tryb zwrotu zryczałtowanych kosztów ponoszonych na przeprowadzenie czynności, o których mowa w pkt 1.

§ 2

Za przeprowadzenie czynności, o których mowa w § 1, Agencji Bezpieczeństwa Wewnętrznego i Służbie Kontrwywiadu Wojskowego przysługuje zwrot zryczałtowanych kosztów w wysokości krotności kwoty przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, zwanego dalej „przeciętnym wynagrodzeniem", ogłoszonego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 7 ust. 1 ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich (Dz. U. Nr 108, poz. 685, z późn. zm.):

1) ponoszonych na przeprowadzenie sprawdzeń przedsiębiorcy:

   a) w wysokości 7-krotności kwoty przeciętnego wynagrodzenia w przypadku ubiegania się przez przedsiębiorcę o świadectwo bezpieczeństwa przemysłowego pierwszego lub drugiego stopnia,

   b) w wysokości 6-krotności kwoty przeciętnego wynagrodzenia w przypadku ubiegania się przez przedsiębiorcę o świadectwo bezpieczeństwa przemysłowego trzeciego stopnia,

2) ponoszonych na przeprowadzenie poszerzonych postępowań sprawdzających w toku postępowania bezpieczeństwa przemysłowego w wysokości 0,65-krotności kwoty przeciętnego wynagrodzenia od każdej sprawdzanej osoby.

§ 3

1) Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego, po złożeniu wniosku o przeprowadzenie postępowania bezpieczeństwa przemysłowego lub poszerzonego postępowania sprawdzającego, wystawia przedsiębiorcy rachunek.

2) Przedsiębiorca, w terminie 21 dni od daty doręczenia rachunku, wnosi, na wskazany przez Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego państwa rachunek bankowy, kwotę wymienioną w rachunku, o którym mowa w ust. 1.

§ 4

Traci moc rozporządzenie Prezesa Rady Ministrów z dnia 29 sierpnia 2005 r. w sprawie wysokości i trybu pobierania, przez służbę ochrony państwa, opłat za przeprowadzenie postępowania bezpieczeństwa przemysłowego, sprawdzeń oraz postępowań sprawdzających (Dz. U. Nr 174, poz. 1447).

§ 5

Rozporządzenie wchodzi w życie .....

Prezes Rady Ministrów

UZASADNIENIE

Nowe rozporządzenie zastąpi obowiązujące dotychczas rozporządzenie Prezesa Rady Ministrów z dnia 29 sierpnia 2005 r. w sprawie wysokości i trybu pobierania, przez służbę ochrony państwa, opłat za przeprowadzenie postępowania bezpieczeństwa przemysłowego, sprawdzeń oraz postępowań sprawdzających (Dz. U. Nr 174, poz. 1447, z późn. zm.).

Zasadnicza zmiana dotyczy wprowadzenia pojęcia zwrotu zryczałtowanych kosztów w miejsce dotychczasowych opłat za czynności przeprowadzane w ramach postępowań bezpieczeństwa przemysłowego i postępowań sprawdzających.

Utrzymuje się zróżnicowane stawki zwrotu zryczałtowanych kosztów ponoszonych przy sprawdzeniach w celu wydania świadectwa bezpieczeństwa przemysłowego pierwszego i drugiego stopnia (wyższa stawka – większy zakres sprawdzeń) lub trzeciego stopnia (niższa stawka – mniejszy zakres sprawdzeń).

Pozostawiono tylko jedną, uśrednioną stawkę zwrotu zryczałtowanych kosztów ponoszonych na czynności przeprowadzane w ramach poszerzonego postępowania sprawdzającego. Zakres tych czynności niezależnie od klauzuli tajności może być, zgodnie z nowymi regulacjami ustawy, taki sam.

Stawki zwrotu zryczałtowanych kosztów są pochodną kosztów (m.in. wynagrodzeń, kosztów materiałów i usług) ponoszonych przez ABW i SKW w związku z czynnościami podczas prowadzenia postępowań bezpieczeństwa przemysłowego i poszerzonych postępowań sprawdzających.

Bez zmian pozostanie wysokość kwoty bazowej, to jest przeciętne wynagrodzenie ogłoszone przez Prezesa Głównego Urzędu Statystycznego na podstawie ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich.

Pozostałe zmiany dotyczą wprowadzenia w miejsce określenia „służba ochrony państwa" nazw służb, to jest ABW i SKW.

WSTĘPNA OPINIA O ZGODNOŚCI PROJEKTU Z PRAWEM UNII EUROPEJSKIEJ

Analiza zapisów zawartych w projekcie rozporządzenia w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych przez Agencję Bezpieczeństwa Wewnętrznego i Służbę Kontrwywiadu Wojskowego na przeprowadzenie sprawdzeń przedsiębiorcy oraz poszerzonych postępowań sprawdzających wskazuje, że uregulowania te są zgodne z prawem Unii Europejskiej.

OCENA SKUTKÓW REGULACJI (OSR)

1. Podmioty, na które oddziałuje projektowana regulacja.

Projektowane rozporządzenie będzie miało wpływ na przedsiębiorców ubiegających się o świadectwo bezpieczeństwa przemysłowego.

2. Zakres przeprowadzonych konsultacji

.....
.....

3. Wpływ regulacji na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego.

Wejście w życie rozporządzenia nie spowoduje wydatków budżetu państwa i budżetów jednostek samorządu terytorialnego.

4. Wpływ na rynek pracy.

Wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy.

5. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczości, w tym na funkcjonowanie przedsiębiorstw oraz sytuacje i rozwój regionalny.

Wejście w życie rozporządzenia nie będzie miało negatywnego wpływu na konkurencyjność gospodarki i przedsiębiorczości oraz rozwój regionalny.

PROJEKT

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia .....

w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego

Na podstawie art. 68 ustawy z dnia ……. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. nr ……, poz……..) zarządza się, co następuje:

§ 1

Ustala się wzór:

1) kwestionariusza bezpieczeństwa przemysłowego, określony w załączniku nr 1 do rozporządzenia,
2) świadectwa bezpieczeństwa przemysłowego, określony w załączniku nr 2 do rozporządzenia,
3) decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, określony w załączniku nr 3 do rozporządzenia;
4) decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego, określony w załączniku nr 4 do rozporządzenia.

§ 2

Świadectwo bezpieczeństwa przemysłowego jest sporządzane na papierze offsetowym w kolorze niebieskim formatu A4 z tłem rastrowanym i z tekstem o treści stanowiącej pełną nazwę Agencji Bezpieczeństwa Wewnętrznego lub Służby Kontrwywiadu Wojskowego.

§ 3

Traci moc rozporządzenie Rady Ministrów z dnia 8 września 2005 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego (Dz. U. Nr 181, poz. 1504, z późn. zm.[1])

§ 4

Rozporządzenie wchodzi w życie…….

Prezes Rady Ministrów

[1] Zmiana tekstu została ogłoszona w Dz. U. z 2006 r. Nr 92, poz. 640

UZASADNIENIE

Nowe rozporządzenie zastąpi obowiązujące dotychczas rozporządzenie Rady Ministrów z dnia 8 września 2005 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego (Dz. U. Nr 181, poz. 1504, z późn. zm.).

Dotychczasowy wzór kwestionariusza bezpieczeństwa przemysłowego zawiera nieprecyzyjnie sformułowane niektóre punkty (pytania), co w toku prowadzonych postępowań bezpieczeństwa przemysłowego zgłaszali przedstawiciele przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych. Odpowiedzi na pytania zawarte w kwestionariuszu stanowią podstawę do sprawdzeń określonych w ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. Niejednokrotnie przedsiębiorcy byli wzywani przez służby ochrony państwa prowadzące postępowania do uściślenia swoich odpowiedzi. Ponowne odpowiedzi niekiedy różniły się w sposób zasadniczy od udzielonych pierwotnie. Zaznaczyć należy, że podanie nieprawdziwych danych w kwestionariuszu może stanowić podstawę decyzji o odmowie wydania bądź o cofnięciu świadectwa bezpieczeństwa przemysłowego.

Poprawiony wzór kwestionariusza ograniczy uznaniowość w interpretacji odpowiedzi udzielanych przez zainteresowane podmioty oraz uprości procedury bezpieczeństwa przemysłowego.

Dotychczas świadectwa bezpieczeństwa przemysłowego wydawane były dla każdego stopnia dostępu do informacji niejawnych oddzielnie. W celu zminimalizowania konieczności wydawania kilku odrębnych dokumentów dotyczących tej samej kwestii, wprowadzono jeden wzór świadectwa bezpieczeństwa przemysłowego dla każdego stopnia zdolności do ochrony informacji niejawnych krajowych i organizacji międzynarodowych. Wzór świadectwa uwzględnia różne terminy ważności dla poszczególnych poziomów dostępu. Wprowadzenie jednego wzoru ograniczy także koszty wykonania odpowiednich druków.

Rozporządzenie Rady Ministrów z dnia 8 września 2005 r. nie zawiera także wzorów: świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego Unii Zachodnioeuropejskiej. O takie świadectwo mogą ubiegać się przedsiębiorcy na podstawie przepisów Unii Zachodnioeuropejskiej (dokument RS 100, wydanie styczeń 1996).

Analogicznie wprowadzono jeden rodzaj decyzji o odmowie i cofnięciu świadectwa bezpieczeństwa przemysłowego dla każdego stopnia zdolności do ochrony informacji niejawnych.

Pozostałe zmiany wszystkich wzorów dotyczą wprowadzenia w miejsce określenia „służba ochrony państwa" nazw służb, to jest ABW i SKW oraz wprowadzenia nowych pojęć w ustawie o ochronie informacji niejawnych, jak np. kierownik przedsiębiorcy.

WSTĘPNA OPINIA O ZGODNOŚCI PROJEKTU Z PRAWEM UNII EUROPEJSKIEJ

Analiza zapisów zawartych w projekcie rozporządzenia w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego wskazuje, że uregulowania te są zgodne z prawem Unii Europejskiej.

OCENA SKUTKÓW REGULACJI (OSR)

1. Podmioty, na które oddziałuje projektowana regulacja.

Projektowane rozporządzenie będzie miało wpływ na przedsiębiorców ubiegających się o świadectwo bezpieczeństwa przemysłowego.

2. Zakres przeprowadzonych konsultacji

.....
.....

3. Wpływ regulacji na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego.

Wejście w życie rozporządzenia nie spowoduje istotnych wydatków budżetu państwa i budżetów jednostek samorządu terytorialnego.

4. Wpływ na rynek pracy.

Wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy.

5. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczości, w tym na funkcjonowanie przedsiębiorstw oraz sytuacje i rozwój regionalny.

Wejście w życie rozporządzenia nie będzie miało negatywnego wpływu na konkurencyjność gospodarki i przedsiębiorczości oraz rozwój regionalny.

Załącznik nr 1

WZÓR

.....
(pieczęć przedsiębiorcy ubiegającego się
o świadectwo bezpieczeństwa przemysłowego)

KWESTIONARIUSZ BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Dane zawarte w niniejszym kwestionariuszu bezpieczeństwa przemysłowego będą wykorzystane zgodnie z ustawą …….. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. z ……. r. Nr ……, poz. ……), zwaną dalej „ustawą", w toku postępowania bezpieczeństwa przemysłowego mającego na celu ocenę zdolności przedsiębiorcy do zapewnienia ochrony informacji niejawnych przed nieuprawnionym ujawnieniem.

1. Dane identyfikujące przedsiębiorcę:

a. Pełna nazwa .....

.....

b. Nazwa skrócona .....

c. Nazwa używana do celów marketingowych .....

d. Adres siedziby .....

(kod pocztowy, miasto, ulica, numer domu i lokalu)

.....

(województwo, powiat, gmina)

.....

(nr telefonu, faksu, adres poczty elektronicznej)

e. Statystyczny numer identyfikacyjny (REGON) .....

f. Numer identyfikacji podatkowej (NIP) .....

g. Forma prawna .....

h. Rejestr działalności gospodarczej[1)].....

.....

(nazwa i siedziba rejestru)

.....

(nr rejestru, data rejestracji)

i. Data rozpoczęcia działalności gospodarczej .....

2. Dane o strukturze kapitału i powiązaniach kapitałowych:

a. Wartość kapitału zakładowego .....

b. Liczba akcji/udziałów .....

c. Wartość nominalna akcji/udziału .....

d. Struktura kapitału:

Imię, nazwisko i adres zamieszkania właściciela lub pełna nazwa i adres posiadacza powyżej 10% akcji/udziałów (a/u)[2)]	Liczba a/u	% a/u	Stosunek i rodzaj uprzywilejowania a/u

e. Udział powyżej 10% w kapitale innych podmiotów:

Nazwa podmiotu, siedziba i numer rejestru działalności gospodarczej i/lub numer NIP i REGON	Adres siedziby	% a/u	Wartość a/u

3. Dane o źródłach pochodzenia środków finansowych i sytuacji finansowej:

a. Wykaz 10 największych umów wykonywanych w ciągu ostatnich 3 lat na rzecz kontrahentów krajowych:

Przedmiot umowy	Nazwa kontrahenta i adres jego siedziby	Wartość umowy	Okres realizacji

b. Wykaz 10 największych umów wykonywanych w ciągu ostatnich 3 lat na rzecz kontrahentów zagranicznych:

Przedmiot umowy	Nazwa kontrahenta i adres jego siedziby	Wartość umowy	Okres realizacji

c. Zysk/strata netto za ostatnie trzy lata obrachunkowe[3)]:

- .....
- .....
- .....

d. Wykaz wierzycieli, wobec których zobowiązania podmiotu przekraczają 20% wartości kapitału akcyjnego/zakładowego:

Nazwa wierzyciela	Adres siedziby wierzyciela	Kwota zobowiązań

e. Czy przedsiębiorca ma zaległości podatkowe[1)]:

☐ TAK ☐ NIE

f. Czy przedsiębiorca ma zaległości w wywiązywaniu się z podatków i opłat lokalnych[1)]:

☐ TAK ☐ NIE

g. Czy przedsiębiorca ma zaległości w odprowadzaniu składek na ubezpieczenia społeczne, ubezpieczenie zdrowotne oraz Fundusz Pracy i Fundusz Gwarantowanych Świadczeń Pracowniczych.[1)]:

☐ TAK ☐ NIE

h. Czy przedsiębiorca jest w trakcie postępowania ugodowego z wierzycielami:

☐ TAK ☐ NIE

i. Czy w odniesieniu do przedsiębiorcy prowadzone jest postępowanie w sprawie o przestępstwo skarbowe lub wykroczenie skarbowe:

☐ TAK ☐ NIE

j. Czy wobec przedsiębiorcy prowadzone jest sądowo-komornicze lub administracyjne postępowanie egzekucyjne:

☐ TAK ☐ NIE

k. Czy wobec przedsiębiorcy toczy sie postępowanie z wniosku o ogłoszenie upadłości:

☐ TAK ☐ NIE

l. Wykaz numerów rachunków bankowych przedsiębiorcy (na pierwszym miejscu numer rachunku podstawowego):

Nr rachunku bankowego	Nazwa i adres banku

4. Dane o strukturze organizacyjnej:

a. Liczba oddziałów .....

b. Podstawowe informacje o oddziałach:

Nazwa oddziału	NIP	REGON	Adres oddziału

5. Dane osób wchodzących w skład organów kontrolnych, zarządzających, przedsiębiorcy i osób działających z ich upoważnienia (prokurenci):

Imię i nazwisko	PESEL[4)]	Adres zamieszkania	Funkcja

6. Dane o kompleksowych systemach ochrony informacji niejawnych:

a. Adres lokalizacji systemu (kod pocztowy, miasto, ulica, numer domu i lokalu)

b. Czy przedsiębiorca zorganizował strefy ochronne:

☐ TAK ☐ NIE

c. Czy przedsiębiorca wprowadził system kontroli dostępu uprawniający do wejścia, przebywania i wyjścia ze stref ochronnych:

☐ TAK ☐ NIE

d. Czy przedsiębiorca zorganizował kancelarię tajną:

☐ TAK ☐ NIE

e. Czy system ochrony informacji niejawnych jest obsługiwany lub wspomagany przez:

- wewnętrzny pion ochrony:

☐ TAK ☐ NIE

- podmiot lub podmioty prowadzące działalność w zakresie ochrony osób i mienia (jeżeli tak, proszę podać pełną nazwę, adres siedziby, numer telefonu, numer koncesji/zezwolenia, datę wydania koncesji/zezwolenia):

☐ TAK ☐ NIE

.....

.....

f. Czy w pomieszczeniach, w których mają być przechowywane informacje niejawne zastosowano wyposażenie i urządzenia służące ochronie informacji niejawnych, którym na podstawie odrębnych przepisów przyznano certyfikaty:

☐ TAK ☐ NIE

g. Czy podjęto działania mające na celu uzyskanie certyfikatu akredytacji bezpieczeństwa teleinformatycznego dla systemu lub sieci teleinformatycznej:

- do poziomu „poufne”

☐ TAK ☐ NIE

- do poziomu „tajne”:

☐ TAK ☐ NIE

- do poziomu „ściśle tajne”:

☐ TAK ☐ NIE

7. Wykazy:

a. osób posiadających poświadczenia bezpieczeństwa uprawniające do dostępu do informacji niejawnych, w tym poświadczenia uprawniające do dostępu do informacji niejawnych organizacji międzynarodowych:

Imię i nazwisko	PESEL[4)]	Klauzula, numer poświadczenia, w tym organizacji międzynarodowych i organ wydający	Data ważności	Nr i data zaświadczenia o przeszkoleniu z zakresu ochrony inf. niejawnych i nazwa organu szkolącego	Stanowisko

b. osób, których ankiety dołączono do wniosku o przeprowadzenie postępowania bezpieczeństwa przemysłowego, w celu przeprowadzenia poszerzonych postępowań sprawdzających:

Imię i nazwisko	PESEL[4)]	Wymagany poziom dostępu do informacji niejawnych (klauzula), w tym informacji niejawnych organizacji międzynarodowych	Stanowisko i/lub funkcja

Imię i nazwisko	PESEL[4)]	Wymagany poziom dostępu do informacji niejawnych (klauzula), w tym informacji niejawnych organizacji międzynarodowych	Stanowisko i/lub funkcja

c. osób, które wykonują lub będą wykonywać funkcje związane z ochroną informacji niejawnych, to jest:

- kierownika przedsiębiorcy w rozumieniu ustawy,
- pełnomocnika ds. ochrony informacji niejawnych
- zastępcy pełnomocnika ds. ochrony informacji niejawnych (w przypadku powołania),
- kierownika kancelarii tajnej,
- inspektora bezpieczeństwa teleinformatycznego,
- pozostałych pracowników pionu ochrony,
- administratora bezpieczeństwa teleinformatycznego:

Imię i nazwisko	PESEL[4)]	Funkcja i numer telefonu służbowego

Imię i nazwisko	PESEL[4)]	Funkcja i numer telefonu służbowego

Niemieszczące się w polach kwestionariusza dane oraz dane o kolejnych, odrębnych systemach wymienionych w pkt. 6 a, w zakresie od pkt. 6 b do pkt. 6 g, należy wpisać na dodatkowych arkuszach, z przywołaniem punktu, i dołączyć do dokumentu.

.....

(podpis i imienna pieczęć osoby upoważnionej do składania oświadczeń woli w imieniu przedsiębiorcy lub kierownika przedsiębiorcy)

Miejscowość .....

Data .....

[1)] Dane powinny być potwierdzone stosownym dokumentem (nie starszym niż 30 dni od daty wypełnienia kwestionariusza).

[2)] W przypadku osób fizycznych: obywateli polskich należy podać numer PESEL, obcokrajowców należy podać: datę i miejsce urodzenia, imię ojca i matki oraz obywatelstwo i narodowość. W przypadku osób prawnych należy podać nazwę, siedzibę i numer rejestru działalności gospodarczej oraz w przypadku podmiotów działających wg prawa polskiego – NIP, REGON.

[3)] Dane powinny być potwierdzone stosownym dokumentem, to jest sprawozdaniem finansowym, a jeżeli podlega ono badaniu przez biegłego rewidenta zgodnie z przepisami o rachunkowości również z opinią o badanym sprawozdaniu, a w przypadku wykonawców niezobowiązanych do sporządzania sprawozdania finansowego innym dokumentem określającym obroty oraz zobowiązania i należności - za okres ostatnich trzech lat obrachunkowych, a jeżeli okres prowadzenia działalności jest krótszy - za ten okres.

[4)] W przypadku obcokrajowców należy podać: datę i miejsce urodzenia, imię ojca i matki oraz obywatelstwo i narodowość.

Załącznik nr 2

(pieczęć nagłówkowa ABW/SKW*)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO PIERWSZEGO/DRUGIEGO/TRZECIEGO* STOPNIA Nr _____

Na podstawie art. 68 pkt 2 ustawy z dnia _____ r. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. z _____ r. Nr ____, poz. ____), po przeprowadzeniu przez:

(nazwa organu, który przeprowadził postępowanie)

postępowania bezpieczeństwa przemysłowego, stwierdza się, że:

(nazwa przedsiębiorcy)

(adres siedziby przedsiębiorcy)

(numer KRS przedsiębiorcy) (numer REGON przedsiębiorcy)

posiada pełną* zdolność do zapewnienia ochrony informacji niejawnych

(nazwa organizacji międzynarodowej)* **oznaczonych klauzulą:**

(nazwa klauzuli tajności) – na okres do: (termin ważności)

(nazwa klauzuli tajności)* – na okres do:* (termin ważności)*

(nazwa klauzuli tajności)* – na okres do:* (termin ważności)*

z wyłączeniem uprawnień do przetwarzania tych informacji we własnych systemach teleinformatycznych/w użytkowanych obiektach*.

(miejscowość i data) m.p. (podpis i imienna pieczęć upoważnionej osoby)

* *niewłaściwe skreślić*

Załącznik nr 3

(pieczęć nagłówkowa ABW/SKW*)

Egzemplarz numer __

DECYZJA Nr _____

O ODMOWIE WYDANIA ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO PIERWSZEGO/DRUGIEGO/TRZECIEGO* STOPNIA

Na podstawie art. 68 pkt 3 ustawy z dnia _____ r. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. z _____ r. Nr ____, poz. ____), po przeprowadzeniu przez:

(nazwa organu, który przeprowadził postępowanie)

postępowania bezpieczeństwa przemysłowego stwierdza się, że:

(nazwa przedsiębiorcy)

(adres siedziby przedsiębiorcy)

(numer KRS przedsiębiorcy) (numer REGON przedsiębiorcy)

nie posiada zdolności do zapewnienia ochrony informacji niejawnych

(nazwa organizacji międzynarodowej)*

UZASADNIENIE

(miejscowość i data) m.p. (podpis i imienna pieczęć upoważnionej osoby)

Pouczenie:

Na decyzję o odmowie wydania świadectwa bezpieczeństwa przemysłowego przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, za pośrednictwem organu, który ją wydał.

** niewłaściwe skreślić*

42-02-aa

Załącznik nr 4

(pieczęć nagłówkowa ABW/SKW*)

Egzemplarz numer __

DECYZJA Nr _____

O COFNIĘCIU ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO PIERWSZEGO/DRUGIEGO/TRZECIEGO* STOPNIA

Na podstawie art. 68 pkt 4 ustawy z dnia _____ r. o ochronie informacji niejawnych oraz o zmianie niektórych ustaw (Dz. U. z _____ r. Nr ____, poz. ____), po przeprowadzeniu przez:

(nazwa organu, który przeprowadził postępowanie)

sprawdzenia z urzędu/kontroli* stwierdza się, że:

(nazwa przedsiębiorcy)

(adres siedziby przedsiębiorcy)

(numer KRS przedsiębiorcy) (numer REGON przedsiębiorcy)

utracił/utraciła/utraciło* zdolność do zapewnienia ochrony informacji niejawnych

(nazwa organizacji międzynarodowej)*

W związku z powyższym

(nazwa uprawnionego organu)

cofa świadectwo bezpieczeństwa przemysłowego nr _____.

UZASADNIENIE

(miejscowość i data) m.p. (podpis i imienna pieczęć upoważnionej osoby)

Pouczenie:

Na decyzję o cofnięciu świadectwa bezpieczeństwa przemysłowego przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego, za pośrednictwem organu, który ją wydał.

** niewłaściwe skreślić*