PRZEDSIĘBIORSTWO HANDLOWO-USŁUGOWE „ONE”

PORADNIK

SPECJALISTY OCHRONY INFORMACJI NIEJAWNYCH

Kod, nazwa zawodu
242110, Specjalista ochrony informacji niejawnych

mgr inż. Marek **ANZEL**[1]

POZNAŃ

2015

[1] Ekspert z zakresu ochrony informacji niejawnych i systemów teleinformatycznych. Wykładowca i konsultant cyklicznych szkoleń organizowanych przez Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Ogólnopolskie Stowarzyszenie Pełnomocników Ochrony Informacji Niejawnych. Wykładowca przedmiotów z zakresu ochrony informacji niejawnych na studiach podyplomowych na Uniwersytecie Śląskim, WSZiB w Krakowie, WSB w Dąbrowie Górniczej. Autor „Vademecum Kancelarii Tajnej”, „Poradnika dla Personelu Kancelarii Tajnej”, „Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle nowej ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych”, „Przykładowa dokumentacja pełnomocnika ochrony w świetle ustawy o ochronie informacji niejawnych”, współautor „Poradnika Pełnomocnika Ochrony”. Ponadto na stałe współpracuje z dwumiesięcznikiem „Ochrona Mienia i Informacji”, w którym prezentuje praktyczną wiedzę z zakresu bezpieczeństwa informacji, w tym ochrony informacji niejawnych oraz systemów teleinformatycznych.

Opracowanie redakcyjne
Marek Anzel, Paweł Chachurski

Projekt okładki
Paweł Chachurski

Wydanie I

Nakład 1000 egz.

ISBN 978-83-930686-3-0

Poznań 2015

Przedsiębiorstwo Handlowo-Usługowe ONE Magdalena Chachurska
Os. Powstańców Warszawy 5/105, 61-656 Poznań
e-mail: one@one1.pl
http://www.one1.pl

Sprzedaż wysyłkowa tylko poprzez sklep internetowy PHU ONE
http://www.one1.pl

SPIS TREŚCI

CZĘŚĆ IX

ZASADY BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Bezpieczeństwo przemysłowe to działania, które mają zapewnić ochronę informacji niejawnych udostępnianych przedsiębiorcy w związku z umową lub wykonywanym zadaniem na podstawie określonych przepisów prawa.

W rozumieniu ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych bezpieczeństwo przemysłowe obejmuje informacje o różnych klauzulach oraz całokształt spraw związanych z właściwą organizacją i zapewnieniem ochrony tych informacji przez przedsiębiorcę.

Jest to, obok bezpieczeństwa osobowego kolejną istotną sferą narodowego systemu bezpieczeństwa. Znaczącą rolę do spełnienia w tym zakresie mają szefowie, dyrektorzy oraz inne osoby funkcyjne, odpowiedzialne za bezpieczeństwo w swoich firmach, przedsiębiorstwach, placówkach naukowych, badawczo-rozwojowych itp.

Zdolność do ochrony informacji niejawnych przedsiębiorcy przeprowadza się w różnych aspektach: finansowym, techniczno-organizacyjnym a także kadrowym. ABW lub SKW przeprowadzają według procedury zawartej w Kwestionariuszu, postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób mających uzyskać dostęp do informacji niejawnych.

Praktycznie każdy przedsiębiorca zamierzający przetwarzać bądź przetwarzający informacje niejawne zobowiązany jest do spełnienia ustawowych wymagań w zakresie ich ochrony.

Dla usystematyzowania rozważań można dokonać podziału przedsiębiorców na dwie kategorie.

Do pierwszej kategorii zaliczyć należy przedsiębiorców, którzy w ramach prowadzonej działalności gospodarczej zamierzają realizować lub już realizują umowy związane z dostępem do informacji niejawnych. Inaczej mówiąc, jest to grupa firm, przedsiębiorstw, instytucji, która spełniając ustawowe wymagania realizuje umowy przynoszące im wymierne korzyści biznesowe.

Druga kategoria to przedsiębiorcy, którzy ze względu na realizowanie zadań wynikających z przepisów prawa zobligowani zostali do spełnienia ustawowych wymogów w zakresie ochrony informacji niejawnych.

Warto w tym miejscu zatrzymać się nad zdefiniowaniem pojęcia prawnego kierownika przedsiębiorcy. W rozumieniu ustawy jest to kierownik jednostki organizacyjnej prowadzącej działalność gospodarczą.

Zgodnie z art. 2 pkt 14 ustawy kierownikiem przedsiębiorcy jest:

- *członek jednoosobowego zarządu lub innego jednoosobowego organu zarządzającego,*
- *cały organ albo członek lub członkowie wieloosobowego organu zarządzającego wyznaczeni co najmniej uchwałą zarządu do pełnienia funkcji kierownika jednostki przedsiębiorcy, z wyłączeniem pełnomocników ustanowionych przez ten organ lub jednostkę,*
- *w spółce jawnej i spółce cywilnej – wspólnicy prowadzący sprawy spółki,*
- *w spółce partnerskiej – wspólnicy prowadzący sprawy spółki albo zarząd,*
- *w spółce komandytowej i spółce komandytowo-akcyjnej – komplementariusze prowadzący sprawy spółki,*
- *w przypadku osoby fizycznej prowadzącej działalność gospodarczą – ta osoba,*
- *likwidator,*
- *syndyk,*
- *zarządca ustanowiony w postępowaniu upadłościowym.*

Bez względu na charakter prowadzonej działalności każdy kierownik przedsiębiorcy ma określone zadania związane z funkcjonowaniem systemu ochrony informacji niejawnych.

Warunkiem dostępu przedsiębiorcy do informacji niejawnych w związku z wykonywaniem umów albo zadań wynikających z przepisów prawa jest zdolność do ochrony informacji niejawnych.

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

Wyjątek stanowi przedsiębiorca wykonujący działalność jednoosobowo i osobiście. W takim przypadku zdolność do ochrony informacji niejawnych potwierdza poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli tajności „poufne" lub wyższej, wydawane przez ABW albo SKW, i zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych wydawane przez ABW albo SKW.

Przepisy dotyczące bezpieczeństwa przemysłowego stosuje się także do przedsiębiorców będących podwykonawcami umów, jeżeli ich wykonywanie wiąże się z dostępem do informacji niejawnych.

W przypadku gdy przedsiębiorca zamierza wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone", świadectwo nie jest wymagane. Przedsiębiorca jest obowiązany spełnić wymagania ustawy w zakresie ochrony informacji niejawnych o klauzuli „zastrzeżone", z wyjątkiem wymogu zatrudnienia pełnomocnika ochrony, jeżeli wykonuje umowę związaną z dostępem do tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach.

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.

Należy przy tym pamiętać, iż w przypadku pozytywnego wyniku postępowania, ustawa przewiduje możliwość wydania świadectwa ubiegającej się firmie na określony czas:

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.

ABW albo SKW wydaje odrębne świadectwa potwierdzające zdolność do ochrony informacji niejawnych o klauzuli stanowiącej zagraniczny odpowiednik klauzuli „tajne" lub „poufne", stosowany przez organizacje międzynarodowe.

Postępowanie bezpieczeństwa przemysłowego jest prowadzone na wniosek przedsiębiorcy. Przesłanie do ABW lub SKW pisemnego wniosku wraz z prawidłowo wypełnionym kwestionariuszem bezpieczeństwa przemysłowego pozwala uruchomić procedury w celu wydania świadectwa bezpieczeństwa przemysłowego. Wzór kwestionariusza przedstawiono w załączniku nr 1 do rozporządzenia Rady Ministrów z dnia z dnia 5 kwietnia 2011 roku w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego.

We wniosku przedsiębiorca określa stopień świadectwa oraz klauzulę tajności informacji niejawnych, których zdolność do ochrony ma potwierdzać świadectwo. Do wniosku, poza kwestionariuszem, przedsiębiorca dołącza ankiety lub kopie poświadczeń bezpieczeństwa niżej wymienionych osób:

- kierownika przedsiębiorcy;
- pełnomocnika ochrony i jego zastępcy;
- osób zatrudnionych w pionie ochrony;
- administratora systemu teleinformatycznego;
- pozostałych osób wskazanych w kwestionariuszu, które powinny mieć dostęp do informacji niejawnych.

Dane przedstawione przez ubiegającego się o wydanie świadectwa bezpieczeństwa przemysłowego w kwestionariuszu są punktem wyjścia w realizowanej procedurze sprawdzeniowej. Dlatego we wspólnym interesie, zarówno ubiegającego się o wydanie świadectwa bezpieczeństwa przemysłowego, jak i prowadzącej postępowanie sprawdzające służby, leży szczegółowe i zgodne z wymogami ustawy oraz rozporządzeń wykonawczych wypełnienie kwestionariusza. Pozwoli to na sprawne przeprowadzenie wielotorowego i pracochłonnego postępowania sprawdzającego. Należy tu nadmienić, iż o wszelkich zmianach danych zawartych w kwestionariuszu, wnioskujący o wydanie stosownego świadectwa zobowiązany jest niezwłocznie powiadamiać służbę, do której kierował swój wniosek.

Postępowanie sprawdzające rozpoczyna się po sprawdzeniu poprawności wypełnienia kwestionariusza bezpieczeństwa przemysłowego.

Ponadto, w toku postępowania bezpieczeństwa przemysłowego sprawdzeniu podlega:

- struktura kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuacja finansowa;
- struktura organizacyjna;
- system ochrony informacji niejawnych, w tym środki bezpieczeństwa fizycznego;
- wszystkie osoby wchodzące w skład organów zarządzających, kontrolnych oraz osoby działające z ich upoważnienia;
- w szczególnie uzasadnionych przypadkach osoby posiadające poświadczenia bezpieczeństwa.

Sprawdzenie przedsiębiorcy przebiega również na podstawie danych zawartych w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie.

Organ prowadzący postępowanie sprawdzające sprawdza, czy wszystkie osoby związane z dostępem do informacji niejawnych oraz zapewnieniem bezpieczeństwa przemysłowego posiadają ważne poświadczenia bezpieczeństwa. Jeżeli osoby te nie posiadają takich poświadczeń, należy w pierwszej kolejności przeprowadzić wobec nich postępowania sprawdzające zgodnie z procedurą określoną w ustawie. Następnie wykonuje się sprawdzenia

w kartotekach, także niedostępnych powszechnie, odpowiedzialnych za kierowanie, wykonanie i bezpośrednią realizację zadań związanych z ochroną informacji niejawnych oraz pozostałych osób wskazanych w kwestionariuszu. Jednocześnie dokonuje się szczegółowych ustaleń dotyczących struktury i pochodzenia kapitału przedsiębiorcy występującego o wydanie świadectwa bezpieczeństwa przemysłowego, struktury organizacyjnej tego przedsiębiorstwa oraz jego władz (zarząd, rada nadzorcza), a także sytuacji finansowej (w tym zadłużenia, posiadane wierzytelności), źródła pochodzenia środków pozostających w dyspozycji przedsiębiorstwa. Sprawdzeniu podlegają również wyniki rocznych bilansów ekonomicznych za okres trzech ostatnich lat rozliczeniowych.

Przedmiotem sprawdzeń jest także system ochrony informacji niejawnych (pion ochrony informacji niejawnych, tajne kancelarie, system ochrony fizycznej itp.) przedsiębiorstwa ubiegającego się o wydanie świadectwa bezpieczeństwa przemysłowego, gdyż właściwe funkcjonowanie tego systemu jest kolejnym warunkiem otrzymania stosownego świadectwa. W związku z tym firma starająca się o wydanie świadectwa bezpieczeństwa przemysłowego musi posiadać pion ochrony kierowany przez pełnomocnika ds. ochrony informacji niejawnych. Zatrudnienie pełnomocnika ochrony oraz utworzenie pionu ochrony nie jest wymagane w przypadku postępowania bezpieczeństwa przemysłowego prowadzonego w celu wydania świadectwa 3-go stopnia.

Kolejnym warunkiem uzyskania świadectwa bezpieczeństwa przemysłowego I lub II stopnia jest posiadanie kancelarii tajnej/niejawnej, zorganizowanej zgodnie z wymogami określonymi w rozporządzeniu Rady Ministrów z dnia z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych.

Bardzo istotny wpływ na decyzję ABW lub SKW w kwestii wydania lub odmowy wydania takiego świadectwa ma również ocena stanu ochrony fizycznej obiektów przedsiębiorstwa.

Jeżeli wynik postępowania sprawdzającego jest pozytywny, wówczas ABW lub SKW wydaje przedsiębiorcy świadectwo bezpieczeństwa przemysłowego potwierdzające jego zdolność do zapewnienia ochrony informacji niejawnych przed nieuprawnionym ujawnieniem. Świadectwo to musi m.in. zawierać dokładne dane identyfikujące przedsiębiorcę, stopień zdolności do ochrony informacji niejawnych, jak również określa klauzulę tajności tych informacji Świadectwo bezpieczeństwa przemysłowego traci ważność z chwilą upływu jego daty ważności. Wzór *świadectw bezpieczeństwa przemysłowego przedstawia* załącznik nr 2 do Rozporządzenia Rady Ministrów z dnia z dnia 5 kwietnia 2011 roku w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego.

Należy przy tym zaznaczyć, iż w przypadku:

- odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa osobie lub osobom, które zajmują stanowisko kierownika przedsiębiorcy;
- braku możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy;
- niezorganizowania, w terminie 6 miesięcy od daty wszczęcia postępowania, kompleksowego systemu ochrony informacji niejawnych w przypadku ubiegania się o świadectwo pierwszego lub drugiego stopnia;
- zatajenia danych w kwestionariuszu lub podania w nim danych nieprawdziwych;
- podania nieprawdziwych informacji o zmianach danych zawartych w kwestionariuszu.

ABW albo SKW odmawia wydania świadectwa, stwierdzając brak zdolności do ochrony informacji niejawnych.

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

- ujawnienia, w wyniku sprawdzenia osób wchodzących w skład organów zarządzających, kontrolnych oraz osób działających z ich upoważnienia, w toku postępowania bezpieczeństwa przemysłowego niedających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1–3 lub 5 lub w art. 24 ust. 3 ustawy;
- niepowiadomienia w terminie 30 dni o zmianie danych zawartych w kwestionariuszu w trakcie postępowania bezpieczeństwa przemysłowego.

Ponadto, ustawa przewiduje obligatoryjne cofnięcie świadectwa przemysłowego. Podstawę do takiego cofnięcia stanowi utrata zdolności do ochrony informacji niejawnych, z powodu:

- odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa osobie lub osobom, które zajmują stanowisko kierownika przedsiębiorcy;
- braku możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy;
- utraty funkcjonalności systemu ochrony informacji niejawnych;
- podania nieprawdziwych danych lub zatajenia danych w ramach przekazywanych ABW albo SKW informacji o zmianach danych zawartych w kwestionariuszu.

Od decyzji o odmowie wydania lub decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej służy odwołanie do Prezesa Rady Ministrów, na którego decyzję lub postanowienie przysługuje skarga do sądu administracyjnego.

Wydawałoby się, że z chwilą wydania świadectwa bezpieczeństwa przemysłowego kończy się rola ABW lub SKW w sferze bezpieczeństwa przemysłowego. Tak jednak nie jest, bowiem organ wydający takie świadectwo, jest uprawniony także do przeprowadzenia z urzędu sprawdzenia przedsiębiorcy w celu ustalenia, czy nie utracił on zdolności do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem.

ABW lub SKW posiada więc m.in. uprawnienia pozwalające na swobodny wstęp do wszystkich obiektów i pomieszczeń jednostki kontrolowanej, gdzie informacje niejawne są przetwarzane. Może także brać udział w posiedzeniach kierownictwa jednostek kontrolowanych, dotyczących problematyki ochrony informacji niejawnych, a także żądać od kierowników i pracowników kontrolowanych jednostek ustnych lub pisemnych wyjaśnień. Jednocześnie pełni funkcje doradcze w sferze całej problematyki związanej z ochroną informacji niejawnych.

Należy również zwrócić uwagę na inne, bardzo ważne elementy, istotne z punktu widzenia ochrony informacji niejawnych, a jednocześnie warunkujące podpisanie umowy związanej z dostępem do informacji niejawnych. 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:

- 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;

– 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.

Instrukcja bezpieczeństwa przemysłowego powinna określać w szczególności:

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

– sposób postępowania z materiałami niejawnymi, które zostaną przekazane przedsiębiorcy lub przez niego wytworzone w związku z wykonywaniem umowy.

Kolejnym, istotnym elementem bezpieczeństwa przemysłowego jest obowiązek informacyjny. Jak wyszczególniono w części V niniejszego Poradnika, kierownikowi jednostki organizacyjnej przypisano kilkadziesiąt szczegółowych obowiązków. Na uwagę zasługuje fakt, że w rozdziale 9 ustawy – *Bezpieczeństwo przemysłowe* – przypisano szereg kolejnych zadań „przedsiębiorcy".

Analizując przedmiotowe zapisy w kontekście zadań kierownika jednostki organizacyjnej, należy wziąć pod uwagę, że to właśnie on faktycznie uprawniony będzie do realizacji tych zadań.

Warto zatem wymienić te „dodatkowe" obowiązki:

– *Przedsiębiorca, który zamierza wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone", jest obowiązany spełnić wymagania ustawy w zakresie ochrony informacji niejawnych o klauzuli „zastrzeżone", z wyjątkiem wymogu zatrudnienia pełnomocnika ochrony, jeżeli wykonuje umowę związaną z dostępem do tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach* – art. 54 ust. 10 ustawy;

– *We wniosku (o wszczęcie postępowania bezpieczeństwa przemysłowego) przedsiębiorca określa stopień świadectwa oraz klauzulę tajności informacji niejawnych, których zdolność do ochrony ma potwierdzać świadectwo* – art. 56 ust. 2 ustawy;

– *Do wniosku przedsiębiorca dołącza kwestionariusz bezpieczeństwa przemysłowego, …, oraz ankiety lub kopie poświadczeń bezpieczeństwa …* – art. 56 ust. 3 ustawy.

Obowiązek informacyjny, o którym wspomniano powyżej, istnieje zarówno w czasie trwania postępowania bezpieczeństwa przemysłowego, a także w okresie ważności świadectwa.

Przedmiotowy obowiązek należy rozpatrywać w dwóch aspektach:

– przedsiębiorca występujący w roli „zleceniobiorcy";

– przedsiębiorca występujący w roli „zleceniodawcy", na przykład zatrudniając podwykonawcę.

W pierwszym przypadku przedsiębiorca ma obowiązek informowania w terminie 30 dni odpowiednio ABW lub SKW o:

– *zmianach danych zawartych w kwestionariuszu, ogłoszeniu upadłości, likwidacji lub rozwiązaniu jednostki organizacyjnej albo innej formie zakończenia przez nią działalności, wypowiedzeniu umowy oraz zakończeniu wykonywania umowy* – art. 70 ust. 1 pkt 1 ustawy;

– *o zawarciu umowy związanej z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej, ze szczególnym uwzględnieniem nazwy i adresu jednostki organizacyjnej zawierającej umowę, przedmiotu umowy oraz najwyższej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonaniem*

umowy, wypowiedzeniu tej umowy oraz zakończeniu jej wykonywania – art. 70 ust. 1 pkt 2 ustawy;

– *o zawarciu umowy z podwykonawcą, związanej z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej, wypowiedzeniu tej umowy oraz zakończeniu jej wykonywania* – art. 70 ust. 1 pkt 3 ustawy.

a ponadto:

Przedsiębiorca, w czasie realizacji umowy, ma obowiązek niezwłocznego informowania osoby wyznaczonej przez „zleceniodawcę" odpowiedzialnej za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę obowiązku ochrony wytworzonych w związku z realizacją umowy lub przekazanych mu informacji niejawnych, o:

– *zmianach w systemie ochrony informacji niejawnych – art. 70 ust. 2 pkt 1 ustawy;*
– *zmianach osób wykonujących umowę* – art. 70 ust. 2 pkt 2 ustawy;
– *o potrzebie zawarcia z podwykonawcą umowy związanej z dostępem do informacji niejawnych* – art. 70 ust. 2 pkt 3 ustawy;

W drugim przypadku, przedsiębiorca może występować w roli jednostki organizacyjnej zawierającej umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej. Tutaj należy podkreślić, iż ustawa nie zwalnia podwykonawcy z obowiązku spełnienia wymagań w zakresie bezpieczeństwa przemysłowego. Dlatego, zawierając umowę z podwykonawcą związaną z dostępem do informacji niejawnych o klauzuli „poufne" i wyżej, należy zwrócić szczególną uwagę na to, czy spełnia on ustawowe wymagania w zakresie bezpieczeństwa przemysłowego, tj. posiada świadectwo bezpieczeństwa przemysłowego.

W omawianym przypadku, kierownikowi jednostki organizacyjnej przypisano następujące zadania, określone w art. 71 ustawy:

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:*
   – *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;*
   – *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) *Kierownik jednostki organizacyjnej zawierającej umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej wyznacza osobę odpowiedzialną za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę obowiązku ochrony wytworzonych w związku z realizacją umowy lub przekazanych mu informacji niejawnych.*
3) *Jednostka organizacyjna, która zawarła umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej, ma obowiązek:*
   a) *niezwłocznego informowania odpowiednio ABW lub SKW o:*
      – *nazwie i adresie przedsiębiorcy, z którym zawarto umowę,*
      – *przedmiocie umowy,*
      – *najwyższej koniecznej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonywaniem umowy,*

– *naruszeniu przepisów o ochronie informacji niejawnych u przedsiębiorcy, z którym zawarto umowę,*
– *zakończeniu wykonywania umowy;*

b) *niezwłocznego przekazania odpowiednio ABW lub SKW:*
– *kopii instrukcji bezpieczeństwa przemysłowego,*
– *kopii świadectwa przedsiębiorcy, z którym zawarto umowę.*

W omawianym temacie, rola oraz zadania kierowników jednostek organizacyjnych w zapewnieniu bezpieczeństwa przemysłowego jest niezwykle ważna. Starałem się wykazać, iż nie wystarczy spełnić ustawowych wymagań określonych tylko w rozdziale ustawy poświęconemu temu zagadnieniu. Problematykę należy rozpatrywać w szerszym aspekcie, biorąc pod uwagę zapisy w całej ustawie i aktach wykonawczych do niej.

Zlekceważenie wymienionych obowiązków skutkować może nieuzyskaniem pożądanego świadectwa lub jego utratą! Warto zauważyć, że takie konsekwencje będą bardzo „bolesne". Szacuje się bowiem, że koszty ponoszone przez przedsiębiorcę w zakresie spełnienia ustawowych wymogów bezpieczeństwa przemysłowego są wysokie i osiągnąć mogą nawet kwotę około 300 tysięcy złotych. Są to przede wszystkim wydatki na odpowiednie środki bezpieczeństwa fizycznego stosowane do zabezpieczenia informacji niejawnych. Zaliczyć do nich możemy:

– bariery fizyczne (ogrodzenia, ściany, bramy, drzwi i okna);
– szafy i zamki stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;
– elektroniczny system kontroli dostępu;
– elektroniczny system sygnalizacji włamania i napadu.

Ale należy pamiętać również o wydatkach związanych z bezpieczeństwem teleinformatycznym. W zależności od klauzul tajności przetwarzanych informacji oraz od wyników tzw. sprzętowej strefy ochrony elektromagnetycznej należy mieć na względzie zakup bardzo kosztownego sprzętu wykonanego w technologii TEMPEST.

Po tak przygotowanym systemie ochrony do kosztów należy wliczyć te poniesione za przeprowadzenie sprawdzeń wobec przedsiębiorcy i postępowań sprawdzających wobec jego pracowników (dodatkowe opłaty za każde postępowanie sprawdzające poszerzone) oraz za akredytację systemu teleinformatycznego (co najmniej kilkanaście tysięcy złotych, nie więcej jednak niż 50-krotność kwoty bazowej).

Podsumowując, bezpieczeństwo przemysłowe to ogrom przedsięwzięć, zadań i obowiązków spoczywających na kierowniku przedsiębiorcy. Dlatego winien on zatrudnić na stanowisku pełnomocnika ochrony osobę wykształconą w zakresie ochrony informacji niejawnych, sumienną i systematyczną. To na pełnomocniku ochrony spoczywać będzie główny ciężar odpowiedzialności za zapewnienie właściwego przestrzegania przepisów o ochronie informacji niejawnych w jednostce organizacyjnej. Obowiązki pełnomocnika ochrony w systemie ochrony informacji niejawnych zostały opisane w art. 15 ust. 1 ustawy. Jednakże, podobnie jak w przypadku kierownika przedsiębiorcy, wiele dodatkowych zadań wynika z kolejnych rozdziałów ustawy, a także z rozporządzeń wykonawczych do ustawy.

LITERATURA

1. Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych;
2. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych;
3. Ustawa z dnia 6 czerwca 1997 r. kodeks karny;
4. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy;
5. Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych;
6. Ustawa z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne;
7. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach;
8. Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 roku w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także trybu i sposobu zmiany lub znoszenia nadanej klauzuli;
9. Rozporządzenie Prezesa Rady Ministrów z dnia 4 października 2011 roku w sprawie zakresu, trybu i sposobu współdziałania Szefa ABW i Szefa SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa ABW;
10. Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 roku w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych;
11. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego;
12. Rozporządzenie Ministra Obrony Narodowej z dnia 2 listopada 2011 roku w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
13. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego;
14. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów poświadczeń bezpieczeństwa;
15. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa;
16. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa;
17. Rozporządzenia Rady Ministrów z dnia z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych;
18. Rozporządzenia Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych;

19. Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie trybu i sposobu nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów;
20. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego;
21. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego;
22. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego;
23. Rozporządzenie Prezesa Rady Ministrów z dnia 22 marca 2011 roku w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających;
24. Rozporządzenie Rady Ministrów z dnia z dnia 5 kwietnia 2011 roku w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego;
25. Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych;
26. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych;
27. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji;
28. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
29. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych;
30. Dokument C-M (2002) 49 – bezpieczeństwo w ramach Organizacji Traktatu Północnoatlantyckiego;
31. Wytyczne Agencji Bezpieczeństwa Wewnętrznego w sprawie postępowania z informacjami niejawnymi międzynarodowymi – bip.abw.gov.pl;
32. Zalecenia DBTI ABW regulujące bezpieczeństwo teleinformatyczne – bip.abw.gov.pl
33. Decyzja Nr 61/MON z dnia 05 marca 2012 roku w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz w komórkach organizacyjnych Ministerstwa Obrony Narodowej;
34. Hoc Stanisław - Ustawa o ochronie informacji niejawnych. Komentarz.