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 koniecznością 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