BOŻENA RADZISZEWSKA
EDYTA KUŚNIERZ

UPRAWNIENIA I OBOWIĄZKI KIEROWNIKA JEDNOSTKI ORAZ PEŁNOMOCNIKA OCHRONY W ŚWIETLE USTAWY O OCHRONIE INFORMACJI NIEJAWNYCH

Ochrona informacji niejawnych jest dziedziną niezwykle trudną i wrażliwą. Aktualnie tematykę tę reguluje ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (DzU Nr 182, poz.1228) obowiązująca od 2 stycznia 2011 r., (zwana dalej uoin). Jednym z powodów wprowadzenia nowej ustawy było dostosowanie polskiego systemu ochrony informacji niejawnych do reguł i praktyk istniejących w Unii Europejskiej i NATO celem umożliwienia sprawnego wykonywania polskiej prezydencji [1].

Wszelkie podmioty, których działania w jakiejkolwiek mierze znajdują się w obszarze przetwarzania informacji niejawnych muszą uwzględnić obowiązek stosowania nowych rozwiązań, jaki narodził się w związku z wejściem w życie tejże ustawy.

Stały użytkownik informacji niejawnych musi mieć świadomość, jakim nowym obowiązkom podlega oraz jakie warunki musi spełniać, by nie uchybić przepisom z zakresu ochrony informacji niejawnych, a tym samym nie narazić się na odpowiedzialność karną, służbową, czy dyscyplinarną, względnie nie utracić swego uprawnienia do dostępu do informacji niejawnych.

Nowa regulacja [2] wpływa na działalność wielu podmiotów. Wystarczy wspomnieć, że zmienia aż 107 innych ustaw. Artykuł 1 pkt 2 ustawy precyzuje zakres podmiotowy jej zastosowania. Należy podkreślić jej szeroki wpływ na działanie organów władzy publicznej i jednostek organizacyjnych podległym lub nadzorowanym przez te organy oraz na

---

[1] Zob. uzasadnienie projektu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, LEX VI . 2791, tekst ze stron internetowych Sejmu (http://www.sejm.gov.pl) i Senatu (http://www.senat.gov.pl).

[2] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (DzU nr 182, poz.1228).

funkcjonowanie jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, a zatem na jednostki organizacyjne Sił Zbrojnych Rzeczypospolitej Polskiej. Wydaje się, że właśnie w tym sektorze, w Siłach Zbrojnych, informacja niejawna ma największe znaczenie i właśnie tutaj omawiana ustawa ma najszersze zastosowanie.

Takie twierdzenie można wyprowadzić już z samej — obecnie zmienionej definicji informacji niejawnych i klasyfikacji tych informacji określonej w art. 5 uoin. Informacja niejawna to bowiem informacja, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej. W zależności od rozmiaru tej szkody informacjom nadaje się stosowne klauzule — „ściśle tajne" (wyjątkowo poważna szkoda), „tajne" (poważna szkoda), „poufne" (szkoda). Natomiast klauzulę „zastrzeżone" nadaje się informacjom niejawnym, którym nie nadano wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć jedynie szkodliwy wpływ na wykonywanie zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych RP. W dużej mierze, jako szkodę dla Rzeczypospolitej Polskiej rozumie się głównie takie zagrożenia, którym Siły Zbrojne RP mają przeciwdziałać.

W nowej ustawie zrezygnowano z podziału na tajemnicę państwową i służbową[3]. Nie ma też załącznika z wykazem rodzajów informacji, stanowiących tajemnicę państwową, na podstawie którego nadawano poszczególne klauzule. Niewątpliwie na wstępnym etapie obowiązywania ustawy wiele trudności sprawi prawidłowe nadawanie klauzul.

Granice pomiędzy klauzulami są niezwykle płynne, bo jak rozróżnić „wyjątkowo poważną szkodę" od „poważnej szkody". Wcześniej, mimo sporych trudności w przyznawaniu najwyższych klauzul, zawarty w załączniku do ustawy wykaz informacji niejawnych wskazywał enumeratywnie jak konkretną informację niejawną należy zakwalifikować. Minusem wykazu była jego obszerność, a przez to mała czytelność poszczególnych kategorii. Obecnie granice pomiędzy klauzulami nie są ostro zakreślone, nie oznacza to jednak dowolności w ich nadawaniu. Według nowych uregulowań, ochronie podlegać mają jedynie takie informacje, których ujawnienie przyniosłoby szkody interesom Państwa. W zależności od poziomu tego zagrożenia względem konkretnego dobra nadaje się wyższą bądź niższą klauzulę. Przykładowo klauzulę „ściśle tajne" w odróżnieniu od „tajne" nadaje się, gdy w grę wchodzi zagrożenie dla niepodległości, suwerenności,

[3] Zob. E. Kuśnierz i B. Radziszewska, *Bez podziału na tajemnicę państwową i służbową*, „Rzeczpospolita" nr 19 (8835) z dnia 25 stycznia 2011 r., s. C10.

zagrożenie dla bezpieczeństwa wewnętrznego czy osłabienia gotowości obronnej Rzeczypospolitej Polskiej, a nie, gdy chronionemu dobru grozi jedynie zakłócenie czy jego pogorszenie. Rozróżnieniem jest całościowe zagrożenie dla danego dobra w stosunku do jego części czy wycinka funkcjonowania. Podobne kryterium zastosowano względem podmiotów osobowych. Klauzule „ściśle tajne" nadaje się informacjom, których nieuprawnione ujawnienie zagrozi lub może zagrozić życiu i zdrowiu lub doprowadzić do identyfikacji osób wykonujących czynności operacyjno-rozpoznawcze. Klauzule „tajne" nadaje się zaś w sytuacji zagrożenia utrudnienia wykonywania czynności operacyjno-rozpoznawczych. Jak widać jednym z najważniejszych kryteriów klasyfikacji jest charakter i rozmiar zagrożonego dobra.

W związku ze zmianą klasyfikacji materiałów niejawnych, jednostki organizacyjne muszą dokonać przeglądu wszystkich materiałów niejawnych pod kątem ewentualnej zmiany lub zniesienia nadanej dotychczas klauzuli tajności. Konieczność taka wynika z uzasadnionych przewidywań, iż znaczna część informacji do tej pory „ściśle tajnych" będzie oznaczana jako „tajne" lub „poufne", natomiast część informacji dotychczas „tajnych" zostanie teraz objęta klauzulami „poufne" i „zastrzeżone" [4].

Ustawa nakłada wiele złożonych obowiązków i powinności jakim muszą sprostać użytkownicy informacji niejawnych.

W świetle ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (DzU Nr 182 poz. 1228) szereg powinności spoczywa głównie na kierowniku jednostki organizacyjnej i pełnomocniku do spraw ochrony informacji niejawnych. Kierownik jednostki organizacyjnej aby prawidłowo wypełniać zadania z zakresu ochrony informacji niejawnej musi pamiętać o:

— własnej odpowiedzialności za ochronę, przetwarzanych w jego jednostce organizacyjnej, informacji niejawnych, a w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony — art. 14 ust. 1 uoin;p

— obowiązku informowania odpowiednio ABW lub SKW o utworzeniu lub likwidacji kancelarii tajnej z określeniem klauzuli tajności przetwarzanych w niej informacji. Ten obowiązek informacyjny pozwala w głównej mierze na bieżące uaktualnianie wykazu kancelarii tajnych. W utworzonej kancelarii tajnej, w której przetwarzane są informacje niejawne o klauzuli „tajne" lub „ściśle tajne" zatrudnia jej kierownika — art. 42 ust. 1 i 6 uoin;

— ustaleniu wzajemnej podległości, zasad finansowania oraz uzyskania zgody SKW w przypadku tworzenia jednej kancelarii tajnej dla dwu lub

[4] Zob. uzasadnienie projektu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, LEX VI. 2791, tekst ze stron internetowych Sejmu (http://www.sejm.gov.pl) i Senatu (http://www.senat.gov.pl).

więcej jednostek organizacyjnych i zawarcia porozumienia z pozostałymi kierownikami jednostek — art. 42 ust. 2 uoin;

— obowiązku wyrażenia pisemnej zgody na zniesienie lub zmianę klauzuli tajności w zakresie informacji niejawnych o klauzuli „ściśle tajne" wobec materiałów, którym klauzula tajności została nadana w jego jednostce organizacyjnej — art. 6 ust. 3 i 5 uoin;

— obowiązku wydawania pisemnych upoważnień dla osób mających uzyskać dostęp do informacji niejawnych o klauzuli „zastrzeżone", a nie posiadających poświadczenia bezpieczeństwa — art. 21 ust. 4 uoin;

— możliwości wydania pisemnej zgody na udostępnienie informacji niejawnych o klauzuli „poufne" osobie zatrudnionej (pełniącej służbę lub wykonującej czynności zlecone) w jego jednostce organizacyjnej, wobec której wszczęto już postępowanie sprawdzające — art. 34 ust. 9 uoin;

— bezpośredniej podległości zatrudnionego w jego jednostce organizacyjnej pełnomocnika do spraw ochrony informacji niejawnych — art. 14 ust. 2 uoin;

— możliwości zatrudnienia zastępcy lub zastępców pełnomocnika ochrony, przy czym osoby te muszą spełniać kryteria wymagane dla pełnomocnika do spraw ochrony informacji niejawnych — art. 14 ust. 4 uoin;

— określeniu szczegółowego zakresu czynności dla zastępcy pełnomocnika ochrony — art. 14 ust. 5 uoin;

— dokonaniu akceptacji planu ochrony informacji niejawnych funkcjonującego w jednostce organizacyjnej, opracowywanego i aktualizowanego przez pełnomocnika ochrony — art. 15 ust. 5 uoin;

— wydawaniu pełnomocnikowi ochrony pisemnego polecenia przeprowadzenia zwykłego postępowania sprawdzającego — art. 23 ust. 1 uoin;

— zatwierdzeniu, opracowanego przez pełnomocnika ochrony sposobu i trybu przetwarzania informacji niejawnych o klauzuli „poufne" — art. 43 ust. 3 uoin,

— zatwierdzeniu opracowanej przez pełnomocnika ochrony dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą w jednostkach organizacyjnych, w których są przetwarzane informacje o klauzuli „poufne" lub wyższej — art. 43 ust. 4 uoin;

— zatwierdzeniu opracowanej przez pełnomocnika ochrony instrukcji o sposobie i trybie przetwarzania informacji niejawnych o klauzuli „zastrzeżone" oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony, w jednostkach organizacyjnych, w których są przetwarzane informacje o klauzuli „zastrzeżone" — art. 43 ust. 5 uoin;

— możliwości powierzenia pełnomocnikowi ochrony oraz pracownikom pionu ochrony wykonywania innych zadań, o ile nie naruszy to

prawidłowego wykonywania zadań z zakresu ochrony informacji niejawnych — art. 15 ust. 4 uoin;

— obowiązku przeglądu wszystkich wytworzonych dokumentów niejawnych raz na pięć lat, celem ustalenia ustawowych przesłanek ochrony — art. 6 ust. 4 uoin;

— obowiązku przeprowadzenia w terminie 36 miesięcy od wejścia w życie ustawy, przeglądu wytworzonych w podległej jednostce organizacyjnej materiałów zawierających informacje niejawne w celu ustalenia czy spełniają ustawowe przesłanki ochrony na podstawie ustawy — art. 181 uoin, obowiązek ten nie obejmuje materiałów spraw zakończonych oraz kartotek ewidencyjnych, w szczególności stanowiących materiał archiwalny przekazany do właściwych archiwów — art. 181 ust. 2 uoin

— obowiązku poddania się co 5 lat szkoleniu, które przeprowadza odpowiednio ABW lub SKW, w przypadku gdy w jednostce organizacyjnej jest zatrudniony pełnomocnik ochrony, służby te, szkolenie przeprowadzają wspólnie z pełnomocnikiem ochrony z zakresu systemu ochrony informacji niejawnych — art. 19 ust. 2 pkt 1 i 2 uoin;

— obowiązku współdziałania ze służbami i instytucjami uprawnionymi do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, polegającego na udostępnianiu funkcjonariuszom, pracownikom albo żołnierzom tych służb i instytucji, po przedstawieniu przez nich pisemnego upoważnienia informacji i dokumentów niezbędnych do realizacji czynności w ramach tych postępowań — art. 13 ust. 1 uoin;

— obowiązku uniemożliwienia osobie sprawdzanej, w trybie kontrolnego postępowania sprawdzającego, dostępu do informacji niejawnej, obowiązek ten rodzi się po otrzymaniu zawiadomienia o wszczęciu takiego postępowania — art. 33 ust.7 uoin

— obowiązku informowania w terminie 7 dni, w przypadku zatrudnienia w jednostce organizacyjnej, na stanowisku, z którym może łączyć się dostęp do informacji niejawnych osobę legitymującą się odpowiednim poświadczeniem bezpieczeństwa, organ, który wydał poświadczenie bezpieczeństwa oraz odpowiednio ABW lub SKW. W przypadku, gdy organem, który wydał poświadczenie bezpieczeństwa jest ABW, to przesyłając informację o zatrudnieniu osoby legitymującej się takim poświadczeniem, jednocześnie będzie spełniony wymóg odrębnego informowania ABW. Co więcej, obowiązek informacyjny ciążący na kierowniku jednostki organizacyjnej zapewnia prawidłowe funkcjonowanie systemu ochrony informacji niejawnych, poprzez weryfikację ważności poświadczeń bezpieczeństwa będących w obrocie prawnym — art. 34 pkt 2 uoin, od wspomnianego obowiązku zwolnieni zostali kierownicy jednostek organizacyjnych następujących podmiotów: Agencji Wywiadu, Centralnego

Biura Antykorupcyjnego, Biura Ochrony Rządu, Policji, Służby Więziennej, Służby Wywiadu Wojskowego, Straży Granicznej, Żandarmerii Wojskowej — art. 34 ust. 3 uoin;

— w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej podlegających akredytacji ABW lub SKW, kierownicy jednostek organizacyjnych w których funkcjonują takie systemy odpowiadają za opracowanie i przekazanie odpowiednio ABW lub SKW dokumentacji bezpieczeństwa systemu teleinformatycznego, zobowiązani są także do akceptacji wyników procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tych systemach oraz odpowiadają za właściwą organizację bezpieczeństwa teleinformatycznego — art. 48 ust. 2, 3 uoin i art. 49 ust. 5, 7 uoin;

— dla systemów przetwarzających informacje niejawne oznaczone klauzulą „zastrzeżone" akredytacji bezpieczeństwa teleinformatycznego raz na 5 lat udziela kierownik jednostki organizacyjnej i w terminie 30 dni przekazuje odpowiednio ABW lub SKW dokumentację bezpieczeństwa teleinformatycznego akredytowanego systemu, w sytuacji zaś, gdy ABW lub SKW zleci przeprowadzenie dodatkowych czynności zwiększających bezpieczeństwo systemu, kierownik jednostki zobowiązany jest w ciągu 30 dni poinformować SKW o realizacji zaleceń — art. 48 ust. 9, 11, 12 uoin;

— wyznaczeniu 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 — art. 52 ust. 1 pkt 1 uoin;

— wyznaczeniu osoby lub zespołu osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwanych dalej „administratorem systemu" — art. 52 ust. 1 pkt 2 uoin;

— możliwości — w uzasadnionych wypadkach przejęcia — uprawnienia do wykonywania zadań pełnomocnika ochrony, z wyłączeniem prowadzenia postępowań sprawdzających przez kierowników jednostek organizacyjnych wymienionych w art. 47 ust. 3, a to: ministrów właściwych do spraw wewnętrznych, administracji publicznej, spraw zagranicznych, finansów publicznych, budżetu i instytucji finansowych, Ministra Obrony Narodowej, Ministra Sprawiedliwości, Prezesa Narodowego Banku Polskiego, Prezesa Najwyższej Izby Kontroli, Pierwszego Prezesa Sądu Najwyższego, Prokuratora Generalnego, Szefów Kancelarii Prezydenta RP, Sejmu, Senatu oraz Prezesa Rady Ministrów, Szefa Agencji Bezpieczeństwa

Wewnętrznego, Szefa Agencji Wywiadu, Szefa Służby Kontrwywiadu Wojskowego, Szefa Służby Wywiadu Wojskowego, Szefa Centralnego Biura Antykorupcyjnego, Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Szefa Biura Ochrony Rządu, Prezesa Instytutu Pamięci Narodowej — art. 44 ust.1 uoin;

— wyznaczeniu, w przypadku zawierania przez jednostkę organizacyjną umowy związanej z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej, osoby odpowiedzialnej za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę obowiązku ochrony wytworzonych w związku z realizacją umowy lub przekazanych mu informacji niejawnych — art. 71 ust. 3 uoin;

— odpowiedzialności za wybór środków bezpieczeństwa fizycznego adekwatnych do zabezpieczenia jednostek i personelu przed zagrożeniami związanymi z nieuprawnionym dostępem do informacji niejawnych lub ich utratą, a to przed: atakami terrorystycznymi, działaniami obcych służb specjalnych, kradzieżą, zniszczeniem materiału, wejściem nieuprawnionych osób do pomieszczeń w których przetwarzane są informacje niejawne czy nieuprawnionym dostępem do informacji niejawnych o wyższej klauzuli aniżeli posiadane uprawnienie. W celu uzyskania ogólnej oceny zagrożenia winni utrzymywać formalny kontakt ze służbami ochrony państwa i ustanowić system alarmowania ze zdefiniowaniem obowiązków w zakresie wdrożenia z góry zaplanowanych środków do zwalczania zagrożenia. Środki zabezpieczenia muszą być przystosowane do uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych, kierownik jednostki organizacyjnej musi rozważyć jakie dodatkowe środki będą mu potrzebne w przypadku stanu nadzwyczajnego (klęski żywiołowej, działania aspołeczne). Niektóre z fizycznych i proceduralnych środków ochrony będą używane cały czas, podczas gdy inne będą przewidziane dla sytuacji wyjątkowych. W końcowym rachunku należy wziąć pod uwagę koszt planowanych środków ochronnych — art. 45 uoin.

Podkreślenia wymaga, iż ABW i SKW są zobowiązane do udzielania kierownikom jednostek organizacyjnych pomocy niezbędnej do realizacji ich zadań, w szczególności wydając zalecenia w zakresie bezpieczeństwa teleinformatycznego (art. 52 ust. 3 uoin). Stanowiska lub funkcje (administrator systemu lub inspektor bezpieczeństwa teleinformatycznego) mogą zajmować lub pełnić osoby spełniające ustawowe wymagania i po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez ABW albo SKW.

Stosownie do treści art. 19 uoin, koszty szkoleń z zakresu ochrony informacji niejawnych, na podstawie umowy, pokrywa jednostka organizacyjna, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje prace zlecone. Jednostki organizacyjne podległe lub nadzorowane

przez Ministra Obrony Narodowej, Policja oraz posłowie i senatorowie nie pokrywają kosztów szkoleń przeprowadzonych przez ABW albo SKW.

Natomiast pełnomocnik ochrony informacji niejawnych, podlegając bezpośrednio kierownikowi jednostki organizacyjnej, odpowiada w danej jednostce za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych (art. 14 ust. 2 uoin). Obecnie osoba, która chce zostać pełnomocnikiem powinna posiadać obywatelstwo polskie, wyższe wykształcenie, poświadczenie bezpieczeństwa i odpowiednie przeszkolenie w zakresie ochrony informacji niejawnych — art. 16 uoin. Ustawodawca nie określił wprost czy wykonywanie zadań pełnomocnika ochrony polega na pełnieniu funkcji, czy też wiąże się z pracą na oddzielnym stanowisku. W świetle przepisów nowej ustawy art. 2 pkt 18 i art. 14 ust. 2 ustawy, zatrudnieniem jest również odpowiednio powołanie, mianowanie lub wyznaczenie. Należy zatem wnioskować, iż w zależności od ustaleń w jednostce organizacyjnej zadania pełnomocnika mogą być wykonywane w ramach funkcji, pełnionego stanowiska lub też dodatkowych zadań. Jako że kancelaria tajna podlega pełnomocnikowi ochrony, kierujący kancelarią kierownik podlega bezpośrednio pełnomocnikowi ochrony to wskazana podległość służbowa uniemożliwia jednoczesne bycie pełnomocnikiem ochrony i kierownikiem kancelarii tajnej — art. 42 ust. 4 uoin.

Obowiązki pełnomocnika ochrony informacji niejawnych określone zostały wprost w art. 15 uoin. Swoje zadania realizuje przy pomocy podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnej, która tworzy tzw. pion ochrony. Pełnomocnik odpowiedzialny jest za prowadzenie szkoleń dla pracowników w zakresie informacji niejawnych co 5 lat i to bez względu na kategorię klauzuli tajności — czy dany pracownik ma dostęp do informacji ściśle tajnych czy jedynie zastrzeżonych. Wyjątkiem jest jedynie szkolenie przeprowadzane względem kierownika tych jednostek organizacyjnych, w których przetwarzane są informacje „ściśle tajne" i „tajne", szkolenie to przeprowadza odpowiednio ABW lub SKW wspólnie z pełnomocnikiem ochrony. Nadto, pełnomocnik opracowuje i cyklicznie aktualizuje plan ochrony informacji niejawnych. Czuwa także nad jego prawidłową realizacją. Winien zapewnić adekwatne dla przetwarzanych w jego jednostce organizacyjnej informacji niejawnych środki bezpieczeństwa fizycznego i stosowną ochronę systemów informatycznych. Nowością jest, że pełnomocnik musi określić w danej jednostce organizacyjnej poziom zagrożeń nieuprawnionego dostępu do informacji niejawnych i dokonać szacowania ryzyka dla bezpieczeństwa informacji niejawnych. Dlatego pełnomocnik jednostki organizacyjnej, w której przetwarzane są informacje niejawne o klauzuli „poufne" lub wyższej, opracowuje dokumentację określającą poziom takich zagrożeń i przedstawia ją do zatwierdzenia kierownikowi jednostki organizacyjnej (zob. art. 43 ust.

4 uoin). Natomiast w sytuacji przetwarzania informacji niejawnych wyłącznie o klauzuli „poufne", pełnomocnik opracowuje jedynie sposób ochrony i tryb przetwarzania informacji o tej klauzuli i przedstawia go do zatwierdzenia kierownikowi jednostki organizacyjnej (zob. art. 43 ust. 3 uoin). W sytuacji zaś przetwarzania w danej jednostce organizacyjnej informacji niejawnych wyłącznie o klauzuli „zastrzeżone", pełnomocnik opracowuje, zatwierdzaną przez kierownika jednostki, instrukcję dotyczącą sposobu i trybu przetwarzania tych informacji oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony (zob. art. 43 ust. 5 uoin).

Pełnomocnik prowadzi także zwykłe i kontrolne postępowanie sprawdzające wobec osób ubiegających się o dostęp do informacji niejawnych o klauzuli „poufne". Nie ma natomiast uprawnień do prowadzenia wymienionych postępowań jedynie wobec swojego pracodawcy, względem którego postępowanie jest zobowiązana prowadzić odpowiednio ABW lub SKW. Do jego obowiązków należy nadto prowadzenie wykazu osób, które w jego jednostce organizacyjnej mają dostęp do informacji niejawnych oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto. Wykaz ten przekazuje do ewidencji odpowiednio ABW lub SKW. W przedmiotowym wykazie powinny być także uwzględniane osoby, wobec których kierownik jednostki organizacyjnej na podstawie art. 34 ust. 5 i ust. 9 ustawy wydał zgodę na udostępnienie informacji niejawnych o klauzuli „poufne". Pełnomocnik ochrony jest zobowiązany do przekazania do ABW lub SKW danych z prowadzonych wykazów, co następuje w formie karty informacyjnej. Zobowiązany jest nadto do okresowej kontroli ochrony informacji niejawnych i przestrzegania przepisów. Taką kontrolę dotyczącą ewidencji, materiałów i obiegu dokumentów winien on przeprowadzać co najmniej raz na trzy lata. W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych to pełnomocnik inicjuje wyjaśnienie okoliczności naruszenia określonych norm i przepisów, i podejmuje wszelkie działania, które ograniczą negatywne skutki takiego naruszenia. Jednocześnie na pełnomocniku ochrony informacji niejawnych ciąży obowiązek niezwłocznego zawiadomienia kierownika jednostki organizacyjnej o zdarzeniu naruszającym przepisy ustawy o ochronie informacji niejawnych. Skala tych naruszeń warunkować może określone konsekwencje dyscyplinarne, porządkowe, a nawet karne. Powyższe skutkować może rozwiązaniem stosunku pracy czy cofnięciem poświadczenia bezpieczeństwa wobec zawinionej utraty uprawnień[5].

Nadmienić należy, że art. 18 uoin desygnuje Ministra Obrony Narodowej do wydania rozporządzenia określającego szczegółowe zadania

[5] Stanisław Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz*, wyd. I, Warszawa 2010, s. 139.

pełnomocników ochrony informacji niejawnych w jednostkach organizacyjnych jemu podległych lub nadzorowanych, mające na celu, przy uwzględnieniu wysokiej rangi informacji niejawnych w tym resorcie, określenie zadań pełnomocników w sposób szczegółowy, umożliwiający realizację obowiązków nałożonych omawianą ustawą. Przepisy wykonawcze wydane w tej materii obowiązują do czasu wejścia w życie przepisów wykonawczych wydanych na podstawie aktualnej ustawy o ochronie informacji niejawnych, nie dłużej jednak niż do 30 grudnia 2011 r. Obecnie obowiązuje jeszcze Rozporządzenie Ministra Obrony Narodowej z dnia 21 czerwca 2007 r. w sprawie szczegółowych zadań pełnomocników ochrony oraz szczególnych wymagań w zakresie ochrony fizycznej jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (DzU z 2008 r. Nr 57, poz. 345).

Przegląd obecnie obowiązującego unormowania w zakresie informacji niejawnych pozwala na stwierdzenie, iż ciężar odpowiedzialności za ochronę informacji niejawnych spoczywa głównie na kierowniku jednostki organizacyjnej, zaś pełnomocnik odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.