OBRONNOŚĆ. Zeszyty Naukowe 4(28)/2018
ISSN 2299-2316

AUTOR
Krzysztof Krzykwa

BEZPIECZEŃSTWO OSOBOWE I OCHRONA FIZYCZNA INFORMACJI NIEJAWNYCH W UNII EUROPEJSKIEJ

Słowa kluczowe: Unia Europejska, bezpieczeństwo osobowe, ochrona informacji niejawnych, poświadczenie bezpieczeństwa

Wszelkie informacje, których nieuprawnione ujawnienie mogłoby lub spowodowałoby szkodę dla państwa lub byłoby niekorzystne z punktu widzenia jego interesów, nazywamy informacjami niejawnymi.

Aby zachować standardy i pewność państw członkowskich, co do zapewnienia należytej ochrony informacjom niejawnym wytwarzanym w Unii Europejskiej (UE) i przekazywanym między państwami członkowskimi, określono minimalne zasady obowiązujące w całej Unii. Tym samym każde państwo członkowskie UE zobowiązane jest przestrzegać przepisów określonych w dokumentach normatywnych, tak aby każda ze stron mogła mieć pewność, że zagwarantowany został równy poziom ochrony informacji niejawnych UE.

Zasady te opublikowano w niżej wymienionych dokumentach regulujących postępowanie z materiałami niejawnymi w UE:

- *Decyzja Komisji (UE, Euratom) 2015/444 w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE*,
- *Decyzja Rady z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (2013/488/UE*), nazywana dalej *Decyzją*.

W Polsce przepisy określające postępowanie z materiałami niejawnymi reguluje *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz. U. z 2018 r., poz. 412 j.t.), nazywana dalej *Ustawą*. Dokument ten głównie ukierunkowany jest na określenie zasad przetwarzania materiałów niejawnych krajowych, ale stanowi także podstawę do organizacji funkcjonowania bezpieczeństwa osobowego, ochrony fizycznej, bezpieczeństwa teleinformatycznego, a także bezpieczeństwa przemysłowego w odniesieniu do materiałów niejawnych międzynarodowych, w tym UE. Nadzór nad funkcjonowaniem systemu ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi sprawuje Agencja Bezpieczeństwa Wewnętrzne-

go[1] (ABW). ABW jest uprawniona do wydawania dokumentów upoważniających do dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej lub innych organizacji międzynarodowych[2]. Szef ABW pełni funkcję krajowej władzy bezpieczeństwa[3]. W odniesieniu do sfery wojskowej funkcja krajowej władzy bezpieczeństwa pełniona jest przez Szefa ABW za pośrednictwem Szefa Służby Kontrwywiadu Wojskowego (SKW)[4]. W celu zapewnienia jednolitości systemu ochrony informacji niejawnych międzynarodowych i jego zgodności z przepisami międzynarodowymi krajowa władza bezpieczeństwa wydała 31 grudnia 2010 r. *Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi*, których stosowanie zaleca.

Przepisy UE definiują pojęcie *dokumentu* jako *każdą zapisaną informację, niezależnie od jej postaci fizycznej lub cech.* W rozumieniu *Ustawy dokumentem jest każda utrwalona informacja niejawna*[5]. Oprócz tego został wprowadzony dodatkowy termin: *materiał*, rozumiany w *Decyzji* jako *jakikolwiek dokument, nośnik danych lub dowolne urządzenia lub sprzęt, już wytworzone lub w trakcie wytwarzania*. Natomiast w *Ustawie* materiałem nazywa się *dokument lub przedmiot albo dowolną jego część, chronione jako informacja niejawna*[6]. Należy zauważyć, że w obu przypadkach definicja materiału zawiera w sobie również definicję dokumentu.

Materiały niejawne UE otrzymują klauzulę tajności[7]:

- TRES SECRET UE/EU TOP SECRET - są to materiały, których nieuprawnione ujawnienie mogłoby wyrządzić wyjątkowo poważną szkodę podstawowym interesom UE lub co najmniej jednego państwa członkowskiego.
- SECRET UE/EU SECRET - są to materiały, których nieuprawnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom UE lub co najmniej jednego państwa członkowskiego.
- CONFIDENTIEL UE/EU CONFIDENTIAL - są to materiały, których nieuprawnione ujawnienie mogłoby zaszkodzić podstawowym interesom UE lub co najmniej jednego państwa członkowskiego.
- RESTREINT UE/EU RESTRICTED.

Powyższe definicje oznaczają, że samo zaistnienie możliwości wyrządzenia szkody stanowi przesłankę do właściwej ochrony informacji niejaw-

[1] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, Dz. U. z 2018 r., poz. 412 j.t., art. 11 ust. 2.
[2] Tamże.
[3] Tamże, art. 11 ust. 1.
[4] Tamże, art. 11 ust. 3.
[5] Tamże, art. 2 pkt 3.
[6] Tamże, art. 2 pkt 4.
[7] *Decyzja Rady z dnia 23 września w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE* (2013/488/UE), art. 2 ust. 2.

nych. Natomiast zgodnie z przepisami krajowymi[8], dopiero nieuprawnione ujawnienie, które taką szkodę spowoduje, stanowi podstawę do nadania odpowiedniej klauzuli tajności.

Tak sformułowane definicje dają w pewnym sensie swobodę interpretacyjną, jakie informacje i w jaki sposób mogą wpłynąć na szkodę państwa. Ciężar odpowiedzialności w tym zakresie został przesunięty w kierunku osoby uprawnionej do podpisania dokumentu, która mocą *Ustawy* została uprawniona do nadania klauzuli tajności[9]. W tym miejscu należy wskazać, że zgodnie z przepisami Unii Europejskiej za określenie poziomu tajności i za początkową dystrybucję informacji odpowiada wytwórca dokumentu niejawnego Unii Europejskiej[10].

Problematyczny jest przepis określony w art. 5 ust. 5 *Ustawy*, który mówi, że informacje niejawne przekazane przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych oznacza się polskim odpowiednikiem klauzuli tajności. Taka treść może być rozumiana jako zmiana klauzuli tajności organizacji międzynarodowych (w tym Unii Europejskiej) na klauzulę tajności krajową. W konsekwencji może to doprowadzić do naruszenia systemu ochrony informacji niejawnych poprzez zapoznanie osoby z informacją niejawną międzynarodową, która nie posiada poświadczenia bezpieczeństwa tej organizacji. Z drugiej strony przepis ten może być rozumiany jako stosowanie podwójnej ochrony dla dokumentów krajowych i międzynarodowych zgodnie z przepisami Unii Europejskiej.

Nie ma jednolitej interpretacji tego przepisu. Odpowiednie postępowanie, zapewniające spełnienie przesłanek ochrony polega na tym, że materiały niejawne przekazane przez państwa na podstawie umów międzynarodowych oznacza się polskim odpowiednikiem klauzuli tajności i od tego momentu chroni się jak dokument krajowy. Natomiast materiałom niejawnym przekazanym przez UE pozostawia się oryginalne klauzule tajności i chroni się zgodnie z przepisami tych organizacji.

Warto zaznaczyć, że przepisy UE[11] dopuszczają przypadek odwrotny, to znaczy możliwość wprowadzenia do struktur lub sieci Unii informacji niejawnych pochodzących z państw członkowskich i oznaczonych klauzulą tajności obowiązującą w danym państwie, z zastrzeżeniem, że materiałowi nadaje się klauzulę tajności równorzędną klauzuli UE, a w uzasadnionych przypadkach można nadać klauzulę wyższą. Krajowe przepisy takiego przypadku nie przewidują.

Wymóg właściwego oznaczania dokumentów i materiałów został zachowany dla każdej informacji niejawnej niezależnie od jej pochodzenia.

[8] *Ustawa o ochronie…*, art. 5 ust. 1 – 3.
[9] Tamże, art. 6 ust. 1.
[10] *Decyzja Rady w sprawie…*, Załącznik III pkt 3.
[11] Tamże, art. 4 ust. 3.

Oznaczenia powinny być wyraźne i poprawne, niezależnie od tego czy dokument niejawny UE występuje w formie pisemnej, ustnej, elektronicznej lub jakiejkolwiek innej. Przez poprawność rozumie się oznaczenie klauzulą tajności składającą się z dwóch członów: nazwy francuskiej łamanej na angielską. Dopuszcza się stosowanie standardowych skróconych oznaczeń klauzul tajności do pojedynczych ustępów tekstu, krótszych niż jedna strona:

- TRES SECRET UE/EU TOP SECRET - TS-UE/EU-TS
- SECRET UE/EU SECRET - S-UE/EU-S
- CONFIDENTIEL UE/EU CONFIDENTIAL - C-UE/EU-C
- RESTREINT UE/EU RESTRICTED - R-UE/EU-R

Skróty te nie zastępują pełnych nazw klauzul tajności. Krajowe przepisy nie przewidują stosowania skrótów klauzul tajności.

Oprócz jednej z klauzul tajności dopuszcza się stosowanie dodatkowych oznaczeń takich jak:

- identyfikacja wytwórcy,
- wszelkie oznaczenia zastrzegające, kody słowne lub akronimy określające obszar działalności, do którego odnosi się dany dokument, szczególny sposób dystrybucji dokumentu zgodnie z zasadą need-to-know lub ograniczenia w zakresie wykorzystania,
- oznaczenia dotyczące możliwości udostępnienia,
- data lub konkretne wydarzenie, po których klauzula tajności może zostać obniżona.

Obowiązkowo numeruje się strony dokumentu, umieszcza datę, numer referencyjny i temat, który nie stanowi informacji niejawnej (chyba, że z jego oznaczenia wynika inaczej), a także oznacza się numer kopii, dla informacji niejawnych SECRET UE/EU SECRET lub wyższej.

Sposób oznaczania krajowych dokumentów niejawnych określa *Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności* (Dz. U. poz. Nr 288). Generalnie krajowe przepisy dotyczące oznaczeń są zbieżne z wymogami Unii. Wymienione rozporządzenie bardzo szczegółowo określa sposób i miejsce wymaganych oznaczeń.

Dyrektywa wskazuje konieczność określenia daty ważności klauzuli niejawności lub wydarzenia, po którym informacje w nim zawarte stają się jawne, w szczególności dotyczy to materiałów oznaczanych klauzulą RESTREINT UE/EU RESTRICTED[12]. Ponadto Sztab Generalny Rady zobowiązany został do prowadzenia regularnych przeglądów materiałów niejawnych znajdujących się w jego posiadaniu, aby stwierdzić, czy dana klauzula tajności ma nadal zastosowanie. Przeglądy takie prowadzone są raz na pięć lat. *Ustawa* nakazuje kierownikom jednostek organizacyjnych,

[12] Tamże, Załącznik III pkt 15.

w takich samych odstępach czasowych[13], prowadzenie przeglądów materiałów niejawnych w celu ustalenia, czy spełniają ustawowe przesłanki ochrony. Z kolei wytyczne ABW zalecają prowadzenie przeglądów materiałów niejawnych pochodzących z wymiany międzynarodowej raz w roku w celu uniknięcia ich gromadzenia. Materiały niejawne nie mające wartości dla jednostki organizacyjnej podlegają brakowaniu. Etapy brakowania obejmują: otrzymanie pisemnej zgody właściwego organu na brakowanie, powołanie komisji (w skład której powinna wchodzić osoba spoza kancelarii z zastrzeżeniem, że posiada dostęp do informacji niejawnych międzynarodowych do najwyższej klauzuli brakowanych dokumentów), faktyczne brakowanie w sposób uniemożliwiający ich odtworzenie oraz sporządzenie protokołu, którego jeden egzemplarz przesyłany jest do SKW lub ABW, według właściwości. Szczegółowe zasady brakowania powinny być określone w Regulaminie kancelarii tajnej międzynarodowej (punktu kontroli informacji niejawnych międzynarodowych), który zatwierdza kierownik jednostki organizacyjnej. Regulamin stanowi integralną część dokumentacji kancelarii tajnej międzynarodowej i powinien być uzgodniony z ABW. Szef Agencji Bezpieczeństwa Wewnętrznego pełniący funkcję krajowej władzy bezpieczeństwa jest odpowiedzialny za zapewnienie, że informacje niejawne UE powinny być objęte klauzulą tajności nie dłużej niż to konieczne.

W tym miejscu warto zaznaczyć, że art. 6 ust. 2 *Ustawy* odnosi się do obniżenia lub zniesienia klauzuli tajności na dokumentach krajowych. Nie przewiduje się możliwości zniesienia klauzul tajności dokumentom pochodzącym z wymiany z organizacjami międzynarodowymi.

Udzielanie dostępu do informacji niejawnych Unii Europejskiej jest możliwe wyłącznie po tym, jak:

- stwierdzono, że dana osoba spełnia zasadę need-to-know,
- została ona poinformowana o zasadach i procedurach bezpieczeństwa służących ochronie informacji niejawnych międzynarodowych UE i potwierdziła że zapoznała się ze swoimi obowiązkami w zakresie ochrony takich informacji.

Spełnienie powyższych warunków jest wystarczające do uzyskania dostępu do informacji niejawnych oznaczonych klauzulą RESTREINT UE/EU RESTRICTED[14]. Tymczasem wytyczne ABW zalecają stosowanie w tym przypadku art. 21 ust. 4 *Ustawy*, który stanowi, że przed dostępem do odpowiednika informacji niejawnych o klauzuli ZASTRZEŻONE, wymagane jest posiadanie odpowiedniego upoważnienia i przeszkolenia z zakresu ochrony informacji niejawnych. Przyjęcie takiego rozwiązania generuje kolejne trudności w interpretacji. Mianowicie można zadać pytanie: Czy takie upoważnienie jest ważne w innej jednostce organizacyjnej?

[13] *Ustawa o ochronie...*, art. 6 ust. 4.
[14] *Decyzja Rady w sprawie…*, Załącznik I pkt 2.

Jeżeli nie, to nasuwa się kolejne pytanie: Czy osobie niezatrudnionej bądź niewykonującej czynności zleconych można wydać takie upoważnienie? Mimo że z przepisów to nie wynika, odpowiedź na drugie pytanie brzmi tak. Postępowanie z materiałami niejawnymi o klauzuli RESTREINT UE/EU RESTRICTED, w tym przechowywanie i oznaczanie, sprowadzone zostało w całości do krajowego odpowiednika (ZASTRZEŻONE).

W przypadku konieczności dostępu do informacji niejawnych o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, oprócz spełnienia dwóch warunków wymienionych powyżej, wymagane jest posiadanie odpowiedniego poświadczenia bezpieczeństwa lub innego upoważnienia, ze względu na pełnione funkcje zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Takim przepisem jest art. 34 ust. 10 i 11 *Ustawy*, który stanowi, że dostęp do informacji niejawnych bez przeprowadzonego postępowania może mieć Prezydent Rzeczypospolitej Polskiej lub osoba wybrana na ten urząd, Marszałek Sejmu, Marszałek Senatu i Prezes Rady Ministrów. Wobec pozostałych osób wymienionych w ust. 10, które posiadają dostęp do informacji niejawnych krajowych, przeprowadza się poszerzone postępowanie sprawdzające.

Każde państwo członkowskie zobowiązane jest określić, które stanowiska w ich strukturach wymagają dostępu do informacji niejawnych o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej i w związku z tym wymagają uzyskania poświadczenia bezpieczeństwa do dostępu do informacji o odpowiedniej klauzuli tajności[15]. Doświadczenie wskazuje na to, że takie wymagania są określane *ad hoc* przez kierowników jednostek organizacyjnych.

W procesie sprawdzenia, na podstawie *Decyzji*, jednoznacznie wskazuje się kryteria wykorzystywane do oceny, czy daną osobę ze względu na lojalność, wiarygodność i rzetelność, można upoważnić do dostępu do informacji niejawnych UE, a także procedury sprawdzające i administracyjne[16]. Warto zauważyć, że jest to podejście różniące się, od tego które obowiązuje w Polsce. *Ustawa* definiuje *rękojmię zachowania tajemnicy* jako zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego[17]. Inaczej mówiąc postępowanie sprawdzające ma na celu ustalenie czy osoba sprawdzana daje rękojmię zachowania tajemnicy. W *Ustawie* nie ma mowy wprost (*explicite)* o lojalności, wiarygodności, czy rzetelności. Organem prowadzącym postępowanie jest krajowa władza bezpieczeństwa. Celem sprawdzenia danej osoby jest określenie czy jest ona lojalna, wiarygodna i rzetelna. Na podstawie wyników postępowania sprawdzają-

[15] Tamże, Załącznik I pkt 3.
[16] Tamże, Załącznik I pkt 7.
[17] *Ustawa o ochronie…*, art. 2 pkt 2.

cego właściwy organ dokonuje ogólnej oceny. Główne kryteria obejmują ustalenie, czy osoba ta:

- popełniła lub usiłowała popełnić akt szpiegostwa, terroryzmu, sabotażu, zdrady lub podżegania, współdziałała z inną osobą w celu popełnienia takiego aktu, pomagała innej osobie w jego popełnieniu lub nakłaniała inne osoby do popełnienia takiego aktu;
- współdziała lub współdziałała ze szpiegami, terrorystami, sabotażystami lub osobami, co do których istnieje uzasadnione podejrzenie, że nimi są lub z przedstawicielami organizacji lub obcych państw, w tym obcych służb wywiadowczych, które mogą stanowić zagrożenie dla bezpieczeństwa Unii lub państw członkowskich, chyba że udzielono zezwolenia na takie współdziałanie w ramach obowiązków służbowych;
- jest lub była członkiem organizacji, która za pomocą aktów przemocy, działalności wywrotowej lub innych nielegalnych środków dąży m. in. do obalenia rządu państwa członkowskiego, zmiany porządku konstytucyjnego państwa członkowskiego lub zmiany formy lub polityki jego rządu;
- jest lub była stronnikiem jakiejkolwiek organizacji opisanej powyżej lub blisko współdziała z członkami takich organizacji,
- świadomie zataiła, fałszywie przestawiła lub sfałszowała istotne informacje, szczególnie informacje związane z bezpieczeństwem, lub świadomie skłamała przy wypełnianiu ankiety bezpieczeństwa osobowego lub podczas rozmowy przeprowadzonej w ramach postępowania sprawdzającego;
- została skazana za popełnienie przestępstwa lub przestępstw;
- kiedykolwiek była uzależniona od alkoholu, zażywała nielegalne środki odurzające lub nadużywała legalnych środków odurzających;
- zachowuje się lub zachowywała się w sposób mogący stwarzać ryzyko szantażu lub presji;
- w czynach lub słowach wykazała się nieuczciwością, nielojalnością, brakiem rzetelności lub wiarygodności;
- poważnie lub wielokrotnie naruszyła przepisy dotyczące bezpieczeństwa lub usiłowała dokonać albo dokonała czynności, do których nie była uprawniona, w systemach teleinformatycznych;
- może podlegać presji (np. poprzez posiadanie jednego lub więcej obywatelstw państw niebędących członkiem UE lub presji krewnych lub bliskich współpracowników, którzy mogą być podatni na wpływy obcych służb wywiadowczych, grup terrorystycznych lub innych wywrotowych organizacji lub osób mogących zagrażać interesom bezpieczeństwa Unii lub państw członkowskich).

W odpowiednich przypadkach oraz zgodnie z krajowymi przepisami ustawowymi i wykonawczymi podczas postępowania sprawdzającego za istotną można uznać także sytuację finansową i zdrowotną danej osoby.

Analogicznie za istotne można także uznać zachowanie i sytuację współmałżonka danej osoby, jej partnera życiowego lub członka bliskiej rodziny.

Zakres postępowania sprawdzającego prowadzonego przez ABW i SKW określa art. 24 i 25 *Ustawy*. Można zauważyć, że *Decyzja* dość szczegółowo określa zakres sprawdzeń. Tymczasem przytoczone przepisy *Ustawy* traktują ustalenia dość ogólnie, polegając na subiektywnej ocenie organu prowadzącego postępowanie. Warto przytoczyć treść art. 24 ust. 4 *Ustawy*, który stanowi, że interes ochrony informacji niejawnych ma pierwszeństwo przed innymi prawnie chronionymi interesami. Zaznaczyć należy także fakt, że zbieranie danych o osobach trzecich (w szczególności współmałżonek, partner życiowy, członek bliskiej rodziny) jest ograniczone do okoliczności określonych w art. 24 ust. 2. Przepis ten może wywoływać trudności interpretacyjne w szczególności w odniesieniu do pkt 4. Ponadto *Ustawa* nie przewiduje uwzględniania przy ocenie dawania rękojmi zachowania tajemnicy podatności i wywierania presji na współpracowników osoby sprawdzanej. Inną nieścisłością jest zażywanie nielegalnych środków odurzających, co według *Decyzji*, może stanowić przyczynę odmowy wydania poświadczenia bezpieczeństwa, tymczasem w przepisach krajowych musi być stwierdzone uzależnienie od alkoholu, środków odurzających lub substancji psychotropowych.

W postępowaniu sprawdzającym prowadzonym na podstawie zapisów *Decyzji* nie ma podziału na postępowania zwykłe i poszerzone. Z tego tytułu, zgodnie z art. 22 ust. 1 pkt lit. d *Ustawy* przed dostępem do informacji niejawnych międzynarodowych, niezależnie od klauzuli tajności, prowadzone jest zawsze postępowanie poszerzone.

Zgodnie z *Decyzją w* przypadku prowadzenia pierwszego postępowania sprawdzającego do klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET obejmuje ono okres ostatnich 5 lat lub okres od 18 roku życia do okresu ubiegania sią o dostęp do informacji w zależności, który jest krótszy, w tym wymagane jest:

- wypełnienie krajowej ankiety bezpieczeństwa do odpowiedniego poziomu niejawności, do którego dostęp może być konieczny danej osobie. Wypełniona ankieta jest przekazywana właściwemu organowi bezpieczeństwa. W odniesieniu do przepisów narodowych, bez względu na to czy wymagany jest dostęp do CONFIDENTIEL UE/EU CONFIDENTIAL czy SECRET UE/EU SECRET, należy wypełnić wszystkie części ankiety, za wyjątkiem VII (wskazanie osób polecających);
- sprawdzenie tożsamości/obywatelstwa/narodowości, które polega na potwierdzeniu daty i miejsca urodzenia danej osoby i sprawdza się jej tożsamość. Ustala się przeszłe i obecne obywatelstwo lub narodowość, obejmuje to ocenę podatności na presję, wywieraną przez osoby z zagranicy, na przykład w związku z poprzednim miejscem pobytu lub przeszłymi powiązaniami;

- sprawdzenie krajowych rejestrów bezpieczeństwa i centralnych rejestrów karnych, o ile te istnieją, lub innych rejestrów rządowych i policyjnych. Sprawdza się rejestry organów ścigania sprawujących jurysdykcję w miejscach, w których dana osoba przebywała lub była zatrudniona. Krajowe przepisy nakazują sprawdzenie w kartotekach niedostępnych powszechnie oraz w ABW, SKW. Niestety nie istnieje definicja kartotek niedostępnych powszechnie w żadnym dokumencie normatywnym. Dane mogą być pozyskiwane z baz krajowego rejestru karnego, systemów policyjnych (KSIP, KCIK), kartotek innych służb (takich jak ABW, SKW, SWW, ŻW), a także zapytań kierowanych do właściwych terytorialnie jednostek Policji.

Warto zaznaczyć, że czynności prowadzone w postępowaniu do klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET są tożsame. Co więcej, dopuszcza się przeprowadzenie w wyżej wymienionych postępowaniach czynności prowadzonych w postępowaniu do klauzuli TRES SECRET UE/EU TOP SECRET. W narodowych procedurach postępowanie do klauzuli POUFNE nie obejmuje sprawdzenia dochodów i poziomu życia, informacji o chorobie psychicznej lub innych zakłóceniach czynności psychicznych, a także uzależnienia od alkoholu, środków odurzających i substancji psychotropowych. Dla postępowania do klauzuli TAJNE nie prowadzi się rozmów z osobami polecającymi.

Wydanie pierwszego poświadczenia bezpieczeństwa w przypadku dostępu do informacji niejawnych oznaczonych klauzula TRES SECRET UE/EU TOP SECRET poprzedzone jest sprawdzeniem obejmującym okres ostatnich 10 lat lub okres od 18 roku życia do okresu ubiegania się o dostęp do informacji w zależności, który jest krótszy. Jeżeli prowadzi się rozmowy z osobami polecającymi, okres sprawdzeń obejmuje 7 lat. Postępowanie obejmuje:

- status finansowy – poszukuje się informacji dotyczących statusu finansowego danej osoby, aby ocenić stopień jej podatności na presję osób z kraju lub z zagranicy z powodu poważnych trudności finansowych lub aby ujawnić wszelkie przychody z nieznanych źródeł;
- wykształcenie – poszukuje się informacji służących weryfikacji wykształcenia danej osoby w szkołach, szkołach wyższych lub placówkach edukacyjnych, do których uczęszczała ona od ukończenia 18 roku życia lub w okresie, który organ prowadzący postępowanie uzna za odpowiedni;
- zatrudnienie – poszukuje się informacji dotyczących obecnego i poprzedniego zatrudnienia, przy wykorzystaniu takich źródeł jak historia zatrudnienia, sprawozdania dotyczące wyników lub wydajności pracy oraz opinie pracodawców lub przełożonych,
- służba wojskowa – w stosownych przypadkach weryfikowany jest stosunek danej osoby do służby wojskowej oraz powód zwolnienia;

- rozmowy – pod warunkiem, że przepisy krajowe przewidują i dopuszczają taką możliwość, przeprowadza się z daną osobą rozmowę lub rozmowy. Rozmowy przeprowadza się również z innymi osobami, które są w stanie przedstawić obiektywną ocenę dotyczącą pochodzenia, działalności, lojalności, wiarygodności i rzetelności osoby sprawdzanej. W przypadku gdy krajowa praktyka przewiduje przedstawienie referencji przez osobę sprawdzaną, przeprowadza się rozmowę z osobami, które dostarczyły tych referencji, chyba że istnieją uzasadnione powody, żeby tego nie czynić.

Ustawa daje organowi prowadzącemu postępowanie narzędzie, umożliwiające weryfikację danych podanych przez osobę sprawdzaną w ankiecie, w postaci wywiadu środowiskowego. Wywiad prowadzony jest na podstawie *Ustawy* z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego* (Dz. U. z 2017 r., poz. 1904 j.t.) art. 214. Powyższe ma delegację do pkt 12 *Decyzji*, który dopuszcza w postępowaniu możliwość prowadzenia dodatkowych wyjaśnień w celu rozwinięcia wszelkich dostępnych istotnych informacji dotyczących danej osoby oraz w celu potwierdzenia lub wykazania fałszywości informacji działających na niekorzyść osoby sprawdzanej.

Przepisy unijne definiują postępowanie w przypadku prowadzenia kolejnego postępowania sprawdzającego, po wydaniu pierwszego poświadczenia bezpieczeństwa oraz pod warunkiem, że w zatrudnieniu danej osoby w administracji krajowej nie wystąpiły przerwy, a dostęp do informacji niejawnych UE w dalszym ciągu jest niezbędny. Przedłużenie ważności poświadczenia bezpieczeństwa tej osoby rozpatrywane jest w odstępach czasu nieprzekraczających pięciu lat dla poświadczenia bezpieczeństwa do klauzuli TRES SECRET UE/EU TOP SECRET oraz dziesięciu lat w przypadku poświadczeń do klauzuli, licząc od daty powiadomienia o wyniku ostatniego postępowania sprawdzającego, na podstawie którego zostały wydane te poświadczenia. Wszelkie postępowania sprawdzające dotyczące przedłużenia ważności poświadczenia bezpieczeństwa obejmują okres od poprzedniego postępowania. Przepisy krajowe nie uszczegółowiają takiego postępowania. *Ustawa* dopuszcza możliwość zapoznania się organu prowadzącego postępowanie z materiałami postępowania sprawdzającego prowadzonego wobec tej samej osoby[18].

Przed przedłużeniem ważności wykonuje się czynności analogiczne jak w przypadku postępowań prowadzonych do klauzul tajności odpowiednio CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET i TRES SECRET UE/EU TOP SECRET. Nie określono natomiast terminu składania wniosku o przedłużenie poświadczenia bezpieczeństwa. Zastrzeżono tylko, że muszą one wpłynąć z odpowiednim wyprzedzeniem, z uwzględnieniem czasu wymaganego do przeprowadzenia postępowania

[18] *Ustawa o ochronie…*, art. 72 ust. 1.

sprawdzającego przez właściwy organ[19]. Krajowe przepisy jasno regulują termin składania wniosku, który wynosi 6 miesięcy przed upływem ważności poświadczenia bezpieczeństwa[20]. Kolejnym udogodnieniem w przepisach Unii jest możliwość przedłużenia ważności obowiązującego poświadczenia bezpieczeństwa o okres nie przekraczający 12 miesięcy, jeżeli wniosek do organu wpłynął wraz z ankietą zanim poświadczenie bezpieczeństwa utraciło ważność, a niezbędne postępowanie nie zostało zakończone. Jeżeli po upływie tego okresu nadal nie zakończono postępowania sprawdzającego, danej osobie przydziela się obowiązki, które nie wymagają posiadania poświadczenia bezpieczeństwa. Krajowe przepisy nie przewidują takiego postępowania. Dopuszczenie do informacji niejawnych organizacji międzynarodowych jest ściśle związane ze stanowiskiem. Praktykuje się wszczynanie postępowań wobec osób planowanych do wyznaczenia na takie stanowiska.

Unijny system ochrony przewiduje możliwość stosowania wyjątkowych okoliczności dostępu do informacji niejawnych UE. Jeżeli interes Unii tego wymaga właściwy organ może uprawnić urzędników krajowych do dostępu do informacji niejawnych UE pod warunkiem, że toczy się wobec nich postępowanie sprawdzające oraz posiadają oni krajowe poświadczenie bezpieczeństwa. Poziom dostępu określony jest jako odpowiednik krajowej klauzuli tajności[21]. W Polsce art. 32 ust. 4 *Ustawy* daje możliwość właściwemu organowi (ABW lub SKW) wydania poświadczenia bezpieczeństwa do informacji niejawnych międzynarodowych osobie, która posiada poświadczenie bezpieczeństwa krajowe. Zastrzega się, że czas dostępu do informacji niejawnych międzynarodowych nie może być dłuższy niż ważność poświadczenia krajowego, a także poziom dostępu musi stanowić odpowiednik narodowy. W tym wypadku prowadzone jest postępowanie sprawdzające, ale wypełnienie ankiety nie jest wymagane.

Kolejnym przypadkiem okoliczności stanowiącej wyjątkowy sposób dostępu do informacji niejawnych UE jest przepis określony w pkt 34 zał. I *Decyzji*, który stanowi, że istnieje możliwość tymczasowego wyznaczenia osoby na stanowisko, na którym wymagane posiadanie poświadczenia bezpieczeństwa o jeden poziom wyższy niż aktualne uprawnienia tej osoby, ale muszą być spełnione poniższe warunki:

- bezwzględna potrzeba dostępu do informacji niejawnych UE o wyższej klauzuli tajności jest uzasadniona pisemnie przez przełożonego,
- dostęp do informacji niejawnych UE jest ograniczony do konkretnych informacji niezbędnych do pracy na tym stanowisku,
- osoba posiada poświadczenie bezpieczeństwa do informacji niejawnych UE (co oznacza, że przepisu tego nie można zastosować dla in-

[19] *Decyzja Rady w sprawie...*, Załącznik I pkt 15.
[20] *Ustawa o ochronie...*, art. 32 ust. 1.
[21] *Decyzja Rady w sprawie…*, Załącznik I pkt 32.

formacji niejawnych oznaczonych klauzulą CONFIDENTIEL UE/EU CONFIDENTIAL),

- podjęto czynności w celu uzyskania upoważnienia do informacji niejawnych na poziomie wymaganym na tym stanowisku (de facto wszczęto wobec niej postępowanie sprawdzające),
- wykonano sprawdzenia, które potwierdziły, że dana osoba nie naruszała poważnie ani wielokrotnie przepisów dotyczących bezpieczeństwa (czyli właściwy organ przeprowadził część sprawdzeń w ramach postępowania),
- objęcie tego stanowiska przez daną osobę zatwierdził właściwy organ (krajowa władza bezpieczeństwa),
- dokumentacja dotycząca przyznania dostępu w drodze wyjątku wraz z opisem informacji, do których zatwierdzono dostęp, przechowywana jest w odpowiedniej kancelarii tajnej.

Przepisy krajowe dopuszczają możliwość wyznaczenia osoby na stanowisko związane z dostępem do informacji niejawnych, nawet gdy osoba nie posiada poświadczenia bezpieczeństwa pod warunkiem, że wszczęto wobec niej postępowanie sprawdzające, natomiast po wyznaczeniu ogranicza się jej dostęp do informacji niejawnych zgodnie z posiadanym upoważnieniem lub poświadczeniem do czasu wydania jej właściwego poświadczenia bezpieczeństwa. Należy zaznaczyć, że procedura ta nie stanowi zasady i jest prowadzona w drodze wyjątku, zgodnie z obowiązującymi przepisami.

Zgodnie z pkt 35 zał. I *Decyzji* z powyższą procedurę można wykorzystać w przypadku umożliwienia jednorazowego dostępu do informacji niejawnych UE o jeden poziom wyższej niż klauzula, do której ta osoba ma dostęp po dokonaniu odpowiedniego sprawdzenia. Z procedury tej nie można korzystać w sposób wielokrotny, co wskazuje, że tę formę dostępu można wykorzystać jednokrotnie. Ustawa o ochronie informacji niejawnych nie przewiduje możliwości jednorazowego dostępu do informacji międzynarodowych, chociaż istnieją wyjątki w zakresie dostępu do informacji krajowych[22].

Ostatni wyjątek stanowią szczególne okoliczności, takie jak misje prowadzone we wrogim środowisku lub w okresie rosnącego napięcia międzynarodowego, i gdy wymagają tego środki nadzwyczajne, w szczególności w celu ratowania życia ludzkiego, państwa członkowskie i Sekretarz Generalny mogą udzielić, w miarę możliwości na piśmie, dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET osobom, które nie posiadają wymaganego poświadczenia bezpieczeństwa, pod warunkiem że takie zezwolenie jest absolutnie niezbędne i nie ma żadnych uzasadnionych

[22] *Ustawa o ochronie…*, art. 34 ust. 5 i 9.

wątpliwości co do lojalności, wiarygodności i rzetelności danej osoby. Zachowuje się dokumentację takiego zezwolenia zawierającą opis informacji, do których dostęp zatwierdzono. Taki dostęp w sytuacjach nadzwyczajnych do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET przysługuje tylko obywatelom Unii, których upoważniono do dostępu do informacji niejawnych o klauzuli krajowej odpowiadającej klauzuli tajności TRÈS SECRET UE/EU TOP SECRET albo do informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET, czyli odpowiednio TAJNE lub ŚCIŚLE TAJNE. Krajowy ustawodawca takiej procedury nie przewiduje.

W *Decyzji* zastrzeżono, że jeżeli krajowe przepisy ustawowe i wykonawcze państwa przewidują bardziej rygorystyczne zasady dotyczące tymczasowych upoważnień, tymczasowego pełnienia obowiązków, jednorazowego dostępu do informacji niejawnych lub dostępu do takich informacji w sytuacjach nadzwyczajnych, wyżej wymienione procedury mogą być stosowane wyłącznie w ramach ograniczeń ustalonych w odpowiednich przepisach ustawowych i wykonawczych.

Dostęp do odpowiedniego poziomu informacji niejawnych wymagany jest także od kurierów, strażników, konwojentów. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie wtargnięciu osoby nieupoważnionej, w sposób niezauważony lub z użyciem siły, powstrzymanie od podjęcia nieuprawnionych działań, udaremnienie ich i wykrycie oraz umożliwienie podziału pracowników pod względem dostępu do informacji niejawnych UE zgodnie z zasadą ograniczonego dostępu. Środkami bezpieczeństwa fizycznego obejmuje się wszystkie obiekty, budynki, biura, pomieszczenia i inne strefy, w których są wykorzystywane lub przechowywane informacje niejawne UE, w tym strefy, w których znajdują się systemy teleinformatyczne. Środki bezpieczeństwa fizycznego dobiera się na podstawie oceny zagrożenia przeprowadzonej przez właściwe organy. Stosuje się proces zarządzania ryzykiem służący ochronie informacji niejawnych, aby zapewnić poziom ochrony fizycznej proporcjonalny do szacowanego ryzyka. Proces zarządzania ryzykiem uwzględnia wszelkie istotne czynniki, a w szczególności:

- klauzulę tajności informacji niejawnych,
- postać i ilość dokumentów zawierających informacje niejawne, z uwzględnieniem faktu, że duża ich ilość lub ich kompilacja mogą wymagać zastosowania bardziej rygorystycznych środków ochrony,
- otoczenie i strukturę budynków lub stref, w których znajdują się informacje niejawne,
- szacowane zagrożenie ze strony służb wywiadowczych, których celem jest Unia lub państwa członkowskie, oraz zagrożenie sabotażem, terroryzmem, działalnością wywrotową lub inną działalnością przestępczą.

Zarządzanie ryzykiem jest jednym z ustawowych obowiązków pełnomocnika kierownika jednostki organizacyjnej do spraw ochrony informacji niejawnych[23]. Proces ten rozpoczyna określenie poziomu zagrożeń, następnie na tej podstawie dobiera się adekwatne środki bezpieczeństwa fizycznego, w końcu przeprowadza się szacowanie ryzyka dla niejawnych systemów teleinformatycznych. W procesie tym należy na bieżąco uwzględniać pojawiające się zagrożenia i stosować odpowiednie środki bezpieczeństwa fizycznego. W tym zakresie obowiązujące przepisy Unii są zbieżne z krajowymi. Decyzja dopuszcza stosowanie środków bezpieczeństwa fizycznego lub ich kombinacji takich jak: ogrodzenie, system alarmowy, kontrola dostępu, pracownicy ochrony, telewizyjny system nadzoru, oświetlenie ochronne i inne. Kontrowersyjny jest pkt 5 zał. II *Decyzji*, który dopuszcza możliwość przeszukania osób wchodzących i wychodzących. W polskim prawie przeszukanie jest czynnością procesową[24], którą zastępuje się, w zależności od okoliczności, kontrolą osobistą, przeglądem zawartości bagażu, czy sprawdzeniem ładunku.

Instalowany sprzęt służący do ochrony fizycznej informacji niejawnych musi spełniać wymagania określone we właściwych normach.

Przepisy Unijne ustanawiają następujące rodzaje stref chronionych fizycznie:

- strefy administracyjne,
- strefy bezpieczeństwa
- strefy technicznie zabezpieczone.

W strefie administracyjnej:

- wyraźnie określa się granicę umożliwiającą kontrolę osób i, jeżeli to możliwe, pojazdów,
- dostęp bez osób uprawnionych (eskorty) umożliwia się tylko osobom, które są odpowiednio upoważnione przez właściwy organ,
- wszystkim innym osobom przez cały czas towarzyszą osoby uprawnione (eskorta) lub poddaje się je równorzędnej kontroli.

W strefie bezpieczeństwa:

- wyraźnie określa się i chroni granicę, na której wszelkie wejścia i wyjścia kontrolowane są za pomocą przepustki lub systemu rozpoznawania osób,
- dostęp bez osoby uprawnionej (eskorty) umożliwia się tylko osobom odpowiednio sprawdzonym i wyraźnie upoważnionym do wejścia do danej strefy zgodnie z zasadą ograniczonego dostępu,
- wszystkim innym osobom przez cały czas towarzyszą osoby uprawnione (eskorta) lub poddaje się je równorzędnej kontroli.

[23] *Ustawa o ochronie…*, art. 15 ust. 1 pkt 3.

[24] *Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego*, Dz. U. z 2017 r. poz. 1904 j.t., art. 219.

Strefy technicznie zabezpieczone są to strefy bezpieczeństwa zabezpieczone przed podsłuchem, poza tym:

- wyposaża się je w system alarmowy, są zamknięte na klucz, gdy nikt w nich nie przebywa, i chronione, gdy ktoś w nich przebywa,
- wszystkie osoby wchodzące do takich stref lub materiały tam wnoszone podlegają kontroli,
- podlegają regularnym inspekcjom fizycznym lub technicznym zgodnie z wymogami właściwego organu bezpieczeństwa. Inspekcje takie przeprowadza się także po każdorazowym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście miało miejsce,
- nie mogą tam się znajdować niezatwierdzone linie komunikacyjne, niezatwierdzone telefony, inne niezatwierdzone urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny.

Jeżeli wejście do strefy bezpieczeństwa jest w praktyce równoznaczne z bezpośrednim dostępem do informacji niejawnych znajdujących się w tej strefie to:

- wyraźnie wskazuje się najwyższą klauzulę tajności, którą przyznano informacjom zwykle przechowywanym w tej strefie,
- wszystkie osoby wchodzące do tej strefy muszą posiadać specjalne upoważnienie do wejścia do tej strefy, przez cały czas towarzyszyć im muszą osoby uprawnione (eskorta) i muszą być odpowiednio sprawdzone, chyba że podjęte zostały kroki służące zapewnieniu, aby nie był możliwy dostęp do informacji niejawnych.

Strefy bezpieczeństwa oraz strefy technicznie zabezpieczone mogą być tworzone tymczasowo na terenie stref administracyjnych w celu zorganizowania niejawnego spotkania (posiedzenia, odprawy) lub w jakimkolwiek innym podobnym celu.

Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683) nakazuje podział na: strefy ochronne III, strefy ochronne II, strefy ochronne I i strefy specjalne. Znaczenie stref ochronnych według powyższego sprowadza się do możliwości zapoznania się z materiałami tam przetwarzanymi. Samo wejście do strefy ochronnej I umożliwia bezpośredni dostęp do materiałów niejawnych o klauzuli POUFNE lub wyższej. W strefie ochronnej II dostęp do tych materiałów jest możliwy, ale nie bezpośrednio. Natomiast strefa ochronna III jest strefą, w obrębie której jest możliwa kontrola osób i pojazdów. Wprowadzono także specjalną strefę ochronną chronioną przed podsłuchem. Granice stref II i I muszą być wyraźnie określone i zabezpieczone, system kontroli dostępu zezwala na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy oraz zapewniony jest nadzór nad osobami innymi, niż wymie-

nione powyżej, zabezpieczając jednocześnie materiały niejawne przed możliwością dostępu do nich.

Materiały o klauzuli RESTREINT UE/EU RESTRICTED mogą być przetwarzane w strefie bezpieczeństwa lub w strefie administracyjnej pod warunkiem, że są chronione przed dostępem osób nieupoważnionych oraz poza tymi strefami w czasie transportu. Dokumenty oznaczone klauzulą RESTREINT UE/EU RESTRICTED przechowywane są w odpowiednim do tego celu zamkniętym meblu biurowym w strefie administracyjnej lub strefie bezpieczeństwa. Mogą być one tymczasowo przechowywane poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwy organ bezpieczeństwa. Przepisy krajowe są bardziej restrykcyjne i nakazują przechowywanie materiałów o klauzuli ZASTRZEŻONE w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu w szafie metalowej, pomieszczeniu wzmocnionym lub zamkniętym na klucz meblu biurowym.

Materiały niejawne o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET przetwarza się podobnie jak RESTREINT UE/EU RESTRICTED z tym, że muszą być pod ciągłą kontrolą osoby upoważnionej, a w przypadku dokumentów papierowych – za wiedzą kancelarii tajnej. Materiały te powinny być przechowywane w strefie bezpieczeństwa – w zabezpieczonej szafie lub we wzmocnionym pomieszczeniu. W kraju, przetwarzanie materiałów niejawnych POUFNE i TAJNE lub ich międzynarodowego odpowiednika, odbywa się wyłącznie w strefie ochronnej, co więcej materiały oznaczone klauzulą TAJNE w strefie ochronnej I lub II.

Przetwarzanie materiałów TRÈS SECRET UE/EU TOP SECRET odbywa się w strefie bezpieczeństwa, a przechowuje na jeden z niżej wymienionych sposobów:

- w szafie stalowej w pomieszczeniu znajdującym się pod ciągłą kontrolą odpowiednio sprawdzonych pracowników ochrony lub służby dyżurnej lub w pomieszczeniu zainstalowano system alarmowy spełniający wymagania odpowiedniej normy,
- we wzmocnionym pomieszczeniu objętym systemem alarmowym spełniającym wymagania odpowiedniej normy.

Polskie przepisy nakazują przechowywanie w szafie stalowej w pomieszczeniu znajdującym się w I lub w II oraz wymagany jest telewizyjny system nadzoru obsługiwany przez personel posiadający odpowiednie poświadczenia bezpieczeństwa lub system alarmowy obsługiwany przez personel z wyżej wymienionymi uprawnieniami.

W sferze cywilnej i wojskowej opracowywane są plany ochrony, zawierające postępowanie w przypadkach awaryjnych. Posiadanie planów awaryjnych uwzględnia potrzebę ochrony informacji niejawnych UE podczas

sytuacji nadzwyczajnych, a także planów ciągłości działania, w których zamieszcza się środki zapobiegawcze i naprawcze służące zminimalizowaniu skutków niedopatrzeń lub incydentów związanych z wykorzystywaniem informacji niejawnych oraz ich przechowywaniem. W planach tych, poza zasadami postępowania wymienionymi powyżej, określa się klauzule tajności informacji niejawnych przetwarzanych w danej strefie, sposób sprawowania nadzoru nad osobami przebywającymi w danej strefie, procedury zarządzania kluczami, kodami dostępu do pomieszczeń i szaf, w których przetwarzane są informacje niejawne.

W odniesieniu do przepisów unijnych sposób organizacji ochrony i miejsc przetwarzania materiałów niejawnych jest dostępny dla osób zatrudnionych. Czyli zastosowano zasadę prewencyjnego poinformowania, z czym może się zapoznać osoba wchodząca do strefy. Natomiast według procedur krajowych, już sama organizacja systemu ochrony daje podstawę do objęcia jej klauzulą niejawności.

Wnioski

Ustawa wraz z aktami wykonawczymi stanowi wypadkową systemu ochrony informacji niejawnych RP i obowiązujących porozumień zawartych z organizacjami międzynarodowymi, takimi jak NATO czy UE. Niemniej jednak krajowe przepisy do końca nie pozwalają na jednoznaczną interpretację, i tym samym nie dają pewności osobom odpowiedzialnym, czy przyjęte rozwiązania zapewniają wymaganą ochronę informacji niejawnych. Przykładem może być przyznawanie dostępu do materiałów oznaczonych klauzulą RESTREINT UE/EU RESTRICTED, czy postępowanie z materiałami pochodzącymi z UE. Część rozwiązań przyjętych w Unii Europejskiej do stosowania w kraju nie zostało dopuszczonych, np. możliwość znoszenia lub obniżania klauzul tajności, dostęp do informacji niejawnych w wyjątkowych okolicznościach, czy wprowadzanie informacji do krajowego systemu ochrony.

Osobno należy rozpatrywać tryb prowadzenia postępowań. Przepisy unijne określają, że do klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL należy stosować okres sprawdzeń nie przekraczający 5 lat. Natomiast w przypadku TRES SECRET UE/UE TOP SECRET okres ten nie może być dłuższy niż 10 lat, a w przypadku prowadzenia rozmów z osobami polecającymi nie może on przekroczyć 7 lat. Wypełnienie obowiązującej w kraju ankiety bezpieczeństwa osobowego wymaga podania wszystkich znanych danych, niezależnie od okresu w jakim zdarzenie miało miejsce. Z drugiej strony zakres prowadzonych czynności jest bardziej restrykcyjny, jeżeli chodzi o tryb określony w Unii, w tym udowodnienie lojalności, wiarygodności i rzetelności. Z kolei w kraju wprowadzono definicję *rękojmi za-*

chowania tajemnicy, która daje pewną niezależność w ocenie materiału pełnomocnikowi do spraw ochrony informacji niejawnych lub służbom i instytucjom upoważnionym do prowadzenia postępowań sprawdzających[25].

W wyniku analizy można stwierdzić, że przepisy unijne dotyczące zabezpieczenia fizycznego informacji niejawnych sprowadzają się do określenia dwóch stref bezpieczeństwa i właściwego ich oznaczenia. W sferze krajowej wprowadzono trzy rodzaje stref oraz podział na klasy urządzeń przeznaczonych do przechowywania dokumentów niejawnych. Dodatkowo, biorąc pod uwagę konieczność spełnienia wymagań określonych w załączniku nr 2 do Rozporządzenia Rady Ministrów w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych[26], samo zaplanowanie ochrony fizycznej informacji niejawnych stanowi swojego rodzaju wyzwanie.

Przytoczone dokumenty normatywne obowiązujące w UE stanowią podstawowe zasady i minimalne normy bezpieczeństwa służące ochronie informacji niejawnych UE. Wdrożenie tych przepisów *explicite* znacznie ułatwiłoby dostęp do informacji niejawnych UE. Harmonizacja (ujednolicenie, unifikacja) prawa UE i polskiego w tym zakresie jest bardzo trudna ze względu na to, że stanowienie przepisów UE to proces skomplikowany i oparty na konsensusie wszystkich krajów członkowskich, dlatego pogodzenie odmiennych standardów wymagało wprowadzenia zasady uznaniowości stron. Każda ze stron uznaje za skuteczne przyjęte rozwiązania drugiej strony, np. szeroko rozumiane bezpieczeństwo osobowe lub brak regulacji w przepisach UE trybu cofnięcia uprawnień do dostępu do informacji niejawnych, czy procedury odwoławczej.

Niemniej jednak wskazana jest pewna racjonalizacja *Ustawy*, która pełna jest niejednoznaczności i dowolności interpretacyjnej (przykładem może być wspomniany tu art. 5 ust. 5, czy dostęp do akt postępowania kontrolnego).

Bibliografia

1. *Decyzja Rady z dnia 23 września w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE*, 2013/488/UE.

2. *Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego*, Dz. U. z 2017 r. poz. 1904 j.t.

[25] *Ustawa o ochronie…*, art. 23.

[26] Metodyka doboru środków bezpieczeństwa fizycznego.

3. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, Dz. U. z 2018 r., poz. 412 j.t.

PERSONAL SAFETY AND PHYSICAL PROTECTION OF CONFIDENTIAL INFORMATION IN THE EU

The author analyses the mode of access to classified information in the EU. The paper contains a comparison of solutions regarding classified information protection systems in the EU and Poland, showing that the regulations observed in Poland are unclear. The author describes in detail the principles of verification proceedings for personnel security clearances in the EU, as well as application of special exceptions regarding access to classified information. There is also a comparison of solutions required in the EU related to the use of physical security measures with the requirements that exist in Poland.

Keywords: European Union, personnel security, classified information protection, personnel security clearance