

# PION OCHRONY INFORMACJI NIEJAWNYCH GABINETU KGP

## Kierownictwo, struktura, zadania



**PODINSP. RADOSŁAW MAZUR**  
Zastępca Dyrektora Gabinetu  
Komendanta Głównego Policji  
ds. ochrony informacji niejawnych

Odpowiada za bezpieczeństwo informacji niejawnych, systemów teleinformatycznych i danych osobowych będących w dyspozycji Policji. Zastępca dyrektora Gabinetu KGP odpowiedzialny za ochronę informacji niejawnych wykonuje zadania Pełnomocnika Komendanta Głównego ds. ochrony informacji niejawnych. Ta część biura prowadzi postępowania sprawdzające wobec wszystkich osób, które są lub mają być zatrudnione w Komendzie Głównej Policji i obsługuje Komendanta Głównego Policji w zakresie upoważnień do dostępu do informacji niejawnych. Właściwa komórka Gabinetu KGP realizuje procedury związane z udostępnianiem materiałów niejawnych, zwalnianiem z obowiązku zachowania informacji niejawnych w tajemnicy oraz ze zmianą lub zniesieniem klauzuli tajności materiałów niejawnych wytworzonych w Policji. Kilkanaście kilometrów póltek z archiwalnymi aktami to też domena Gabinetu KGP. Archiwum – wbrew obiegowej opinii – cały czas żyje: zmienia się status dokumentów, niektóre są udostępniane, inne niszczone, a archiwizacja kolejnych ciągle trwa.

*Roman Miśkiewicz, Naczelnik Wydziału Prezydialnego Gabinetu KGP  
Irena Fedorowicz, główny specjalista Wydziału Prezydialnego Gabinetu KGP*



Schemat struktury organizacyjnej pionu ochrony informacji niejawnych Gabinetu KGP

# Działalność w zakresie ochrony informacji niejawnych

**P**ion ochrony KGP strukturalnie jest umiejscowiony w Gabinetcie Komendanta Głównego Policji. W jego skład wchodzi cztery komórki organizacyjne: Wydział Bezpieczeństwa Teleinformatycznego, Wydział Bezpieczeństwa Osobowego, Kancelaria Tajna oraz Sekcja – Główne Archiwum Policji. Oczywiście, zdaję sobie sprawę, że dla czytelników „Kwartalnika Policyjnego” nie jest tajemnicą, czym zajmuje się pion ochrony, jednak Komenda Główna Policji, jako centralny organ administracji policyjnej, ma swą specyfikę i pewne odmienności w stosunku do pionów ochrony funkcjonujących w jednostkach Policji niższych szczebli.

Ochrona informacji niejawnych ma dla Policji szczególnie ważne znaczenie. Cała działalność naszej formacji jest nacechowana koniecznością zapewnienia co najmniej szczególnego rodzaju dyskrekcji. Celowo używam takiego właśnie sformułowania, by wyraźnie zaakcentować wagę ochrony informacji niejawnych jako szczególnego rodzaju tajemnicy prawnie chronionej. Policja działa na rzecz społeczeństwa i jej podstawowa działalność wymaga żywego z nim kontaktu, a więc tak ważną rolę odgrywają tu komórki np. komunikacji społecznej czy prewencji kryminalnej. W związku z tym jednak, że nie każdemu przestępstwu da się zapobiec, musimy także prowadzić działania dochodzeniowo-śledcze oraz operacyjno-rozpoznawcze, a im dalej pójdziemy w kierunku pracy operacyjnej, tym więcej spotkamy informacji niejawnych, począwszy od „zastrzeżonych” i „poufnych”, po „ściśle tajne”, które występują przy najpoważniejszych sprawach realizowanych jako np. operacje specjalne czy związane są z ochroną świadków koronnych.

Przed prezentacją wybranych zagadnień z obszaru ochrony informacji niejawnych przez poszczególne komórki organizacyjne, pokrótce przedstawię, czym one się zajmują w codziennej pracy.

Wydział Bezpieczeństwa Teleinformatycznego dba o zachowanie poufności policyjnych informacji, których przetwarzanie odbywa się w sieciach systemów teleinformatycznych, a dodam tylko, że jest ich kilkadziesiąt. Zadaniem z tego kręgu tematycznego zajmują się inspektorzy bezpieczeństwa teleinformatycznego, którzy muszą m.in. posiadać specjalistyczną wiedzę informatyczną oraz mieć ukończone szkolenia z tego zakresu, organizowane przez Agencję Bezpieczeństwa Wewnętrznego. Zadanie to, jakkolwiek wiodące, nie jest jedynym realizowanym przez wydział. W strukturach wydziału funkcjonuje też, wraz ze wspierającymi go pracownikami, Administrator Bezpieczeństwa Informacji. Ta część wydziału dba o to, aby nie tylko w niejawnych systemach, ale wszędzie tam w Policji, gdzie przetwarzane są dane osobowe, były przestrzegane przepisy regulujące problematykę ochrony tych właśnie danych.

Wydział Bezpieczeństwa Osobowego wykonuje zadania, które również można przyporządkować dwóm obszarom tema-

tycznym. Pierwszym z nich jest prowadzenie postępowań sprawdzających wobec policjantów i pracowników cywilnych Komendy Głównej Policji, mających na celu urzędowe potwierdzenie dawania przez nich rękąmi zachowania tajemnicy. Ponadto wydział pośredniczy w uzyskiwaniu poświadczeń bezpieczeństwa z zakresu informacji niejawnych Unii Europejskiej i NATO (organem wydającym poświadczenia jest tu Agencja Bezpieczeństwa Wewnętrznego). Przez wydział „przechodzą” również liczne tomy z prowadzonej przez Policję pracy operacyjnej. Pracownicy wydziału przygotowują rekomendacje Komendantowi Głównemu Policji na temat zgody (lub jej braku) na zniesienie klauzuli tajności poszczególnych materiałów oraz opracowują projekty stanowisk KGP przesyłanych następnie Ministrowi Spraw Wewnętrznych, w których Komendant rekomenduje (lub nie) zwolnienie policjantów lub pracowników Policji z obowiązku zachowania tajemnicy. Chyba nikogo nie muszę przekonywać, jaką wagę ma właściwe i skrupulatne wykonywanie tego rodzaju zadań.

Kancelaria Tajna KGP jest zlokalizowana na terenie Warszawy, w kilku obiektach komendy. Komórka ta robi dokładnie to, co kancelarie tajne innych jednostek Policji, jednak na większą skalę. W ciągu roku rejestruje około 50 tys. materiałów niejawnych, w tym materiałów o klauzuli „ściśle tajne” (tych ostatnich np. w ubiegłym roku było 660) oraz materiałów oznaczonych klauzulami tajności organizacji międzynarodowych (UE i NATO).

Główne Archiwum Policji to swego rodzaju składnica akt (czyli „archiwum” znane w jednostkach terenowych Policji szczebla powiatowego), tylko w skali makro. W obiektach magazynowych GAP znajduje się około 6 km bieżących najróżniejszych archiwaliów policyjnych. Składowane są one w kilku naprawdę dużych pomieszczeniach magazynowych. Wyobraźmy sobie, ile pracy muszą wykonać pracownicy GAP, aby najpierw przyjąć te materiały (w najbliższych tygodniach do GAP spłynę m.in. ok. 20 tys. tomów akt archiwalnych poza już składowanymi), następnie właściwie je przechowywać, udostępniać oraz brakować (na wybrakowanie czeka obecnie niemal 59 tys. tomów akt archiwalnych). GAP prowadzi także bieżącą współpracę z IPN-em, co jest swoistą konsekwencją dawnego powiązania organizacyjnego Milicji Obywatelskiej ze strukturami Służby Bezpieczeństwa. Poza tym GAP rozpoczął i prowadzi prace związane z digitalizacją zasobu archiwalnego Komendy Głównej Policji.

Po tej krótkiej prezentacji zapraszam czytelników „Kwartalnika Policyjnego” do zapoznania się z wybranymi aspektami merytorycznego zaangażowania poszczególnych komórek organizacyjnych pionu ochrony KGP.

*nadkom. w st. spocz. Andrzej Sprycha  
Pełnomocnik Komendanta Głównego Policji  
ds. ochrony informacji niejawnych*

## UDOSTĘPNIANIE INFORMACJI NIEJAWNYCH

Zasadniczym zadaniem **Wydziału Bezpieczeństwa Osobowego** jest prowadzenie postępowań sprawdzających mających na celu ustalenie, czy poddane sprawdzeniu osoby dają rękojmię zachowania tajemnicy. W pozytywnych przypadkach Pełnomocnik Komendanta Głównego Policji ds. Ochrony Informacji Niejawnych wydaje poświadczenia bezpieczeństwa upoważniające policjantów i pracowników Komendy Głównej Policji oraz komendantów wojewódzkich Policji i Dyrektora Centralnego Laboratorium Kryminalistycznego Policji do dostępu do informacji niejawnych. Jest to bardzo istotne z uwagi na konieczność ochrony informacji niejawnych znajdujących się w obiegu w Policji. Należy także pamiętać, iż jednym z warunków zostania policjantem jest właśnie dawanie rękojmi zachowania tajemnicy.

Niezależnie od powyższego wydział realizuje również zadania związane z udostępnianiem informacji niejawnych dla potrzeb prokuratur, sądów i innych uprawnionych podmiotów, a także zmianą klauzuli tajności dokumentów podpisanych przez Komendanta Głównego Policji oraz wszystkich oznaczonych klauzulą „ściśle tajne”, wytworzonych w Komendzie Głównej Policji. Najistotniejsza – z uwagi na bezpośredni związek informacji niejawnych z postępowaniami karnymi – jest problematyka udostępniania tego rodzaju informacji.

Wiele zadań realizowanych w Policji regulują niejawnie przepisy wewnętrzne. Także czynności wykonywane w toku realizacji tych zadań z reguły są oznaczane klauzulami tajności. Najwięcej dokumentów niejawnych jest wytwarzanych w związku z prowadzonymi czynnościami operacyjno-rozpoznawczymi. Jesteśmy zobowiązani do ochrony informacji o formach, zasadach i organizacji tego rodzaju czynności, a także o prowadzonych działaniach oraz stosowanych środkach i metodach ich realizacji. W szczególności musimy chronić dane identyfikujące osoby udzielające pomocy Policji w czynnościach operacyjno-rozpoznawczych oraz policjantów realizujących te zadania. Ujawnienie informacji niejawnych osobom nieuprawnionym jest z reguły przestępstwem. Z drugiej strony należy podkreślić, że celem pracy operacyjnej jest m.in. zapobieganie, rozpoznawanie, ujawnianie czynów zabronionych oraz wykrywanie i ściganie ich sprawców, odnajdywanie osób ukrywających się przed wymiarem sprawiedliwości czy odzyskiwanie rzeczy utraconych w wyniku czynów zabronionych. Realizacja tych zadań wymaga niejednokrotnie wykorzystania informacji niejawnych uzyskanych w toku pracy operacyjnej do celów procesowych. Właśnie w tym zakresie wydział koordynuje czynności związane z opiniowaniem wystąpień uprawnionych podmiotów o udostępnienie informacji niejawnych.

Obowiązujące przepisy określają zasady udostępniania informacji niejawnych poza resort spraw wewnętrznych. Głównymi regułami są: wymóg uzyskania zgody ministra właściwego do spraw wewnętrznych na udzielenie wiadomości stanowiącej informację niejawną oraz udostępnianie tych informacji jedynie w przypadkach podejrzenia popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych. Najczęściej takie sytuacje pojawiają się, gdy mamy do czynienia z nieprawidłowościami dotyczącymi wydatkowania funduszu operacyjnego, ujawnianiem osobom nieuprawnionym informacji uzyskanych w toku czynności operacyjno-rozpoznawczych

czy uzyskaniem korzyści za odstąpienie od prowadzonych czynności.

Od tych zasad są oczywiście wyjątki. Udostępnienie materiałów uzyskanych w związku ze stosowaniem kontroli operacyjnych (m.in. podsłuchów rozmów czy kontroli korespondencji), kontrolowanego zakupu czy wręczenia lub przyjęcia korzyści majątkowej oraz przesyłki niejawnie nadzorowanej nie wymaga zgody ministra. W przypadkach uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania dokumentacja przekazywana jest prokuratorowi bezpośrednio przez osobę uprawnioną do wnoszenia o zarządzenie lub zarządzenia tych czynności, a więc Komendanta Głównego Policji lub komendanta wojewódzkiego/stołecznego Policji.

W szczególnie uzasadnionych przypadkach Komendant Główny Policji może wyrazić pisemną zgodę na jednorazowe udostępnienie informacji niejawnych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa. W praktyce tego rodzaju decyzje są wydawane celem umożliwienia zapoznania operatora telekomunikacyjnego lub internetowego, ewentualnie pracownika banku, z postanowieniem o zarządzeniu kontroli operacyjnej lub udostępnieniu informacji, dokonania tłumaczenia tekstu czy przeprowadzenia ekspertyzy. Wydział pośredniczy w uzyskiwaniu zgody Komendanta w tym zakresie. Sytuacje wymagające takiej zgody zachodzą także w trakcie prowadzenia ochrony osoby np. świadka koronnego w celu załatwienia spraw bezpośrednio dotyczących osoby chronionej lub jej rodziny w urzędach czy np. szkole. Z uwagi na charakter prowadzonych czynności ochronnych zgodę na jednorazowe udostępnienie tego rodzaju informacji z reguły uzyskuje bezpośrednio pion prowadzący ochronę.

Kolejnym wyjątkiem od wskazanych zasad jest możliwość udostępnienia informacji o osobie uzyskanych w czasie wykonywania czynności operacyjno-rozpoznawczych na żądanie sądu lub prokuratora w celu ścigania karnego, jeżeli taki obowiązek wynika z umów międzynarodowych czy ustawy, a także w przypadkach gdy zatajenie takiej informacji prowadziłoby do zagrożenia życia lub zdrowia innych osób. Wyżej opisane sytuacje dotyczą z reguły możliwości przekazania jawnych informacji o osobie.

W pozostałych przypadkach istnieje wymóg uzyskania zgody ministra i w związku z tym – w celu ujednoczenia praktyki i jednocześnie z uwagi na równorzędność podmiotów – przyjęto, iż opracowane w wydziale, na podstawie opinii właściwych jednostek lub komórek organizacyjnych, stanowisko Policji dotyczące wystąpień uprawnionych podmiotów o udostępnienie informacji niejawnych przekazuje do ministra właściwego do spraw wewnętrznych Komendant Główny Policji.

Udostępnienie informacji niejawnych dotyczy oczywiście dokumentów pisanych, a także informacji utrwalonych na różnego rodzaju nośnikach. Inną formą udostępniania informacji niejawnych, w szczególności do postępowań karnych, jest zwalnianie od obowiązku zachowania informacji niejawnych w tajemnicy. Jedynym podmiotem uprawnionym do zwolnienia policjantów, byłych funkcjonariuszy Policji, pracowników i byłych pracowników Policji od obowiązku zachowania w tajemnicy informacji niejawnych jest minister właściwy do spraw wewnętrznych.

Udostępnienie informacji niejawnych, w tym zwolnienie od obowiązku zachowania informacji niejawnych w tajemnicy, nie oznacza zniesienia ochrony tych informacji. Pozostają one niejawne i w związku z tym zarówno udostępnione materiały, jak i protokoły przesłuchań osób zwolnionych od obowiązku zachowania informacji niejawnych w tajemnicy, są przechowywane i wykorzystywane procesowo zgodnie z przepisami dotyczącymi ochrony informacji niejawnych w postępowaniu karnym.

Niezależnie od wyżej wskazanych ograniczeń istnieje możliwość udostępniania, w przypadkach szczególnie uzasadnionych, za zgodą ministra właściwego do spraw wewnętrznych, innych informacji niejawnych, w tym dotyczących metod lub taktyki prowadzenia czynności operacyjno-rozpoznawczych czy przepisów regulujących tę problematykę, do postępowań karnych, a także innym podmiotom, np. komisji sejmowej, Trybunałowi Konstytucyjnemu, Ministerstwu Sprawiedliwości czy innym służbom, lub np. wskazanym imiennie prokuratorom w celu umożliwienia uczestnictwa w specjalistycznym szkoleniu z zakresu pracy operacyjnej. Powyższa możliwość jest niezbędna z uwagi na nieprecyzyjność obowiązujących przepisów, a jednocześnie niejednokrotnie skomplikowany charakter czynności dowodowych wymuszający wykorzystanie informacji operacyjnych w procesie.

Z punktu widzenia ochrony informacji o czynnościach operacyjno-rozpoznawczych szczególnie istotna jest – jak wyżej wskazano – ochrona danych identyfikujących osoby udzielające pomocy Policji w zakresie czynności operacyjno-rozpo-

znawczych, policjantów realizujących konkretne czynności operacyjne, a także ochrona informacji dotyczących zasad i metod realizowania tego rodzaju czynności. W związku z powyższym konieczne jest każdorazowe dokonywanie dokładnej analizy materiałów wnioskowanych o udostępnienie pod kątem możliwości ich wykorzystania w postępowaniu karnym, a jednocześnie ochrony informacji niejawnych, które nie są niezbędne dla toczącego się postępowania. W każdym przypadku wydział ocenia zarówno korzyści dla toczącego się postępowania, jak i negatywne skutki udostępnienia określonych informacji niejawnych oraz proponuje zakres udostępnianych informacji, tak aby udostępnić jedynie materiały niezbędne do toczącego się postępowania. Zakres udostępnienia informacji niejawnych, w tym zwolnienia od obowiązku zachowania informacji niejawnych w tajemnicy musi być precyzyjnie określony, żeby nie nastąpiło niekontrolowane, a jednocześnie zalegalizowane ich udostępnienie. Między innymi w tym celu w wydziale jest prowadzona elektroniczna ewidencja „udostępnień” zrealizowanych pozytywnie i negatywnie, w której każdy kolejny wniosek w tej samej sprawie sprawdzany jest pod kątem wcześniejszych decyzji.

W przypadku wątpliwości dotyczących wyżej opisanej problematyki funkcjonariusze i pracownicy wydziału udzielają bieżących, także telefonicznych, konsultacji zainteresowanym osobom.

*Jerzy Młynkiewicz*

*główny specjalista Wydziału Bezpieczeństwa Osobowego Gabinetu KGP*

## STANDARYZACJA OCHRONY DANYCH OSOBOWYCH W POLICJI

**P**rzetwarzanie danych osobowych jest powszechne we współczesnym świecie. Czyni to m.in. Policja, która dysponuje tzw. danymi zwykłymi oraz wrażliwymi. Przepisy ustawy o ochronie danych osobowych nakładają określone, jednakowe obowiązki na podmioty przetwarzające takie dane, co powoduje konieczność ujednoczenia (przynajmniej w zakresie działania jednej służby czy podmiotu) ich ochrony.

Chcąc się w pełni odnieść do zagadnienia standaryzacji ochrony danych osobowych, a więc podejmowanych w Policji od lat kroków zmierzających do uzyskania optymalnego zorganizowania systemu bezpieczeństwa danych osobowych, należy przypomnieć generalne zasady leżące u jej podstaw. Po pierwsze, zgodnie z Konstytucją RP, organy Policji działają na podstawie i w granicach prawa. Po drugie, ochrona danych osobowych jest oparta na dwóch ustawowych filarach, którymi są przesłanki legalności ich przetwarzania (mówiące, kiedy w ogóle można je przetwarzać) oraz zasady ich przetwarzania. Przesłanki oraz zasady wyznaczają ramy procesowi standaryzacji ochrony danych osobowych. Istotne jest zatem, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne do celu, w jakim są pozyskiwane, a także przechowywane w postaci umożliwiającej identyfikację osób,

których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

W Policji w zakresie ogólnokrajowych zbiorów danych osobowych oraz danych osobowych przetwarzanych wyłącznie w KGP administratorem danych osobowych, a więc podmiotem decydującym o celach i środkach przetwarzania danych oraz odpowiedzialnym za właściwe działania, jest Komendant Główny Policji. Wraz ze zbiorami danych osobowych wdraża się przepisy regulujące ich funkcjonowanie oraz prowadzi dokumentację opisującą środki techniczne i organizacyjne podjęte w celu zapewnienia przetwarzanym danym niezbędnego bezpieczeństwa. Dokumentacjami tymi są polityki bezpieczeństwa i instrukcje zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych. W ramach standaryzacji, w odniesieniu do policyjnych zbiorów danych o zasięgu ogólnokrajowym, na poziomie Komendy Głównej Policji powstają tzw. dokumentacje matki, wiążące wszystkie jednostki Policji w kraju. Dla jednostek terenowych płynie z nich obowiązek wypełniania stosownych załączników celem uszczegółowienia lokalnych rozwiązań w zakresie ochrony danych (np. wskazania obszarów ich przetwarzania, zastosowania dodatkowych środków zabezpieczających) czy też wypełnienia kart charakteryzujących lokalne zabezpieczenie pomieszczeń. Powstają też dokumentacje wzory, na bazie któ-



rych można tworzyć kolejne, opisujące rozwiązania lokalne. Co do zasady, Komendant Główny Policji powierza realizację obowiązków administratora danych dyrektorom biur KGP oraz innym równorzędnym, a w zakresie właściwości miejscowej – komendantom wojewódzkim/stołecznemu Policji. Komendant Główny Policji dla zapewnienia nadzoru nad przestrzeganiem wdrożonych zasad ochrony danych wyznaczył w Komendzie Główniej Policji administratora bezpieczeństwa informacji. Zlokalizowany w Wydziale Bezpieczeństwa Teleinformatycznego Gabinetu Komendanta Głównego Policji administrator bezpieczeństwa informacji KGP sprawuje nadzór w powyższym zakresie, przekazując stosowne uwagi, wytyczne i zalecenia zmierzające do zapewnienia zakładanych i deklarowanych standardów ochrony. Inicjowana na szczeblu Komendy Główniej Policji standaryzacja ochrony danych osobowych stanowi zatem nie tylko proces, ale również efekt realizowanego w Gabinetzie Komendanta Głównego Policji nadzoru administratora bezpieczeństwa informacji KGP i współpracy z pozostałymi komórkami KGP w tym zakresie.

Takie uporządkowanie zadań administratora danych ma kluczowe znaczenie w kwestii spełniania dalszych wymogów prawa ochrony danych osobowych, tj. nadawania upoważnień do przetwarzania danych, ewidencjonowania osób upoważnionych, zabezpieczenia danych, a w szczególności zapewniania kontroli nad całym procesem przetwarzania, w tym reagowania w przypadku ewentualnych incydentów oraz dokładania szczególnej staranności w celu ochrony interesów osób, których dane dotyczą.

Takie same zasady dotyczą kierowników terenowych jednostek organizacyjnych Policji, którzy z mocy ustawy o ochronie danych osobowych są administratorami danych i powołują swoich administratorów bezpieczeństwa informacji.

Każdy upoważniony do przetwarzania danych osobowych musi mieć świadomość i przestrzegać zasad ochrony danych opisanych w dokumentacji, zakresu udzielonego upoważnienia, obowiązku niezwłocznego informowania o ewentualnym zaistniałym incydencie, a przede wszystkim obowiązku zapewnienia poufności danych, do których ma dostęp, oraz określonych sposobów ich zabezpieczenia. Nie bez znaczenia zatem jest przeprowadzanie w szkoleniach w tym zakresie. Stanowią one bowiem element niezbędny do uzyskania upoważnienia do przetwarzania danych osobowych i są standardowym etapem w drodze do ich bezpiecznego przetwarzania. Należy także przypomnieć, iż przetwarzanie danych osobowych to jakakolwiek operacja na takich danych, a więc już samo przechowywanie jest przetwarzaniem. Co za tym idzie, każdy, kto w jakikolwiek sposób ma do nich dostęp, nawet na etapie rejestracji pisma w kancelarii lub sekretariacie, bez merytorycznego załatwienia sprawy, już te dane przetwarza. Trzeba pamiętać, iż człowiek jest pierwszym potencjalnym źródłem nieuprawnionego ujawnienia takich danych. A zatem począwszy od pracowników przetwarzających dane w formie zapoznania się z dokumentem papierowym (bez względu na to, czy zajmą się daną sprawą merytorycznie), a na pracownikach merytorycznych, a w szczególności użytkownikach systemów informatycznych skończywszy – wszyscy muszą zostać przeszkoleni w zakresie ochrony danych osobowych, uzyskać upoważnienie do ich przetwarzania oraz przestrzegać wiążących zasad w tym zakresie. Przeszkolenie zapewnia komórka, do której regulaminowych zadań należy przeprowadzanie doskonalenia zawodowego w powyższym zakresie – odpowiednio w KGP/KWP/KSP.

W odniesieniu do policyjnych zbiorów danych osobowych prowadzonych w formie tradycyjnej, a więc manualnych (prowadzonych w postaci dokumentacji papierowej), zastosowanie mają zasady ogólne. Każda osoba przetwarzająca dane jest zobowiązana do przechowywania dokumentów poza zasięgiem wzroku osób trzecich, niepozostawiania dokumentów w drukarkach, nieprzekazywania ich osobom nieuprawnionym, utylizowania materiałów niepotrzebnych za pomocą niszczarki. Jeśli ich zniszczenie jest niedopuszczalne, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

Przetwarzanie danych osobowych w systemie informatycznym wiąże się z koniecznością przestrzegania wielu przyjętych w Policji standardów odnoszących się do użytkowania Policyjnej Sieci Transmisji Danych, m.in. procedury nadawania uprawnień oraz zapewnienia rozliczalności prowadzonych operacji przetwarzania, czyli stosowania obowiązujących w Policji mechanizmów zapewniających monitoring podejmowanych działań. Chodzi zatem o to, aby każdą osobę przetwarzającą dane można było rozliczyć z tego, do czego ma dostęp, w jakim celu korzysta z tych danych i czy w ogóle powinna mieć do nich dostęp. Administrator danych musi zatem kontrolować, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone oraz komu są przekazywane. Stąd też zastosowanie mają ogólne zasady dotyczące zapewnienia standardów, w większości przypadków możliwie wysokiego poziomu bezpieczeństwa w zakresie przydzielania indywidualnych identyfikatorów, uwierzytelniania przy wykorzystaniu kart mikroprocesorowych z wprowadzaniem kodów PIN bądź nazw użytkownika (loginów) oraz haseł (w tym ogólnych zasad co do polityki haseł wraz z zobowiązaniem do poufności w zakresie szczegółów uwierzytelniania), zasad dotyczących użytkowania komputerów przenośnych, czy też bezpiecznego postępowania z nośnikami danych, gdzie szczególną rolę odgrywają mechanizmy kryptografii, czyli szyfrowania danych. Należy w tym miejscu podkreślić, iż jednym z założeń standaryzacji jest, aby wszystkie rozwiązania systemu ochrony danych osobowych dla systemów informatycznych były zgodne z podstawowymi standardami bezpieczeństwa teleinformatycznego, w tym z normami Polskiego Komitetu Normalizacyjnego.

Nie można też pominąć generalnych standardów ochrony fizycznej obiektów i pomieszczeń Policji, w których odbywa się przetwarzanie danych osobowych. Do technicznych środków ochrony należą ogrodzenia, mury, kraty, zamki, system kontroli dostępu, system sygnalizacji alarmu włamania i napadu, system kontroli wejść i wyjść zarówno uprawnionych funkcjonariuszy, jak i personelu cywilnego oraz gości, osobową ochroną obiektów w postaci służb wartowniczych i patrolowych, przepustki na teren obiektów Policji etc.

Odrębnym zagadnieniem jest też kwestia rejestracji policyjnych zbiorów danych osobowych w rejestrze prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych. Kierownicy jednostek organizacyjnych Policji w zakresie, w jakim przetwarzają dane osobowe w zbiorach, podlegają – analogicznie do każdego innego administratora danych – ogólnym przepisom dotyczącym rejestracji takich zbiorów. Organ Policji – jako administrator danych, dokonując analizy obowiązku rejestracyjnego, powinien zawsze mieć na uwadze wyłączenia przewidziane w tym zakresie w ustawie oraz łączącą się z powyższym zagadnieniem odpowiedzialność. Standary-

## Inwentaryzacja dokumentów niejawnych

zacja ochrony danych osobowych w Policji ma – jak wynika z powyższego – wiele aspektów. Należy ją przy tym postrzegać nie tylko jako pewien stan faktyczny, dotyczący jednakowych, powtarzalnych działań funkcjonariuszy i pracowników formacji mających do czynienia z przetwarzaniem danych osobowych, lecz także jako ciągły proces, wynikający z nie-

ustannego postępu technologicznego (coraz więcej zagrożeń, coraz skuteczniejsze sposoby zabezpieczeń) oraz zmieniającego się otoczenia prawnego.

*Anna Ankiewicz*

*główny specjalista Wydziału Bezpieczeństwa Teleinformatycznego  
Gabinetu KGP*

## INWENTARYZACJA DOKUMENTÓW NIEJAWNYCH W KGP

**I**nwentaryzacja dokumentów niejawnych ma na celu porównanie stanu faktycznego dokumentacji niejawnej ze stanem ewidencyjnym w urządzeniach ewidencyjnych (tzn. dzienniki ewidencji, rejestr wydanych przedmiotów) prowadzonych w kancelarii tajnej. Każda informacja niejawna, bez względu na dokonane w niej modyfikacje (skreślenia, adnotacje itp.) dotyczące zmiany statusu klauzuli tajności, podlega rozliczeniu w kancelarii tajnej.

Osoby zatrudnione w Komendzie Głównej Policji powinny znać przepisy o ochronie informacji niejawnych oraz zasady obiegu dokumentów zawierających takie informacje. Dlatego też kontrola ewidencji materiałów niejawnych odbywa się corocznie w pierwszym kwartale roku w każdej jednostce organizacyjnej Policji. W tym celu kierownik jednostki organizacyjnej lub pełnomocnik ochrony powołuje komisję do spraw inwentaryzacji materiałów niejawnych. W skład takiej komisji nie powinny wchodzić osoby prowadzące urządzenia ewidencyjne jednostki lub komórki organizacyjnej, w której odbywa się inwentaryzacja.

W związku z powyższym przewodniczący komisji inwentaryzacyjnej przesyła wzór karty inwentaryzacyjnej. Funkcjonariusze i pracownicy Policji sporządzają wykaz materiałów niejawnych (karta inwentaryzacyjna) pozostających w ich dyspozycji (tzw. spis z natury). Karta inwentaryzacyjna zostaje podpisana przez osobę sporządzającą wykaz oraz bezpośredniego przełożonego, a następnie przekazana komisji inwentaryzacyjnej, która dokonuje porównania zapisów sporządzonych przez policjantów i pracowników Policji z wykazami w urządzeniach ewidencyjnych prowadzonych przez kancelarie tajne. Zdarzają się przypadki, iż dokumenty wskazane w kartach inwentaryzacyjnych funkcjonariuszy i pracowników Policji nie zawsze są zgodne z zapisami w urządzeniach ewidencyjnych. Świadczy to o niezgodnej z przepisami praktyce wzajemnego przekazywania dokumentów, z pominięciem ewidencji w kancelarii tajnej. Aby wyeliminować takie nieprawidłowości, należy przypominać policjantom i pracownikom o zasadach regulujących obieg dokumentów niejawnych oraz o sposobie postępowania w nimi, a także szkolić ich w tym zakresie.

Priorytetem komisji jest sprawdzenie, czy w dyspozycji policjantów i pracowników Policji znajdują się materiały niejawne niebędące na ich stanie ewidencyjnym. Ponadto komisja inwentaryzacyjna porównuje zapisy w dzienniku ewidencji dotyczące liczby egzemplarzy, liczby stron dokumentu lub innych jednostek miary oraz liczbę załączników przesłanych pismem przewodnim. Porównuje także zgodność i spójność zapisów w dziennikach ewidencyjnych z zapisami w kartach inwentaryzacyjnych. W przypadku stwierdzenia niezgodności zapisów komisja podejmuje czynności w celu wyjaśnienia przyczyn zaistniałych rozbieżności między jednostką organizacyjną Policji a kancelarią tajną.

Po zakończeniu czynności inwentaryzacyjnych komisja sporządza protokół, który powinien w szczególności zawierać informacje dotyczące zgodności stanu ewidencyjnego materiałów ze stanem faktycznym, liczbę materiałów objętych inwentaryzacją, odrębnie dla każdej klauzuli tajności, a także informację o stwierdzonych nieprawidłowościach i podjętych w związku z tym czynnościach. Następnie jeden egzemplarz protokołu komisja przekazuje pełnomocnikowi ochrony, który sporządza sprawozdanie z przeprowadzonych w jednostce organizacyjnej Policji czynności inwentaryzacyjnych i do 31 maja każdego roku przedkłada kierownikowi jednostki organizacyjnej do zatwierdzenia.

Zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), za zorganizowanie i zapewnienie funkcjonowania tej ochrony odpowiada kierownik jednostki organizacyjnej, w której takie informacje są przetwarzane. Natomiast pełnomocnik ochrony odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. Obydwaj nie ponoszą bezpośredniej odpowiedzialności za świadome lub nieświadome naruszenia przepisów przez poszczególnych policjantów i pracowników Policji. Odpowiedzialność spoczywa na każdym, wobec kogo przeprowadzono postępowanie sprawdzające i kto wszedł w posiadanie informacji niejawnych, niezależnie od tego, czy nastąpiło to w sposób uprawniony, czy też przypadkowo.

Jak stanowi art. 17 ust. 1 ustawy o ochronie informacji niejawnych: „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”.

Funkcjonariusz lub pracownik, który dopuścił się ujawnienia informacji niejawnych, niezależnie od odpowiedzialności karnej, podlega również odpowiedzialności dyscyplinarnej. Nie każde jednak przewinienie służbowe jest przestępstwem, postępowanie dyscyplinarne może być zatem prowadzone samoistnie i zakończyć się wymierzeniem jednej z kar dyscyplinarnych.

Coroczna kontrola ochrony informacji niejawnych jest bardzo istotna, ponieważ pozwala zredukować liczbę naruszeń wynikających często z niesystematycznego rozliczania się z dokumentów niejawnych dotyczących spraw ostatecznie zakończonych. Nierozliczanie się z dokumentów niejawnych na bieżąco przez wszystkich policjantów i pracowników powoduje dezorganizację pracy kancelarii tajnej oraz zbyt duże gromadzenie dzienników ewidencji z lat ubiegłych, zajmujących bardzo dużo miejsca w szafach i pomieszczeniach kancelarii tajnej.

*Beata Biesiadecka*

*kierownik Kancelarii Tajnej Gabinetu KGP*

# ROLA GŁÓWNEGO ARCHIWUM POLICJI W KSZTAŁTOWANIU POLICYJNEGO ZASOBU ARCHIWALNEGO

**G**łówne Archiwum Policji jest centralnym archiwum formacji, bezpośrednio nadzorowanym przez Komendanta Głównego Policji. Jego początki sięgają kwietnia 1991 r., kiedy to po okresie dynamicznego przejmowania zasobu archiwalnego byłego Ministerstwa Spraw Wewnętrznych w strukturach Komendy Głównej Policji postanowiono powołać instytucję archiwalną. Główne zadanie komórki stanowiło kształtowanie polityki archiwalnej Policji w skali całego kraju, jak również nadzór nad działalnością archiwów i składnic akt w ramach całej formacji. Nie bez znaczenia była jednocześnie konieczność zorganizowania i prowadzenia bieżącego archiwum zakładowego Komendy Głównej Policji.

W pierwszych latach funkcjonowania zasób Głównego Archiwum Policji stanowiły akta wytworzone w komórkach organizacyjnych byłej Komendy Głównej Milicji Obywatelskiej, takich jak Biuro Operacyjne, Biuro Dochodzeniowo-Śledcze oraz Zakład Kryminalistyki. W tamtym czasie w zbiorach Głównego Archiwum Policji znalazły się dokumenty dotyczące powstania Milicji Obywatelskiej czy też pełna dokumentacja najciekawszych spraw kryminalnych z okresu PRL, takich jak sprawa o kryptonimie „ANNA” dotycząca ścigania sprawcy brutalnych morderstw kobiet (m.in. bratanicy Edwarda Gierka).

Drugim filarem tworzenia zasobu Głównego Archiwum Policji od początku funkcjonowania – oprócz przejmowania dokumentów o proveniencji milicyjnej – jest gromadzenie dokumentów wytworzonych we wszystkich komórkach organizacyjnych Komendy Głównej Policji. Do dzisiaj Główne Archiwum Policji konsekwentnie gromadzi i przechowuje akta centrali Policji, poczynając od spraw typowo administracyjnych, a kończąc na aktach operacyjnych. To właśnie Główne Archiwum Policji jest miejscem gromadzenia akt m.in. Centralnego Biura Śledczego czy też Biura Spraw Wewnętrznych.

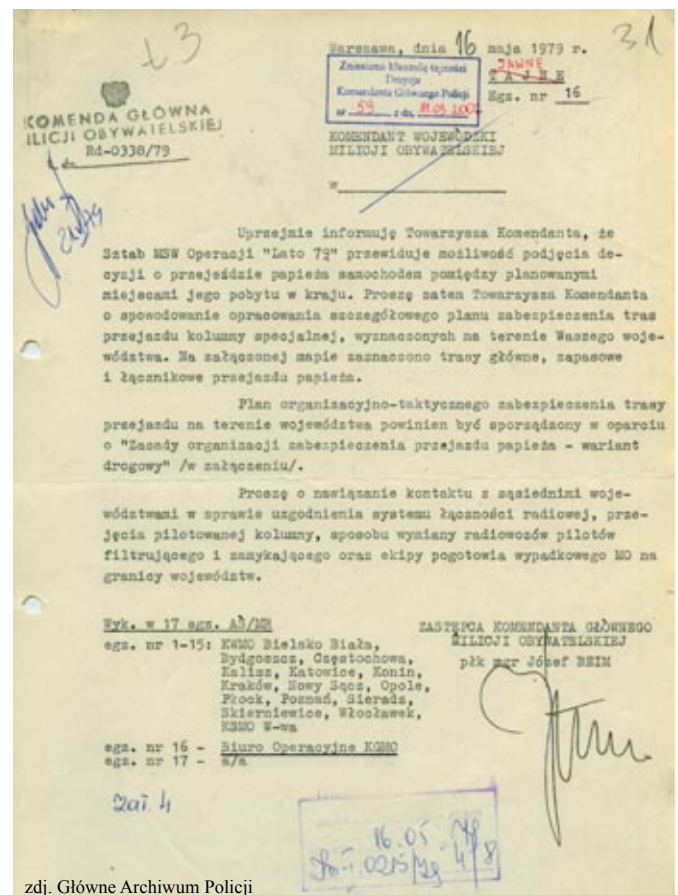
W archiwum Komendy Głównej Policji obecnie są przechowywane dokumenty z ostatnich 60 lat. Jest to spowodowane koniecznością wypełnienia dyspozycji ustawy z dnia 18 grudnia 1998 r. o Instytucji Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (Dz. U. z 2007 r. Nr 63, poz. 424, z późn. zm.), która nałożyła na Policję konieczność przekazania do tej instytucji wszelkiej dokumentacji wytworzonej do grudnia 1954 r. To właśnie blisko 15 lat temu zapoczątkowano proces, który zobligował Policję do przekazania ogromnej części własnego zasobu do Instytutu Pamięci Narodowej. Z oficjalnych danych wynika, iż obecny zasób archiwalny IPN-u w ponad 50% jest złożony z dokumentów przekazanych przez Policję.

Główne Archiwum Policji, wypełniając wymogi ustawowe, zostało zobowiązane do przekazania do IPN-u dokumentów dotyczących powstania Milicji Obywatelskiej i jej funkcjonowania w pierwszym dziesięcioleciu istnienia czy też zwalczania podziemia niepodległościowego i opozycji antykomunistycznej w ramach udzielania pomocy Służbie Bezpieczeństwa PRL. Wtedy na przykład przekazano dokumentację filmową

wieczu, który odbył się na Politechnice Warszawskiej w 1968 r. Obecnie w Głównym Archiwum Policji trwa proces przeglądu dokumentów archiwalnych wytworzonych i zgromadzonych od 15 grudnia 1954 r. do 31 lipca 1990 r., realizowany przez upoważnionych przedstawicieli IPN-u.

W tym kontekście warto wspomnieć o działaniach zainicjowanych w ostatnich latach przez Główne Archiwum Policji, które zostały zwieńczone zawarciem porozumienia Komendanta Głównego Policji i Prezesa Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu z dnia 8 lutego 2013 r. w sprawie określenia zasad współdziałania w zakresie działalności archiwalnej Policji i Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu. W skali całego kraju – uwzględniając Wojsko Polskie, jak również służby specjalne – jest to właściwie jedyny akt prawny regulujący w sposób kompleksowy zasady współpracy z IPN-em.

Obecnie wielkość zasobu Głównego Archiwum Policji sięga blisko 6 kilometrów bieżących akt. Znajduje się w nim m.in. całość dokumentacji papierowej Centralnej Kartoteki Kryminalnej, która była poprzedniczką funkcjonującego obecnie w wersji elektronicznej Krajowego Systemu Informatycznego Policji.



zdj. Główne Archiwum Policji



## Główne Archiwum Policji

Zgromadzony w Głównym Archiwum Policji zasób jest podstawą do prowadzenia poszukiwań – kwerend archiwalnych, które skutkowały następnie udostępnieniem materiałów archiwalnych. Do najciekawszych tego typu działań przeprowadzonych w ostatnich latach należały m.in.:

- 1) udostępnienie dla redakcji „SUPERWIZJERA” TVN akt pierwszej pielgrzymki papieża Jana Pawła II do Polski, która odbyła się w 1979 r. (dokumentacja dotycząca zabezpieczenia porządku i bezpieczeństwa w ramach operacji „LATO-79”),
- 2) kompleksowa kwerenda realizowana we współpracy z Biurem Służby Kryminalnej oraz Centralnym Laboratorium Kryminalistycznym Policji na temat zarchiwizowanych akt identyfikacji NN zwłok, mających na celu dalsze działania związane z identyfikacją profilu DNA,
- 3) kwerenda i udostępnienie do projektu badawczego pn. „Systemowe i strukturalne uwarunkowania funkcjonowania pionu dzielnicowych w Polsce – wnioski dla praktyki”, w ramach którego dokonano poszukiwań dokumentów wytworzonych przez cały okres funkcjonowania Milicji Obywatelskiej i Policji do chwili obecnej,
- 4) kwerenda i udostępnienie do badań naukowych na temat służby ruchu drogowego Milicji Obywatelskiej i Policji w garnizonie stołecznym w latach 1945–2000 r.,
- 5) udostępnienie materiałów do publikacji naukowej pt. „Aparat represji wobec księdza Jerzego Popiełuszki”.

Ponadto gros materiałów zgromadzonych w zasobie Głównego Archiwum Policji posiada znaczenie historyczne, np. akta zabezpieczenia prewencyjnego wizyt apostolskich papieża Jana Pawła II w Polsce z lat 80. ubiegłego wieku, dokumentacja filmowa byłego Zakładu Kryminalistyki Komendy Głównej Milicji Obywatelskiej oraz ostatnio pozyskana dokumentacja dotycząca przebiegu i zabezpieczenia przez Policję Turnieju Finałowego Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012.

W dobie kształtowania się społeczeństwa informacyjnego i postępującej cyfryzacji administracji państwowej Główne Archiwum Policji w ostatnim okresie rozpoczęło długofalowy proces digitalizacji posiadanych materiałów archiwalnych. Mając na względzie przenoszenie zapisów z tradycyjnych nośników do postaci elektronicznej, w archiwum Komendy Głównej Policji utworzono pracownię digitalizacyjną wyposażoną w profesjonalny sprzęt informatyczny, przeznaczony zarówno do cyfrowej archiwizacji materiałów papierowych, jak i fotografii, klisz czy negatywów. Do chwili obecnej wykonano blisko 70 tys. odwzorowań cyfrowych. Należy przy tym podkreślić, iż całość procesu digitalizacji materiałów archiwalnych została przeprowadzona we współpracy z Narodowym Archiwum Cyfrowym w Warszawie, które stanowi Centrum Kompetencji ds. Digitalizacji Ministerstwa Kultury i Dziedzictwa Narodowego.

Oprócz prowadzenia współpracy z Narodowym Archiwum Cyfrowym i Instytutem Pamięci Narodowej – Komisją Ścigania Zbrodni przeciwko Narodowi Polskiemu, Główne Archiwum Policji rozwija kontakty z Centralnym Archiwum Wojskowym im. mjr. Bolesława Waligóry w Warszawie – Rembertowie oraz z Archiwum Agencji Bezpieczeństwa Wewnętrznego. Celem współpracy z wymienionymi instytucjami jest nie tylko rozwój archiwistyki policyjnej, ale także poszerzenie wiedzy i doświadczeń w zakresie działalności archiwalnej.

Główne Archiwum Policji – w ramach działu administracji rządowej sprawy wewnętrzne – jest najbardziej aktywną instytu-



zdj. Główne Archiwum Policji

cją biorącą udział w nowelizacji ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2011 r. Nr 123, poz. 698 i Nr 171, poz. 1016). Ponadto prowadzi intensywne działania związane z tworzeniem nowych aktów prawnych związanych z zarządzaniem i archiwizacją dokumentacji, zarówno w postaci papierowej, jak i elektronicznej. Jest to o tyle istotne, iż Policja stoi przed wyzwaniem przejścia do systemu Elektronicznego Zarządzania Dokumentacją.

*Piotr Borysiuk*  
referendarz Sekcji Główne Archiwum Policji Gabinetu KGP

### Akty prawne

Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2011 r. Nr 123, poz. 698 i Nr 171, poz. 1016).

Ustawa z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (Dz. U. z 2007 r. Nr 63, poz. 424, z późn. zm.).

Rozporządzenie Rady Ministrów z dnia 22 czerwca 2011 r. w sprawie i trybu udostępniania materiałów archiwalnych znajdujących się w archiwach wyodrębnionych (Dz. U. nr 196, poz. 1161).

Zarządzenie nr 93 Ministra Spraw Wewnętrznych i Administracji z dnia 17 grudnia 2007 r. w sprawie jednolitego rzeczowego wykazu akt Policji (Dz. Urz. MSWiA z 2008 r. Nr 1, poz. 1), zmienione zarządzeniem nr 53 Ministra Spraw Wewnętrznych z dnia 28 sierpnia 2012 r. zmieniającym zarządzenie w sprawie jednolitego rzeczowego wykazu akt Policji (Dz. Urz. MSW poz. 58).

Zarządzenie nr 45 Ministra Spraw Wewnętrznych i Administracji z dnia 20 maja 2008 r. w sprawie postępowania z materiałami archiwalnymi i dokumentacją niearchiwalną w archiwach wyodrębnionych podległych Ministrowi Spraw Wewnętrznych i Administracji lub przez niego nadzorowanych (Dz. Urz. MSWiA Nr 9, poz. 42).

Zarządzenie nr 920 Komendanta Głównego Policji z dnia 11 września 2008 r. w sprawie metod i form wykonywania zadań w zakresie działalności archiwalnej w Policji (Dz. Urz. KGP Nr 16, poz. 95).