Centrum Ekspertyzy Lokalnej

Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego

OPINIE I KOMENTARZE FRDL

OPINIA nr 19/2022

STATUT PRAWNY PEŁNOMOCNIKA OCHRONY INFORMACJI NIEJAWNYCH W JST

dr Mariusz Paradowski

Wstęp

Od kilku lat w strukturach jednostek samorządu terytorialnego istnieje tendencja do zatrudniania wielu najrozmaitszych specjalistów na stanowiskach doradców, asystentów lub pełnomocników organów wykonawczych. Zdaniem L. Jaworskiego: „mamy tu pełnomocników do spraw: rodziny, systemu zarządzania jakością, rozwoju kultury fizycznej, polityki senioralnej, jakości powietrza, komunikacji rowerowej, interwencji lokatorskich, strategii rozwoju, centrum nauki, równego traktowania, rewitalizacji miasta, inwestycji, inwestorów kluczowych i zatrudnienia, finansów, budżetu i przedsiębiorczości czy estetyki miasta"1. W perspektywie kreowania nowych stanowisk pracy wydaje się cennym spostrzeżeniem, iż włodarze organów samorządowych niechętnie pamiętają o konieczności obsadzania niektórych stanowisk pracy, w szczególności zatrudniania pełnomocników powołanych ex lege do działania prawnego w jednostkach samorządu terytorialnego. O ile obecność wymienionych pełnomocników w strukturze zatrudnienia jednostek samorządowych jest fakultatywny i uzależniony do polityki kadrowej pracodawcy, o tyle istnienie innych podmiotów, głównie pełnomocnika ds. ochrony informacji niejawnych lub inspektora ochrony danych osobowych jest już obligatoryjne. Taki pogląd wynika nie tylko z norm ustawowych, ale także ze stanowiska doktryny prawniczej. J. Depo, S. Mazur zwrócili uwagę, iż: „pełnomocnikiem ochrony do spraw ochrony informacji niejawnych (dalej: pełnomocnik ochrony) jest osoba specjalnie zatrudniona, bezpośrednio podległa kierownikowi jednostki organizacyjnej i w pełni niezależna od pozostałych pracowników jednostki. Utworzenie stanowiska pełnomocnika ochrony jest obligatoryjne w każdej jednostce organizacyjnej, w której są przetwarzane informacje niejawne"

[1] L. Jaworski, Samorządowa moda na pełnomocników budzi kontrowersje [w:] Dziennik Gazeta Prawna, Warszawa 2019, wyd. z dnia 2 stycznia 2019 r. (https://prawo.gazetaprawna.pl/artykuly/1389978,pelnomocnik-w-urzedzie-miasta-praktyka-i-prawo-nieklarowne.html)
[2] t. j. Dz. U. z 2021 r. poz. 735, 1491, 2052.

Nie ulega wątpliwości, że problematyka dotycząca statusu prawnego pełnomocnika ds. ochrony informacji niejasnych w jednostkach samorządu terytorialnego należy do ważnych zagadnień normatywnych dość często niedostrzeganych w aparacie administracyjnym. Podstawę prawną stanowi tutaj ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych1. Trudno wyobrazić sobie sprawnie funkcjonującą samorządową jednostkę organizacyjną, która nie posiadałaby w swej strukturze pracownika wyposażonego w kompetencje prawne do przetwarzania informacji niejawnych[3]. Z uwagi na zagrożenia związane z bezpieczeństwem jednostki samorządu terytorialnego oraz obiegiem tajnych dokumentów, niezbędne jest wyodrębnienie stanowisk pracy lub pionu organizacyjnego mającego na celu ochronę informacji niejawnych.

2.Kandydat na stanowisko pełnomocnika ochrony – wymagania formalne i procedura

Podstawowym podmiotem prawnym w strukturze samorządowej jednostki organizacyjnej mającym na celu ochronę informacji niejawnych jest pełnomocnik do sprawy informacji niejawnych. Stosownie do treści przepisu art. 14 ust. 2 i 3 de lege lata ustawy o ochronie informacji niejawnych kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej pełnomocnikiem ochrony, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. I tak, pełnomocnikiem ochrony może być osoba, która posiada: obywatelstwo polskie, wykształcenie wyższe, odpowiednie poświadczenie bezpieczeństwa wydane przez ABW albo SKW, a także przez były Urząd Ochrony Państwa lub byłe Wojskowe Służby Informacyjne oraz zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych przeprowadzonym przez ABW albo SKW, a także przez byłe Wojskowe Służby Informacyjne.

Należy pamiętać, że posiadanie obywatelstwa polskiego przez kandydata ubiegającego się o zatrudnienie na przedmiotowym stanowisku pracy jest podstawowym elementem oceny formalnej wniosków o zatrudnienie. Legitymowanie się wyłącznie obywatelstwem polskim może sprzyjać uniknięciu w przyszłości zwerbowania pracownika do współpracy z obcym wywiadem, podejmowania działalności szpiegowskiej, sabotażowej sprzecznej z interesem państwa polskiego oraz lokalnej wspólnoty samorządowej. Warto dostrzec, iż posiadanie dwóch lub więcej obywatelstw albo statusu cudzoziemca nie dawałoby gwarancji rzetelności oraz uczciwości w wykonywaniu obowiązków służbowych. Kandydat na stanowisko pełnomocnika ochrony powinien również wykazywać się posiadaniem wykształcenia wyższego. Ustawodawca nie wymaga od kandydata dyplomu ściśle określonego kierunku studiów. Niemniej jednak z uwagi na charakter obowiązków służbowych powierzonych pełnomocnikowi ochrony oczekiwanym od kandydata wykształceniem jest wyższe techniczne. Za takim argumentem niewątpliwie przemawiają względy faktyczne. Zatrudnienie w charakterze pełnomocnika ochrony wiąże się z koniecznością posiadania zdolności informatycznych, umiejętności analitycznych oraz podstawowej wiedzy prawniczej. Nie bez znaczenia pozostaje również sprawność fizyczna. W przypadku wystąpienia bezpośredniego zagrożenia dla życia i zdrowia człowieka pełnomocnik ochrony stoi w gotowości do przeciwdziałania temu stanowi. Z tego względu od pracownika zatrudnionego na stanowisku pełnomocnika ochrony można oczekiwać również ukończenia specjalistycznych studiów podyplomowych przygotowujących do wykonywania pracy na tym stanowisku.

[3] t. j. Dz. U. z 2019 r. poz. 742

Warto odnotować, że o wyborze kandydata na wymienioną posadę świadczy nie tylko jego przygotowanie merytoryczne, ale także predyspozycje osobowościowe. Pełnomocnik ochrony musi być osobą komunikatywną, zawsze będącą w gotowości do współpracy z kierownikiem samorządowej jednostki organizacyjnej. Kierownik z kolei nawiązując stosunek pracy z pełnomocnikiem ochrony powinien mieć świadomość szczególnego charakteru powierzonych obowiązków. Kształtując politykę kadrową w samorządowej jednostce organizacyjnej jej kierownik powinien uwzględnić stabilność zatrudnienia na stanowisku pełnomocnika ochrony. Ze względu na ochronę interesu publicznego oraz dobro jednostki samorządowej nie będą pożądanym zjawiskiem notoryczne zmiany kadrowe na stanowisku pełnomocnika ochrony. Koniecznym jest zauważyć, iż osoba zatrudniona na tym stanowisku odpowiada za organizację kancelarii tajnej. Wszelkiego rodzaju rotacje w zatrudnieniu mogłoby przyczynić się do utraty kontroli nad należytym zabezpieczeniem informacji niejawnych. Co istotne, pełnomocnikiem ochrony może zostać osoba dysponująca zaświadczeniem o odbyciu szkolenia w zakresie ochrony informacji niejawnych. Zgodnie z treścią przepisu art. 19 de lege lata ustawy o ochronie informacji niejawnych niniejsze szkolenie przeprowadza się w celu zapoznania z kandydata na pełnomocnika ochrony z przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych, zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka oraz sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia. Wymienione szkolenie dla pełnomocników ochrony nie rzadziej niż raz na pięć lat przeprowadzają: Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego. Ustawodawca przewidział możliwość odstąpienia od przeprowadzenia szkolenia w przypadku, gdy kandydat na stanowisko pełnomocnika ochrony przedstawi zaświadczenie o odbyciu szkolenia. Trzeba również nadmienić, że warunkiem nawiązania stosunku pracy z kandydatem na pełnomocnika ochrony jest pozytywny wynik postępowania sprawdzającego prowadzonego przez organ administracji publicznej (ABW oraz SKW). Celem tej procedury jest potwierdzenie w toku postępowania dowodowego, iż osoba sprawdzana będzie dawała rękojmi zachowania tajemnicy. Oznacza to, iż organ administracji publicznej działając na podstawie treści przepisu art. 22 ust. 2 pkt 2b analizowanej ustawy w stosunku do kandydata na przedmiotowe stanowisko dokonuje wszczęcia poszerzonego postępowania sprawdzającego opierającego się na czynnościach procesowych wykluczających możliwość jego uczestnictwa, współpracy lub popierania działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko Rzeczypospolitej Polskiej. W toku postępowania wyjaśniającego organ administracji publicznej musi wyjaśnić realność ewentualnych zagrożeń wobec osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu. Organ ten powinien usunąć wszelkie wątpliwości względem: naruszenia przez kandydata na pełnomocnika ochrony porządku konstytucyjnego Rzeczypospolitej Polskiej oraz przynależności do partii politycznych lub innych organizacji, o których mowa w art. 13 Konstytucji RP; ukrywania lub świadomego niezgodnego z prawdą podawania w ankiecie bezpieczeństwa osobowego lub w postępowaniu sprawdzającym informacji mających znaczenie dla ochrony informacji niejawnych; wystąpienia okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji oraz wymienionych w tym źródle prawa niewłaściwych form postępowania z informacjami niejawnymi. Co znamienne, w trakcie poszerzonego postępowania sprawdzającego organ administracji publicznej bada: poziom życia osoby sprawdzanej wyraźnie przewyższający uzyskiwane przez nią dochody, gromadzi informacje o ewentualnej chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do wykonywania prac, związanych z dostępem do informacji niejawnych oraz stan uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych.

Poszerzone postępowanie sprawdzające poza czynnościami procesowymi, o których mowa w treści przepisu art. 25 niniejszej ustawy obejmuje również rozmowę z przełożonymi osoby sprawdzanej oraz z innymi osobami, przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej oraz sprawdzenie stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, w szczególności wobec Skarbu Państwa. Postępowanie sprawdzające kończy się z wynikiem pozytywnym wydaniem poświadczenia bezpieczeństwa, wynikiem negatywnym poprzez odmowę wydania poświadczenia bezpieczeństwa lub umorzeniem postępowania. Poświadczenie bezpieczeństwa wydaje się na okres: dziesięciu lat – w przypadku dostępu do informacji niejawnych o klauzuli „poufne", siedmiu lat – w przypadku dostępu do informacji niejawnych o klauzuli „tajne" lub pięciu lat – w przypadku dostępu do informacji niejawnych o klauzuli „ściśle tajne". Dostęp do informacji niejawnych o klauzuli tajności „zastrzeżone" może nastąpić po pisemnym upoważnieniu przez kierownika jednostki organizacyjnej, jeżeli nie posiada się poświadczenia bezpieczeństwa oraz po przeszkoleniu w zakresie ochrony informacji niejawnych[4]. Decyzja o odmowie wydania poświadczenia bezpieczeństwa z kolei powinna zawierać: podstawę prawną oraz uzasadnienie faktyczne i prawne; wskazanie wnioskodawcy postępowania sprawdzającego; określenie organu, który przeprowadził postępowanie sprawdzające; datę i miejsce wydania; imię, nazwisko i datę urodzenia osoby sprawdzanej; określenie rodzaju przeprowadzonego postępowania sprawdzającego, ze wskazaniem klauzuli informacji niejawnych, do których osoba sprawdzana miała mieć dostęp; stwierdzenie, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy; imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW oraz pouczenie o dopuszczalności i terminie wniesienia odwołania do Prezesa Rady Ministrów. Umorzenie postępowania sprawdzającego zaś następuje w przypadku: śmierci osoby sprawdzanej; rezygnacji osoby sprawdzanej z ubiegania się o stanowisko albo zajmowania stanowiska lub wykonywania prac, związanych z dostępem do informacji niejawnych; odstąpienia przez kierownika jednostki organizacyjnej od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac, związanych z dostępem do informacji niejawnych lub gdy postępowanie z innej przyczyny stało się bezprzedmiotowe.

Od decyzji o odmowie wydania poświadczenia bezpieczeństwa lub o umorzeniu postępowania sprawdzającego wydanej przez ABW lub SKW osobie sprawdzanej przysługuje prawo do wniesienia środka zaskarżania w postaci odwołania. Nie wymaga ono uzasadnienia. Odwołanie wnosi się do Prezesa Rady Ministrów w terminie czternastu dni od dnia doręczenia osobie sprawdzanej decyzji administracyjnej. Rozpatrzenie odwołania powinno nastąpić nie później niż w ciągu 3 miesięcy od dnia jego otrzymania Wniesienie odwołania nie wstrzymuje wykonania tej decyzji. Warto dodać, że Prezes Rady Ministrów w drodze postanowienia może stwierdzić niedopuszczalność odwołania lub uchybienie terminowi do wniesienia odwołania. Odwołanie uznaje się za niedopuszczalnie w przypadku, gdy zostało wniesione przez osobę nie będącą stroną postępowania. Jeżeli osoba sprawdzana dokona wniesienia odwołania po upływie terminu ustawowego może wnioskować o przywrócenie terminu do wniesienia tego odwołania. Warunkiem skutecznego przywrócenia tego terminu jest uprawdopodobnienie, iż wystąpiły przesłanki obiektywne uniemożliwiające dokonanie tej czynności procesowej w wymaganym czasie. Podstawę prawną stanowi treść przepisu art. 58 ustawy z dnia 14 czerwca 1060 r. - Kodeks postępowania administracyjnego[5].

Na gruncie postępowania sprawdzającego Prezes Rady Ministrów wydaje decyzję, w której: utrzymuje w mocy decyzję podmiotu, który przeprowadził postępowanie sprawdzające; uchyla decyzję podmiotu, który przeprowadził postępowanie sprawdzające, i nakazuje mu wydanie poświadczenia bezpieczeństwa; uchyla decyzję podmiotu, który przeprowadził postępowanie sprawdzające i przekazuje sprawę do ponownego rozpatrzenia lub stwierdza nieważność decyzji podmiotu, który przeprowadził postępowanie sprawdzające.

[4]https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-osobowe/146,BEZPIECZENSTWO-OSOBOWE.html
[5] t. j. Dz. U. z 2021 r. poz. 735, 1491, 2052.

W tym miejscu uwzględniając zasadę dwuinstancyjności postępowania sprawdzającego zakończeniu ulega procedura administracyjna. Osobie sprawdzanej przysługuje natomiast skarga do sądu administracyjnego w terminie 30 dni od dnia doręczenia decyzji lub postanowienia. Sąd administracyjny rozpatruje skargę na posiedzeniu niejawnym. Na rozstrzygnięcie Wojewódzkiego Sądu Administracyjnego stronie przysługuje prawo do wniesienia skargi kasacyjnej do Naczelnego Sądu Administracyjnego w myśl treści przepisów ustawy z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi[6]. Warto dodać, że na podstawie treści przepisu art. 33 i nast. de lege lata ustawy o ochronie informacji niejawnych w przypadku gdy o osobie, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy, przeprowadza się kontrolne postępowanie sprawdzające. Tryb i zasady kontrolnego postępowania sprawdzającego zawarte się w analizowanej ustawie.

Zadania pełnomocnika ochrony

Stosownie do treści przepisu art. 15 ust. 1 omawianej ustawy do zadań pełnomocnika ochrony należy:

- zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;
- zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne;
- zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;
- 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;
- 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;
- prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
- prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających;
- 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, obejmującego wyłącznie (imię i nazwisko, numer PESEL, imię ojca, datę i miejsce urodzenia, adres miejsca zamieszkania lub pobytu, określenie dokumentu kończącego procedurę, datę jego wydania oraz numer)
- przekazywanie odpowiednio ABW lub SKW do ewidencji, o których mowa w art. 73 ust. 1, danych, o których mowa w art. 73 ust. 2, osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, na podstawie wykazu, o którym mowa w pkt 8

Nie może umknąć uwadze fakt, że 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. W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli „poufne" lub wyższej pełnomocnik ochrony zawiadamia niezwłocznie również odpowiednio ABW lub SKW. Wymienione zadania pełnomocnik ochrony realizuje przy pomocy wyodrębnionej i podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnych, zwanej dalej „pionem ochrony", jeżeli jest ona utworzona w jednostce organizacyjnej.

[6] t. j. Dz. U. 2022 poz. 329

Teoretyzując tymi słowy warto dokonać analizy zadań powierzonych przez ustawodawcę ex lege. Elementarnym zadaniem pełnomocnika ochrony jest zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego. W opinii E. Gwardzińskiej: „ustawa o ochronie informacji niejawnych nie zawiera prawnej definicji informacji niejawnych. Należy przyjąć że informacje niejawne to te, którym wytwórca nadał jedną z czterech klauzul tajności: ściśle tajne, tajne, poufne lub zastrzeżone. Klasyfikacja informacji niejawnych oparta jest na kryterium szkody, która może powstać w wyniku jej ujawnienia"[7]. Niemniej należy zauważyć, że przedmiotowa ochrona ma miejsce w obliczu stosowania przepisów wymienionej ustawy. Oznacza to, że prawodawca w polskim systemie prawnym uregulował sferę informacji niejawnych podlegających ochronie. Ważną rolę w tym zakresie spełniają organy administracji publicznej. W ustawodawstwie zwykłym wiele uwagi poświęca się kwestiom ustrojowym dotyczącym kompetencji podmiotów publicznych w płaszczyźnie zapewnienia ochrony informacji niejawnych. Jedynym z istotnych obszarów działania władzy publicznej jest stosowanie środków bezpieczeństwa fizycznego. Wedle treści przepisu art. 45 ust. 1 i 2 de lege lata ustawy o ochronie informacji niejawnych jednostki organizacyjne, w których są przetwarzane informacje niejawne, stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności chroniące przed: działaniem obcych służb specjalnych; zamachem terrorystycznym lub sabotażem; kradzieżą lub zniszczeniem materiału; próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne oraz nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień. Zakres stosowania środków bezpieczeństwa fizycznego uzależnia się od poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą. W myśl treści przepisu art. 46 tej ustawy w celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej należy w szczególności: zorganizować strefy ochronne; wprowadzić system kontroli wejść i wyjść ze stref ochronnych; określić uprawnienia do przebywania w strefach ochronnych oraz stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.

Nie oznacza to jednak, że w przypadku zagwarantowania ochrony informacji niejawnych objętych klauzulą zastrzeżone, przedmiotowe obostrzenia nie obowiązują. Kierownik samorządowej jednostki organizacyjnej oraz pełnomocnik ochrony muszą stworzyć warunki ochrony informacji niejawnych znajdujących się w zasobach urzędów gmin, powiatów, województw oraz jednostek organizacyjnych im podległych. Warto podkreślić, że w systemie lokalnych źródeł prawa organy władzy publicznej powinny stworzyć regulacje normatywne, które stanowią przykład doprecyzowania norm ustawowych. Takie akty prawne sprzyjają usprawnieniu przestrzegania prawa w sferze dotyczącej ochrony informacji niejawnych. Co więcej, normy ustawowe stają się bardziej jasne i zrozumiałe, jeżeli w drodze aktów prawa miejscowego organ administracji publicznej zawrze normy prawne istotne z punktu widzenia ochrony informacji niejawnych na szczeblu jednostki samorządu terytorialnego. W odniesieniu do środków bezpieczeństwa fizycznego definicja legalnego tego zwrotu językowego znalazła się w aktach wykonawczych centralnych organów administracji rządowej. Podobne rozwiązanie prawne może być zastosowanie w sferze samorządu terytorialnego. I tak, stosowanie do treści przepisu § 3 ust. 1 zarządzenia Ministra Sprawiedliwości z dnia 23 stycznia 2014 r. w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych[8] system środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, w tym stref ochronnych, których kryteria tworzenia zostały określone w § 5 ust. 1 i 4 rozporządzenia, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych. Innymi słowy, system środków bezpieczeństwa fizycznego obejmuje zespół ograniczeń i kontroli w sposobie przemieszania się osób uprawnionych w dostępie do informacji niejawnych oraz weryfikację prawidłowości stosowania systemów teleinformatycznych wykorzystywanych w celu przetwarzania informacji niejawnych.

[7] E. Gwardzińska, Bezpieczeństwo teleinformatyczne informacji niejawnych [w:] Kwartalnik Nauk O Przedsiębiorstwie nr 3, Warszawa 2011, s. 25
[8] Dz .Urz. MS.2014.32

Kluczowym obszarem zadań pełnomocnika ochrony pozostaje obszar działań w zakresie bezpieczeństwa teleinformatycznego. Na temat tego zwrotu językowego wypowiada się doktryna prawnicza. P. Swoboda wskazał, że: „bezpieczeństwo informacji niejawnych [to] całokształt przedsięwzięć technicznych i organizacyjnych ukierunkowanych na zabezpieczenie procesów przetwarzania informacji istotnych z punktu widzenia bezpieczeństwa i podstawowych interesów państwa"[9]. Nie wolno zapominać, iż zapewnieniu ochrony systemów teleinformatycznych znajdujących się w zasobach samorządowej jednostki organizacyjnej sprzyjają standardy technologiczne wdrożone przez kierownika jednostki organizacyjnej. Zgodnie z treścią przepisu art. 48 analizowanej ustawy systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego. ABW albo SKW udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej. Akredytacji tej udziela się na czas określony, nie dłuższy niż pięć lat. Wymienione organy administracji publicznej udzielają albo odmawiają udzielenia akredytacji w terminie sześciu miesięcy od otrzymania kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego. W uzasadnionych przypadkach, w szczególności wynikających z rozległości systemu i stopnia jego skomplikowania, termin ten może być przedłużony o kolejne sześć miesięcy. Od odmowy udzielenia akredytacji nie służy odwołanie. Potwierdzeniem udzielenia akredytacji jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego. W świetle niniejszych rozwiązań normatywnych należy odnotować, iż ogromną rolę na etapie bezpieczeństwa teleinformatycznego spełniają kryteria zastosowania właściwego systemu teleinformatycznego, w tym sprzętu komputerowego oraz oprogramowania. W pracy zawodowej pracowników samorządowych wykonujących czynności z zakresu ochrony informacji niejawnych, w szczególności osoby obsługujące kancelarię tajną oraz pracownicy pionu ochrony powinni wykonywać zadania na sprzęcie komputerowym sprawnym technicznie oraz o wysokiej jakości technologicznej. Oprogramowania komputerowe muszą być zabezpieczone hasłem dostępu, które powinno być cyklicznie zmieniane. M. Kiedrowicz oraz J. Koszela nadmienili, że: „w organizacji, w której przewiduje się przetwarzanie dokumentów wrażliwych, oprócz zatrudnionego pełnomocnika ochrony informacji niejawnych tworzy się pion ochrony, bezpośrednio podległy pełnomocnikowi ochrony informacji niejawnych. W zależności od potrzeb w pionie tym mogą być zatrudnieni: kierownik kancelarii tajnej; zastępca kierownika kancelarii tajnej; kancelista; personel bezpieczeństwa wykonujący czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń, w których są przetwarzane informacje niejawne wyłącznie przez osoby uprawnione; inspektor bezpieczeństwa teleinformatycznego oraz administrator systemu teleinformatycznego"[10].

Ważnym zadaniem do wykonania dla pełnomocnika ochrony pozostaje sfera zarządzania ryzykiem bezpieczeństwa informacji niejawnych oraz jego szacowania. K. Liderman dostrzegł, iż: „zarządzanie ryzykiem (na potrzeby bezpieczeństwa teleinformatycznego) ma na celu: wykazanie, których ryzyk i jak można uniknąć, stosując rozwiązania organizacyjne i techniczne w zakresie przetwarzania, przesyłania i przechowywania informacji w firmowych systemach IT, zapewnienie optymalnego, ze względu na koszty i znane/zadane ograniczenia, stanu ochrony ww. informacji oraz zminimalizowanie ryzyka szczątkowego tak, aby stało się ryzykiem akceptowalnym"[11]. Nie pozostaje kwestią sporna, że w każdym obszarze pracy zawodowej, niezależnie od jej charakteru oraz poziomu trudności i złożoności istnieje ryzyko wystąpienia pewnych nieprawidłowości. Analogicznie z problematykę ryzyka dostrzega się na gruncie bezpieczeństwa informacji niejawnych. Należy więc przewidzieć (oszacować) stopień możliwości wystąpienia takiego ryzyka.

[9] P. Swoboda, Bezpieczeństwo informacji niejawnych [w:] Vademecum bezpieczeństwa informacyjnego t. I, praca zbiorowa pod red. O. Wasiuty oraz R. Klepki, Kraków 2019, s. 73
[10] M. Kierdowicz, J. Koszela, Model kancelarii przetwarzającej dokumenty wrażliwe z wykorzystaniem technologii RFID [w:] Roczniki Kolegium Analiz Ekonomicznych nr 42, Warszawa 2016, s. 70-71
[11] K. Liderman, Zarządzanie ryzykiem jako element zapewnienia określonego poziomu bezpieczeństwa teleinformatycznego [w:] Biuletyn Instytutu Automatyki i Robotyki nr 23, Warszawa 2006, s. 48

Nigdy bowiem nie ma stuprocentowej gwarancji bezbłędności, sprawności i prawidłowości należytego zabezpieczenia danych podlegających ochronie. Niewątpliwie na przedmiotowe ryzyko składa się szereg okoliczności, w szczególności: niesprawność systemu teleinformatycznego, omyłki w wykonywaniu czynności służbowych przez pracowników samorządowych jednostek organizacyjnych oraz zawinione, umyślne i zaplanowane działania tych pracowników mających na celu świadome ujawnienie informacji niejawnych. Szanowanie stopnia ryzyka nieuprawnionego dostępu do informacji niejawnych odbywa się przy pomocy skomplikowanych analiz statystycznych z wykorzystaniem metadanych. Oznacza to, że w procedurze szacowania ryzyka powinni uczestniczyć pracownicy posiadający wykształcenie techniczne oraz wiedzę z zakresu informatyki oraz matematyki.

W obszarze czynności pełnomocnika ochrony mieszczą się również zadania polegające na prowadzeniu kontroli 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. Przedmiot tej kontroli skupia się wokół zagadnień stricte powiązanych z zakresem regulacji prawnej objętej obowiązującą ustawą o ochronie informacji niejawnych, głównie ma na celu ocenę poprawności wykonywania zadań przez pracowników zatrudnionych w pionie ochrony oraz obsługujących kancelarię tajną, weryfikację sposobów ewidencjonowania dokumentów i materiałów objętych klauzulami tajności oraz organizacji całego systemu informacji niejawnych w samorządowej jednostce organizacyjnej. W przypadku uprawdopodobnienia, że pracownik naruszył przepisy wymienionej ustawy pełnomocnik ochrony zobligowany jest poinformować o tym fakcie kierownika samorządowej jednostki organizacyjnej zatrudniającego pracownika, a nawet zgłosić zaistniałe naruszenie prawa ABW oraz SKW. W uzasadnionych sytuacjach wobec osoby sprawdzanej może zostać wszczęte kontrolne postępowanie sprawdzające. W myśl treści przepisu art. 33 ust. 11 niniejszej ustawy kontrolne postępowanie sprawdzające kończy się: decyzją o cofnięciu poświadczenia bezpieczeństwa; poinformowaniem o braku zastrzeżeń w stosunku do osoby, którą objęto kontrolnym postępowaniem sprawdzającym, z jednoczesnym potwierdzeniem dalszej jej zdolności do zachowania tajemnicy w zakresie określonym w posiadanym przez nią poświadczeniu bezpieczeństwa lub decyzją o umorzeniu postępowania, w przypadku gdy postępowanie to nie zostanie zakończone przed upływem dwunastu miesięcy od dnia jego wszczęcia.

Następną płaszczyzna działania pełnomocnika ochrony w strukturze aparatu administracyjnego jest 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. Wymieniony dokument jest swoistym odzwierciedleniem obowiązujących w samorządowej jednostce organizacyjnej przepisów de lege lata ustawy o ochronie informacji niejawnych. Praktyka administracyjna dowodzi, że plan ochrony informacji niejawnych może być mniej lub bardziej złożonym w swej treści dokumentem, który przyjmując formę zarządzenia organu wykonawczego staje się częścią prawa miejscowego. W przedmiotowym dokumencie uwzględnia się w szczególności: wyjaśnienie terminu planu ochrony informacji niejawnych, podstawę prawną uchwalenia tego źródła prawa, definicje legalne przyjęte w zarządzeniu, charakterystykę obiektu, w którym przetwarzane są informacje niejawne, zasady udostępniania, przechowywania i zabezpieczania dokumentów zawierających informacje niejawne, zagrożenia wewnętrzne i zewnętrzne w zawiązku z ryzykiem nienależytego zabezpieczenia tych informacji i inne aspekty istotne z normatywnego punktu widzenia dla samorządowej jednostki organizacyjnej. W biuletynach informacji publicznej jednostek samorządu terytorialnego istnieje wiele przykładów planów ochrony informacji niejawnych[12].

Zamienną kompetencją pełnomocnika ochrony jest prowadzenie szkoleń w zakresie ochrony informacji niejawnych w samorządowej jednostce organizacyjnej.

[12] https://bip-v1-files.idcom-jst.pl/sites/47235/wiadomosci/477026/files/zal1.pdf
https://bip.malopolska.pl/e,pobierz,get.html?id=1838677
http://www.mierzecice.bip.info.pl/plik.php?id=2033.

Cel przedmiotowego szkolenia jest analogiczny z celem szkolenie organizowanego przez ABW oraz SKW dla pełnomocników ochrony. W siedzibie samorządowej jednostki organizacyjnej szkolenie przeprowadza samodzielnie pełnomocnik ochrony lub we współudziale wymienionych organów administracji publicznej. Pełnomocnik ochrony odpowiada również za prowadzenie ewidencji pracowników mających uprawienia dostępu do informacji niejawnych oraz sporządza wykaz osób, którym organ odmówił dostępu do dokumentów i materiałów o tym charakterze. Pełnomocnik ochrony wykonuje również inne zadania powierzone przez kierownika samorządowej jednostki organizacyjnej mające na celu usprawnienie wykonywania obowiązków służbowych w zakresie informacji niejawnych.

4.Zakończenie

Tematyka dotycząca statusu prawnego pełnomocnika ochrony informacji niejawnych w jednostkach samorządu terytorialnego zaliczana się do kręgu fundamentalnych zadań publicznych lokalnej administracji. Ze względu na zakres kompetencji tego podmiotu oraz szczególny charakter techniczny profesji pełnomocnika ochrony nie każdy kandydat aplikujący na wymienione stanowisko pracy spełnia wymagane kryteria podmiotowe i osobowościowe. Zmysł analityczny, wizja taktyczna oraz sprawność w podejmowaniu decyzji są podstawowymi elementami predyspozycji w wykonywaniu obowiązków służbowych przez pełnomocnika ochrony. Cennym atutem kandydata na wskazaną funkcję jest posiadanie odpowiedniego stażu pracy wykazującego doświadczenie zawodowe na uprzednio zajmowanym stanowisku pełnomocnika ochrony lub zatrudnienia w pionie ochrony samorządowej jednostki organizacyjnej. Z uwagi na samodzielność działania pełnomocnik ochrony powinien wykazywać się dużym stopniem kompetencji zawodowej. Nie może być to osoba jedynie zdobywająca wiedzę praktyczną na zajmowanym stanowisku pracy.

Omawiając przedmiotową płaszczyznę normatywną należy odnotować, że de lege lata ustawa o ochronie informacji niejawnych jest stosunkowo trudnym źródeł prawa w wykładni jej przepisów prawnych. Niewiele uwagi poświęca też zagadnieniom dotyczącym pełnomocnika ochrony. Jeśli nawet precyzuje pewne kwestie, to czyni to w sposób rozproszony utrudniając tym samym interpretację ustawy. Ważną role muszą więc spełniać lokalne źródła prawa poświęcone problematyce dotyczącej informacji niejawnych. Prawodawca na gruncie wymienionej ustawy tworzy fundament w regulacji prawnej, ale także daje narzędzia samorządowym jednostkom organizacyjnym do uszczegóławiania aspektów normatywnych enigmatycznie i lapidarnie dostrzeżonych w sferze ustawowej. Prawidłowo przygotowane zarządzenie organu wykonawczego w obszarze dotykającym zagadnień związanych z ochroną informacji niejawnych jest swoistym drogowskazem dla prawidłowego stosowania przepisów normatywnych w płaszczyźnie samorządu terytorialnego. Dotychczasowa analiza nie wyczerpuje całości zakresu problemowego, jednak zwraca uwagę na najistotniejsze kwestie determinujące status prawny pełnomocnika ochrony w samorządowych jednostkach organizacyjnych.

O AUTORZE

dr Mariusz Paradowski - doktor nauk prawnych, kwalifikacje III stopnia uzyskał na Wydziale Prawa, Administracji i Stosunków Międzynarodowych Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego w Krakowie. Dysertację doktorską pt. Pozwolenie budowlane napisał pod kierunkiem prof. zw. dra hab. Józefa Filipka. Był słuchaczem studiów podyplomowych z zakresu prawa, ekonomii i pedagogiki: w Warszawskiej Szkole Zarządzania – Szkole Wyższej w Warszawie, Wyższej Szkole Ekonomii i Innowacji w Lublinie, Politechnice Krakowskiej im. Tadeusza Kościuszki w Krakowie, Politechnice Częstochowskiej oraz Wyższej Szkole Zarządzania w Częstochowie. Studia magisterskie ukończył na Wydziale Prawa i Administracji Uniwersytetu Śląskiego w Katowicach.

Warszawa, lipiec 2022
www.frdl.org.pl
Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego
ul. Żurawia 43, 00-680 Warszawa