# Informacje niejawne – ochrona

Tomasz A. Winiarczyk

## zagadnienia

- pojęcia podstawowe
- klasyfikacja informacji niejawnych
- nadawanie klauzuli tajności
- zasady ochrony informacji niejawnych
- ochrona informacji niejawnych w jednostce organizacyjnej
- dopuszczanie osoby do pracy z informacjami niejawnymi
- kancelarie tajne
- systemy teleinformatyczne
- zdolność przedsiębiorcy do ochrony informacji niejawnych
- instrukcja postępowania z materiałami niejawnymi

# podstawa prawna

- USTAWA z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych



# rękojmia zachowania tajemnicy

- zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego

# dokument w rozumieniu ustawy

- każda utrwalona informacja niejawna



# materiał w rozumieniu ustawy

- dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna,
  - zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia

# przetwarzanie informacji niejawnych

- wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach,
  - w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie



# dokument szczególnych wymagań bezpieczeństwa

- systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;

**dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego**

- opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp



# dokumentacja bezpieczeństwa systemu teleinformatycznego

- opracowane zgodnie z zasadami określonymi w ustawie
  - dokument szczególnych wymagań bezpieczeństwa
  - dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego

# akredytacja bezpieczeństwa teleinformatycznego

- dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych



# certyfikacja i audyt

- **certyfikacja** — proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych
- **audyt bezpieczeństwa systemu** teleinformatycznego — weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego

# zasady ogólne – art. 4 ust. 1

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



# zasady ogólne – art. 4 ust. 2

- Zasady zwalniania od obowiązku zachowania w tajemnicy informacji niejawnych oraz sposób postępowania z aktami spraw zawierającymi informacje niejawne w postępowaniu przed sądami i innymi organami określają przepisy odrębnych ustaw.

# zasady ogólne – art. 4 ust. 3

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



# ściśle tajne

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

1) zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
2) zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
3) zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
4) osłabi gotowość obronną Rzeczypospolitej Polskiej;
5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
6) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
7) zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. — Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.), lub osób dla nich najbliższych.

# tajne

**Art. 5. 2.** Informacjom niejawnym nadaje się klauzulę „tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
2) pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
3) zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
4) utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
5) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
6) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

# poufne

**Art. 5. 3.** Informacjom niejawnym nadaje się klauzulę „poufne”, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
6) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

# zastrzeżone

**Art. 5. 4.** Informacjom niejawnym nadaje się klauzulę „zastrzeżone”, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

# nadawanie klauzuli tajności

- Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.
  - Osoba ta może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.
  - Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez tę osobę albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony.
- Informacje niejawne podlegają ochronie w sposób określony w ustawie do czasu zniesienia lub zmiany klauzuli tajności.
- Kierownicy jednostek organizacyjnych przeprowadzają nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.

# informacje niejawne bez względu na upływ czasu

- Chronione bez względu na upływ czasu, z zastrzeżeniem art. 7 ust. 2, są:

1) dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji, uprawnionych do wykonywania na podstawie ustawy czynności operacyjno-rozpoznawczych jako funkcjonariuszy, żołnierzy lub pracowników wykonujących te czynności;
2) dane mogące doprowadzić do identyfikacji osób, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy;
3) informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.



# zasada ograniczonego dostępu do informacji niejawnych

- informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy na zajmowanym stanowisku
- tzw. zasada **„need-to-know”**

# zasada ograniczenia udostępniania

- udostępnianie informacji niejawnych wyłącznie osobom gwarantującym ich ochronę przed nieuprawnionym ujawnieniem



# zasada podporządkowania środków ochrony typowi klauzuli

- środki ochrony fizycznej i zasady bezpieczeństwa obiegu dokumentów muszą być dostosowane do klauzuli tajności wytwarzanych, przetwarzanych i przechowywanych informacji
- dzięki temu dokumenty i materiały, które zawierają informacje niejawne takiej samej wagi są w każdej instytucji chronione w taki sam lub podobny sposób.

# zasada dostosowania ochrony

- dostosowanie zakresu środków ochrony fizycznej do uwarunkowań i specyfiki danej instytucji
- zakres stosowania środków ochrony fizycznej musi jednocześnie:
  - być adekwatny do klauzuli tajności i ilości informacji niejawnych, zgodnie z zasadą podporządkowania środków ochrony klauzuli informacji, jak również poziomowi dostępu do tego typu informacji osób zatrudnionych
  - uwzględniać zalecenia służb ochrony państwa, związane z ochroną przed zagrożeniami pochodzącymi od obcych służb specjalnych



# zasada kontroli wytwórcy nad sposobem ochrony informacji

- każda osoba, która ma prawo do podpisania dokumentu lub oznaczenia materiału innego niż dokument ma również prawo do określenia klauzuli tajności, która wpływa na dobór środków ochrony danej informacji

# zasada odpowiedniości klauzuli

- zakaz zaniżania lub zawyżania klauzuli tajności
- zasada ta wymusza stosowanie środków ochrony, które będą adekwatne do wagi określonej informacji, czego konsekwencją jest uniknięcie ponoszenia niepotrzebnych kosztów, które wiązałyby się z praktykami zawyżania klauzuli tajności, jak również koncentrowanie środków na ochronie informacji, która wymaga specjalnych środków bezpieczeństwa



# oznaczenia klauzul tajności

- oznaczenia klauzul tajności:

1) „00”— dla klauzuli „ściśle tajne”;
2) „0” — dla klauzuli „tajne”;
3) „Pf”— dla klauzuli „poufne”;
4) „Z”— dla klauzuli „zastrzeżone”.

# nadzór nad funkcjonowaniem systemu ochrony informacji niejawnych

- kompetencja ABW i SKW
- Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.
- Krajowa władza bezpieczeństwa jest właściwa do nadzorowania systemu ochrony informacji niejawnych w stosunkach RP z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do informacji niejawnych NATO, Unii Europejskiej lub innych organizacji międzynarodowych.



# współpraca

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

# odpowiedzialność kierownika jednostki

- Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.



# pełnomocnik ochrony

- Kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

# pełnomocnik ochrony

- Kierownik jednostki organizacyjnej może zatrudnić zastępcę lub zastępców pełnomocnika ochrony, z zastrzeżeniem spełnienia przez te osoby warunków określonych w ustawie.
- Szczegółowy zakres czynności zastępcy pełnomocnika ochrony określa kierownik jednostki organizacyjnej.



# zadania pełnomocnika ochrony

- Do zadań pełnomocnika ochrony należy:

1) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;
2) zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne;
3) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;
4) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów;
5) opracowywanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji;
6) prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
7) prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających;
8) prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto;
9) przekazywanie odpowiednio ABW lub SKW do ewidencji danych osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa.

# pion ochrony

- Swoje zadania pełnomocnik ochrony realizuje przy pomocy wyodrębnionej i podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnych, jeżeli jest ona utworzona w jednostce organizacyjnej.



# naruszenie przepisów

- W przypadku stwierdzenia naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych pełnomocnik ochrony zawiadamia o tym kierownika jednostki organizacyjnej i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków.

# szkolenia – art. 19 i nast.

- Wszystkie osoby mające dostęp do informacji niejawnych będą szkolone w zakresie ochrony tych informacji nie rzadziej niż co 5 lat.



# zaświadczenie

- Odbierając zaświadczenie o odbyciu szkolenia w zakresie ochrony informacji niejawnych, osoba przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.

# dopuszczenie do pracy

- Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej może nastąpić po:

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



# dopuszczenie do pracy

Osoby nieposiadające obywatelstwa polskiego nie mogą być dopuszczone do pracy lub pełnienia służby na stanowiskach albo wykonywania czynności zleconych, z którymi łączy się dostęp do informacji niejawnych o klauzuli „tajne” lub „ściśle tajne”.

– istnieją w tym zakresie wyjątki

# postępowanie sprawdzające

- Pełnomocnik ochrony przeprowadza **zwykłe postępowanie sprawdzające** na pisemne polecenie kierownika jednostki organizacyjnej.
  - Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.
- W szczególnych sytuacjach przeprowadza się **poszerzone lub specjalne postępowanie sprawdzające**.



# postępowanie sprawdzające

- **zwykłe** – prowadzone przez pełnomocników ochrony (do „poufne”)
- **poszerzone** – prowadzone przez ABW lub SKW (do „ściśle tajne” i „tajne”).

# poświadczenie bezpieczeństwa

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



# kancelarie tajne – art. 42 i nast.

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

# systemy teleinformatyczne

- Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego.
  - Potwierdzeniem udzielenia przez ABW albo SKW akredytacji jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.
    - Udziela się go na czas określony, nie dłuższy niż 5 lat.



# dot. ochrony danych osobowych

- Uwzględniając kategorie przetwarzanych danych o raz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:

1) podstawowy;
2) podwyższony;
3) wysoki.

ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

# systemy teleinformatyczne

- ABW albo SKW może odstąpić od przeprowadzenia audytu bezpieczeństwa systemu teleinformatycznego, jeżeli system jest przeznaczony do przetwarzania informacji niejawnych o klauzuli „poufne”.
- Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.



# zdolność przedsiębiorcy do 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.
  - W przypadku przedsiębiorcy wykonującego działalność jednoosobowo i osobiście zdolność do ochrony informacji niejawnych potwierdza poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli tajności „poufne” lub wyższej, wydawane przez ABW albo SKW, i zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych wydawane przez ABW albo SKW.

# rodzaje świadectw

- 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.



# okresy ważności świadectw

- Świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli:

1) „ściśle tajne” potwierdza zdolność do ochrony informacji niejawnych o klauzuli:
   a) „ściśle tajne” — przez okres 5 lat od daty wystawienia,
   b) „tajne” — przez okres 7 lat od daty wystawienia,
   c) „poufne” — przez okres 10 lat od daty wystawienia;
2) „tajne” potwierdza zdolność do ochrony informacji niejawnych o klauzuli:
   a) „tajne” — przez okres 7 lat od daty wystawienia,
   b) „poufne” — przez okres 10 lat od daty wystawienia;
3) „poufne” potwierdza zdolność do ochrony informacji niejawnych o tej klauzuli przez okres 10 lat od daty wystawienia.

# instrukcja postępowania z materiałami niejawnymi

- konieczność posiadania przez jednostkę
- może stanowić część instrukcji kancelaryjnej



# elementy instrukcji

- zakres rzeczowy informacji niejawnych
- warunki dostępności do informacji niejawnych
- zasady ewidencjonowania dokumentów niejawnych
- uprawnienia do dostępu do informacji niejawnych
- zasady udostępniania informacji niejawnych
- wymagania w zakresie opracowywania i oznaczania dokumentów niejawnych
- zasady przygotowania dokumentów do wysyłki
- zasady gromadzenia dokumentów niejawnych
- zasady odpowiedzialności za informacje niejawnych
- zasady nadzoru w zakresie ochrony informacji zastrzeżonych