Rewolucja czy ewolucja w ochronie informacji niejawnych. Ułatwienie czy utrudnienie dla przedsiębiorców

Tadeusz KOCZKOWSKI - Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice

Prosimy cytować jako: CHEMIK 2011, **65,** 3, 179-180

W Polsce od wielu lat wskazywano na potrzebę stworzenia nowego aktu prawnego regulującego zasady funkcjonowania systemu ochrony informacji niejawnych, uwzględniającego aktualny stan rozwoju nowoczesnych technologii. 5 sierpnia 2010 r. uchwalona została przez Sejm i podpisana przez Prezydenta RP, nowa ustawa o ochronie informacji niejawnych, zastępująca starą ustawę o tym samym tytule z 22 stycznia 1999 r., która w ciągu 11 lat doczekała się aż 23 nowelizacji.

Jednym z powodów opracowania nowego aktu prawnego jest fakt, iż w bieżącym roku Polska obejmuje przewodnictwo w Radzie Unii Europejskiej, co wiąże się z nowymi wymaganiami wobec administracji państwowej, w tym z koniecznością dostosowania polskiego systemu ochrony informacji niejawnych do reguł i praktyki obowiązującej w instytucjach Unii Europejskiej i innych krajach członkowskich. Praktyka ujawniła także potrzebę stworzenia nowej ustawy wprowadzającej kompleksowe, spójne, konsekwentne i łatwe do zastosowania regulacje prawne, zmierzające do uproszczenia obowiązującego systemu ochrony informacji niejawnych, przy równoczesnym zwiększeniu jego efektywności. Celem pośrednim wprowadzenia nowej ustawy jest zwiększenie zakresu dostępu obywateli do informacji publicznej zgodnie z wymogami ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.

Wśród podmiotów, na które oddziałuje nowa ustawa znaleźli się m.in. przedsiębiorcy zamierzający ubiegać się lub już ubiegający się o zawarcie lub wykonujący umowy, związane z dostępem do informacji niejawnych, kierownicy jednostek organizacyjnych, w których przetwarzane są informacje niejawne i pełnomocnicy ochrony informacji niejawnych, a także organy władzy publicznej, Siły Zbrojne RP i ich jednostki organizacyjne, jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, państwowe osoby prawne i państwowe jednostki organizacyjne.

W przepisach ogólnych zdecydowano się na rozszerzenie pojęcia „przedsiębiorców", uwzględniając w tej grupie niektóre z pominiętych we wcześniejszej ustawie podmiotów gospodarczych, jak np. spółdzielnie, które również mają prawo ubiegać się o realizację umów związanych z dostępem do informacji niejawnych. Wprowadzono również definicje nowych terminów, takich jak „kierownik przedsiębiorcy", „przetwarzanie informacji niejawnych", „ryzyko", „szacowanie ryzyka" i „zarządzanie ryzykiem".

Jedna krajowa władza bezpieczeństwa odpowiedzialna za ochronę informacji niejawnych

Jednym z fundamentalnych założeń nowej ustawy jest rezygnacja z podziału informacji niejawnych na tajemnicę państwową i służbową, który w praktyce okazał się sztuczny i niepotrzebny, na rzecz ściślejszego zdefiniowania klauzul, wśród których wyróżniono klauzule „ściśle tajne", „tajne", „poufne" i „zastrzeżone". Postanowiono również odejść od rozbudowanych formalnych wykazów informacji niejawnych, w zamian zobowiązując wytwórców informacji do kierowania się nowymi definicjami poszczególnych klauzul i rzetelnego przydzielania ich poszczególnym informacjom znajdującym się w ich kompetencjach. Stworzono możliwość „odwołania się" od decyzji wytwórcy, dotyczącej nadania klauzuli tajności, do ABW lub SKW, w szczególnych sytuacjach do Prezesa Rady Ministrów, w przypadku, kiedy wydaje się być ona bezpodstawnie zawyżona.

Istotną zmianą jest wprowadzenie, na wzór zdecydowanej większości krajów NATO i UE, jednej krajowej władzy bezpieczeństwa odpowiedzialnej za ochronę informacji niejawnych wymienianych z NATO i UE, której funkcję pełnić będzie Szef ABW. Dotychczas funkcja ta była pełniona równolegle przez szefów ABW i SKW, co tłumaczono istnieniem odmiennych standardów ochrony informacji niejawnych w sferze cywilnej i wojskowej. Nowa ustawa czyni Szefa SKW tylko pośrednikiem krajowej władzy bezpieczeństwa, odpowiedzialnym za realizację jej zadań wobec podmiotów sfery wojskowej. Precyzyjne i jednoznaczne określenie w ustawie kompetencji ABW i SKW ma na celu wyeliminowanie przypadków prowadzenia przez obie służby czynności wobec tych samych podmiotów. Uregulowano zasady prowadzenia przez ABW i SKW kontroli stanu zabezpieczenia informacji niejawnych, czego brakowało w poprzedniej ustawie.

W celu uproszczenia systemu ochrony informacji niejawnych, poprzez zmniejszenie ich liczby oraz liczby jednostek je przetwarzających, a co za tym idzie obniżenie wydatków budżetowych, postanowiono zrezygnować z traktowania informacji dotyczących prawnie chronionych interesów obywateli i jednostek organizacyjnych, jako informacji niejawnych, gdyż są one objęte tajemnicami różnego rodzaju i uwzględnione w aktach prawnych normalizujących te tajemnice. Ochronie określonej przepisami tej ustawy podlegać będą wyłącznie informacje, których ujawnienie przyniosłoby szkodę całemu państwu.

Zarządzanie ryzykiem poziomu bezpieczeństwa

Nowa ustawa umożliwia stosowanie zarządzania ryzykiem przy określaniu poziomów bezpieczeństwa fizycznego i teleinformatycznego. Dopasowanie odpowiednich środków ochrony do liczby i rangi chronionych informacji oraz rzeczywistego poziomu istniejących dla nich zagrożeń, pozwoli na ograniczenie nadmiernych wydatków z nimi związanych. Zaletą tego rozwiązania jest ułatwienie akredytacji systemów teleinformatycznych, służących przekazywaniu i przetwarzaniu informacji niejawnych, co zyska duże znaczenie w okresie prezydencji Polski w Unii Europejskiej.

Dążąc do większej elastyczności systemu ochrony informacji niejawnych, zrezygnowano ze ścisłej kontroli obiegu dokumentów o niższych klauzulach, zwłaszcza o klauzuli „zastrzeżone". Rozwiązanie to umożliwi zaoszczędzenie znacznych środków finansowych w budżetach administracji państwowej i samorządowej przeznaczanych na zbędne środki ochrony informacji o niższej randze.

Do najważniejszych zmian zaliczyć należy także wprowadzenie okresowego przeglądu dokumentów niejawnych (nie rzadziej niż raz na 5 lat) w celu określenia, czy informacje w nich zawarte nadal spełniają ustawowe warunki, będące podstawą do nadania im klauzuli tajności. W zależności od wyniku przeprowadzonego przeglądu, klauzula może zostać utrzymana, zmieniona lub też całkowicie zniesiona. Wprowadzono również możliwość określenia z góry daty lub wydarzenia, po którym nastąpi zmiana lub zniesienie klauzuli tajności, jak również możliwość odrębnego klauzulowania poszczególnych części dokumentu. Możliwość zmiany lub zniesienia klauzuli tajności nie dotyczy informacji służących identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji uprawnionych do wykonywania czynności operacyjno-rozpoznawczych oraz osób udzielających pomocy w wykonywaniu tych czynności.

Zgodnie z art. 42 nowej ustawy obowiązek organizacji kancelarii tajnych nałożono wyłącznie na jednostki organizacyjne dysponujące informacjami oznaczonymi klauzulami „tajne" lub „ściśle tajne". Zasady obiegu informacji „poufnych" będzie określał kierownik jednostki organizacyjnej. Za zgodą ABW lub SKW będzie można zorganizować kancelarię tajną obsługującą dwie lub więcej jednostek organizacyjnych, których kierownicy zawrą porozumienie w zakresie jej podległości i zasad finansowania. Powodem wprowadzenia tych przepisów są wysokie koszty organizacji kancelarii tajnych, na które nie zawsze może sobie pozwolić każda jednostka organizacyjna.

Istotne znaczenie ma również wprowadzenie obowiązku szkolenia w zakresie ochrony informacji, nie rzadziej niż co 5 lat, wszystkich osób mających dostęp do informacji niejawnych. Szkolenia dla kierowników jednostek organizacyjnych prowadzić będzie ABW lub SKW wspólnie z pełnomocnikami ochrony.

Bezpieczeństwo osobowe

Opracowano wiele nowych przepisów dotyczących bezpieczeństwa osobowego, jak np. wprowadzenie zapisu o zniesieniu istniejącego do tej pory obowiązku prowadzenia postępowań sprawdzających wobec osób, które mają uzyskać dostęp do informacji niejawnych o klauzuli „zastrzeżone". Od chwili wejścia ustawy w życie wystarczy uzyskać pisemne upoważnienie kierownika jednostki organizacyjnej po odbyciu stosownego przeszkolenia. W miejsce trzech dotychczasowych rodzajów postępowań sprawdzających wprowadzono tylko dwa: zwykłe postępowanie sprawdzające prowadzone przez pełnomocników ochrony wobec osób ubiegających się o dostęp do informacji niejawnych o klauzuli „poufne" oraz postępowanie poszerzone prowadzone przez ABW lub SKW wobec osób ubiegających o dostęp do informacji niejawnych o klauzuli „tajne" i „ściśle tajne", a w niektórych przypadkach również „poufne". W celu uniknięcia sytuacji, w której pełnomocnik ochrony prowadziłby postępowanie sprawdzające w stosunku do swojego pracodawcy wprowadzono zasadę prowadzenia przez służby postępowań wobec wszystkich kierowników jednostek organizacyjnych niezależnie od klauzuli. *Novum* jest również dopisanie do listy osób mających dostęp do informacji niejawnych bez postępowania sprawdzającego osoby wybranej na urząd Prezydenta RP.

W rozdziale szóstym ustawy określono m.in. tryb odwoływania się od decyzji o odmowie lub cofnięciu poświadczenia bezpieczeństwa, do czego prawo 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.

Bezpieczeństwo teleinformatyczne

W obszarze przepisów dotyczących bezpieczeństwa teleinformatycznego wprowadzono zapis, na mocy którego akredytacji 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 systemu, przy czym jego obowiązkiem będzie przekazanie ABW lub SKW dokumentacji bezpieczeństwa teleinformatycznego akredytowanego systemu. Natomiast systemy teleinformatyczne przetwarzające informacje niejawne o klauzuli „poufne" lub wyższej, będą akredytowane przez ABW lub SKW. Służby te dokonują oceny dokumentacji bezpieczeństwa teleinformatycznego oraz audytu bezpieczeństwa teleinformatycznego. Wszystkie urządzenia i narzędzia kryptograficzne przeznaczone do ochrony informacji niejawnych będą podlegać procesowi certyfikacji prowadzonemu również przez ABW lub SKW, co umożliwi ich stosowanie w NATO i UE. Z obowiązku akredytacji wyłączono systemy teleinformatyczne służące pozyskiwaniu i przekazywaniu w sposób niejawny informacji uzyskanych w trakcie czynności operacyjno-rozpoznawczych przez uprawnione do tego podmioty oraz systemy 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.

Pewnych transformacji dokonano również w zakresie regulacji związanych z bezpieczeństwem przemysłowym. W związku ze zmianą definicji klauzul tajności świadectwo bezpieczeństwa przemysłowego określono jako dokument potwierdzający zdolność do ochrony informacji niejawnych o klauzuli „poufne" i wyżej, dostosowując w ten sposób przepisy krajowe do standardowych rozwiązań stosowanych w krajach NATO i UE. Świadectwa bezpieczeństwa przemysłowego nie muszą już uzyskiwać przedsiębiorcy wykonujący działalność osobiście, którym wystarczy poświadczenie bezpieczeństwa potwierdzające zachowanie przez nich tajemnicy. Zniesiono również konieczność tworzenia pionów ochrony przez przedsiębiorców ubiegających się o świadectwo bezpieczeństwa przemysłowego trzeciego stopnia, co wiązało się z dużymi kosztami. Obowiązek przeszkolenia pracownika przedsiębiorcy w zakresie ochrony informacji niejawnych spada na pełnomocnika ochrony jednostki zamawiającej. W uzasadnionych przypadkach przedsiębiorca może ubiegać się o tymczasowy i jednorazowy dostęp do informacji niejawnych. Nowa ustawa, w odróżnieniu od wcześniejszej, określa przesłanki odmowy i cofnięcia świadectwa bezpieczeństwa przemysłowego. W okresie ważności świadectwa ABW lub SKW może przeprowadzić sprawdzenie przedsiębiorcy pod kątem spełniania wymogań określanych w przepisach, w celu ustalenia, czy nie utracił on zdolności do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem.

Twórcy nowej ustawy zakładają że będzie ona miała istotny wpływ na usprawnienie funkcjonowania systemu ochrony informacji niejawnych w Polsce, w tym na zwiększenie jego elastyczności, pośrednio również na sektor finansów publicznych, zwłaszcza na budżet państwa i budżet jednostek samorządu terytorialnego, na konkurencyjność gospodarki i przedsiębiorczość, bezpieczeństwo państwa, czy jakość demokracji.

Wdrażanie ustawy

Aktualnie trwa proces wdrażania ustawy. Ukazało się pięć nowych rozporządzeń a pozostałe są w trakcie przygotowywania. Krajowe Stowarzyszenie Ochrony Informacji Niejawnych (KSOIN) prowadzi cykl szkoleń dla kierowników jednostek organizacyjnych i pracowników pionów ochrony. Szczególnej uwadze polecam Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych pod patronatem Generalnego Inspektora Ochrony Danych Osobowych (GIODO) Pana Ministra Wiewiórowskiego (25-27 maja br., Spała, Ośrodek Przygotowań Olimpijskich) oraz II Forum Kierowników Jednostek Organizacyjnych połączone z VI Forum Pełnomocników Ochrony, które odbędzie się w listopadzie br. Poza tym proponowane są inne formy szkoleń (konwersatoria, seminaria, kursy i warsztaty) z ochrony informacji niejawnych, biznesowych i danych osobowych. Możliwe jest również przeprowadzenie auditu ochrony informacji i danych osobowych w firmie. Wszystkie informacje na powyższe tematy można znaleźć na naszej stronie www.ksoin.pl.

Płk mgr Mieczysław Tadeusz KOCZKOWSKI – Prezes Zarządu Krajowego Stowarzyszenia Ochrony Informacji (KSOIN) oraz Wiceprezes Międzynarodowego Stowarzyszenia Oficerów Rezerwy Wojska, Krąg Mars i Merkury-Polska. Pomysłodawca i animator utworzenia stowarzyszeń zrzeszających pracowników pionów ochrony i innych osób zainteresowanych problematyką bezpieczeństwa informacji. Inicjator i współtwórca Podyplomowych Studiów Ochrony Informacji Niejawnych, Danych Osobowych i Innych Prawnie Chronionych w Administracji i Biznesie prowadzonych na kilku wyższych uczelniach. Organizator wielu specjalistycznych kursów, forum, kongresów, warsztatów i innych szkoleń z zakresu ochrony informacji i danych osobowych kierowanych do różnych grup i środowisk zawodowych. KSOIN współpracuje z wieloma ośrodkami naukowymi, izbami gospodarczymi, wyspecjalizowanymi firmami z branży security, uczestniczy w targach i wystawach związanych z obronnością i bezpieczeństwem państwa, wspiera i udziela pomocy pracownikom pionów ochrony oraz przedsiębiorcom przy ocenie zagrożeń i wdrażaniu procedur bezpieczeństwa informacji.