Warszawa, dnia 6 kwietnia 2013 r.

Poz. 29

DECYZJA NR 126
KOMENDANTA GŁÓWNEGO POLICJI

z dnia 5 kwietnia 2013 r.

w sprawie prowadzenia w Policji zestawu zbiorów danych „System Informacji Operacyjnych”

Na podstawie § 6 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych z dnia 31 grudnia 2012 r. w sprawie przetwarzania informacji przez Policję (Dz. U. z 2013 r. poz. 8) postanawia się, co następuje:

§ 1. Decyzja określa:

1) cel prowadzenia zestawu zbiorów danych;

2) zakres informacyjny, rzeczowy i terytorialny informacji przetwarzanych w zestawie zbiorów danych;

3) podmioty odpowiedzialne za prowadzenie zestawu zbiorów danych;

4) podmioty uprawnione do korzystania z zestawu zbiorów danych;

5) procedury nadawania, zmiany, odbierania uprawnień osobom uprawnionym do przetwarzania danych w zestawie zbiorów danych;

6) strukturę zestawu zbioru danych oraz procedury przetwarzania informacji w nim zgromadzonych;

7) techniczne i organizacyjne warunki wykonywania czynności służbowych niezbędnych do realizacji ustalonego celu prowadzenia zestawu zbioru danych oraz zapewniających zgodne z prawem efektywne przetwarzanie informacji w nim zgromadzonych, w realizacji ustawowych zadań Policji.

§ 2. Użyte w decyzji określenia oznaczają:

1) SIO – zestaw zbiorów danych o nazwie „System Informacji Operacyjnych”;

2) SMI – zbiór danych o nazwie „System Meldunku Informacyjnego”;

3) CBIU – zbiór danych o nazwie „Centralna Baza Informacji z Ustaleń”;

4) MWD – Moduł Wprowadzania Danych będący funkcjonalnością zestawu zbioru danych SIO poprzez który wprowadza się informacje do SIO;

5) ustawa o Policji – ustawę z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, z późn. zm.[1)]);

6) ustawa o ochronie danych osobowych – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.[2)]);

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2011 r. Nr 217, poz. 1280 i Nr 230, poz. 1371 oraz z 2012 r. poz. 627, 664, 908, 951 i 1529.

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238, z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228 i Nr 229, poz. 1497 oraz z 2011 r. Nr 230, poz. 1371.

7) ustawa o ochronie informacji niejawnych – ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228);

8) rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych z dnia 31 grudnia 2012 r. w sprawie przetwarzania informacji przez Policję;

9) zarządzenie – zarządzenie nr pf–634 Komendanta Głównego Policji z dnia 30 czerwca 2006 r. w sprawie metod i form wykonywania przez Policję czynności operacyjno-rozpoznawczych zmienione zarządzeniami nr pf-1292 z dnia 19 grudnia 2008 r. oraz nr pf-671 z 7 czerwca 2011 r.;

10) dyrektor biura KGP – dyrektor biura Komendy Głównej Policji lub kierownik równorzędnej komórki organizacyjnej Komendy Głównej Policji;

11) Centralny Administrator Merytoryczny SIO – policjant lub pracownik Policji odpowiedzialny za kontrolę i nadzór nad jakością i aktualnością informacji przetwarzanych w SIO, pisemnie upoważniony w tym zakresie przez dyrektora biura KGP właściwego w sprawach wywiadu kryminalnego;

12) podmioty uprawnione – komórki organizacyjne służby kryminalnej i śledczej Policji oraz podmioty pozapolicyjne, które mogą uzyskiwać dane z SIO na podstawie odrębnych przepisów;

13) dokument – dokument źródłowy zawierający informacje podlegające wprowadzeniu do SIO;

14) komunikat systemowy – komunikat generowany automatycznie, zawierający dane policjanta zlecającego ochronę informacji wprowadzonej do zestawu zbiorów danych SIO.

§ 3. 1. W biurze KGP właściwym w sprawach wywiadu kryminalnego prowadzi się w systemie teleinformatycznym, obejmujący terytorium całego kraju, zestaw zbiorów danych SIO.

2. SIO składa się ze zbiorów:

1) SMI, utworzonego z dniem 1 czerwca 2004 r.[3)] ;

2) CBIU, utworzonego z dniem 20 kwietnia 2007 r.[4)] ;

3) zbioru danych ARCHIWUM, utworzonego z dniem 1 czerwca 2004 r. i przekształconego z dniem 20 kwietnia 2007 r. w drodze wyodrębnienia ze zbiorów wymienionych w pkt. 1 i 2.

3. SMI i CBIU są przeznaczone do gromadzenia informacji wykorzystywanych przez służbę kryminalną i śledczą Policji podczas wykonywania czynności operacyjno-rozpoznawczych, a także do sprawdzania miejsc podczas wykonywania czynności dochodzeniowo-śledczych.

4. Zbiór danych ARCHIWUM jest przeznaczony do weryfikacji informacji przetwarzanych w SMI i CBIU, prowadzonej w celu usuwania informacji uznanych za nieprzydatne do realizacji ustawowych zadań Policji.

§ 4. 1. W SIO przetwarza się informacje uzyskane przez policjantów w trakcie wykonywania czynności służbowych, przydatne do zapobiegania, rozpoznawania, ujawniania i wykrywania przestępstw, ustalania metod ich popełniania oraz wykrywania i zatrzymywania sprawców, w tym także:

1) informacje o zdarzeniach, miejscach, pojazdach, dokumentach oraz osobach fizycznych i innych podmiotach nie będących osobami fizycznymi;

2) informacje o telekomunikacyjnych urządzeniach końcowych, wykorzystywanych do przekazu informacji, z wyłączeniem danych pozyskanych w trybie określonym w art. 20c ustawy o Policji;

3) informacje o rachunkach w bankach lub innych instytucjach finansowych oraz o czynnościach bankowych, z zastrzeżeniem ograniczeń dostępu do tych informacji określonych w art. 20 ust. 3 i 4 ustawy o Policji.

2. Do przetwarzania informacji w SIO stosuje się system teleinformatyczny opatrzony świadectwem akredytacji bezpieczeństwa teleinformatycznego, w trybie określonym w przepisach o ochronie informacji niejawnych.

[3)] Wymieniony zbiór został utworzony na podstawie decyzji nr 192 Komendanta Głównego Policji z dnia 26 maja 2004 r. w sprawie założenia oraz zasad prowadzenia centralnego zbioru informacji dla potrzeb analizy kryminalnej (Dz. Urz. KGP Nr 10, poz. 51).

[4)] Wymieniony zbiór został utworzony na podstawie decyzji nr 256 Komendanta Głównego Policji z dnia 13 kwietnia 2007 r. w sprawie założenia i prowadzenia na potrzeby Policji centralnego zbioru Systemu Informacji Operacyjnych (Dz. Urz. Nr 8, poz. 69 i Nr 13, poz. 103).

§ 5. 1. Informacje w poszczególnych zbiorach, wymienionych w § 3 ust. 2 pkt 1 i 2 wprowadza się na podstawie dokumentów:

1) meldunek informacyjny, sporządzony według wzoru określonego w załączniku nr 1 do decyzji;

2) zapytanie/typowanie, sporządzone według wzoru określonego w załączniku nr 2 do decyzji;

3) wniosek o obserwację i komunikat z obserwacji, o których mowa w § 66 ust. 1 i § 75 ust. 1 pkt 1 zarządzenia;

4) innego dokumentu wytworzonego w Policji oraz poza Policją, zawierającego dane przydatne do realizacji celów określonych w § 4 ust. 1.

2. Meldunek informacyjny sporządza się w każdym przypadku uzyskania przez policjanta informacji mogącej przyczynić się do osiągnięcia celów określonych w § 4 ust. 1.

§ 6. 1. Informacje do SIO wprowadzane są poprzez aplikację MWD lub ze stanowisk dostępowych do SIO.

2. Szczegółowy obieg dokumentów wprowadzanych za pomocą MWD jest określony w Procedurach Bezpiecznej Eksploatacji SIO.

§ 7. 1. Policjant sporządzający dokument zawierający informacje podlegające wprowadzeniu do SIO:

1) jest odpowiedzialny za rzetelne i kompletne podanie uzyskanych informacji;

2) jest obowiązany zweryfikować uzyskane informacje w dostępnych policyjnych i pozapolicyjnych zbiorach informacji, a wynik tej weryfikacji umieścić w treści dokumentu źródłowego.

2. Przed rejestracją w SIO dokument źródłowy musi być sprawdzony i zatwierdzony pod względem formalnym i merytorycznym przez właściwego:

1) kierownika komórki organizacyjnej Komendy Głównej Policji,

2) kierownika komórki organizacyjnej komendy wojewódzkiej (Stołecznej) Policji,

3) komendanta powiatowego (miejskiego, rejonowego) Policji oraz komendanta komisariatu Policji, komisariatu specjalistycznego Policji

– zwanych dalej „komendantami i kierownikami”.

3. Komendanci i kierownicy mogą upoważnić na piśmie podległych policjantów do wykonywania czynności, o których mowa w ust. 2.

4. Policjant sporządzający dokument jest obowiązany, z zastrzeżeniem ust. 2, niezwłocznie po wykonaniu czynności służbowych wynikających z charakteru tego dokumentu, przekazać go:

1) komórce organizacyjnej właściwej do spraw wywiadu kryminalnego – w przypadku dokumentu, o którym mowa w § 5 ust.1 pkt 1, 2 i 4;

2) komórce organizacyjnej właściwej do spraw techniki operacyjnej – w przypadku dokumentu, o którym mowa w § 5 ust.1 pkt 2 i 3;

3) innej, właściwej rzeczowo komórce organizacyjnej uprawnionej do wprowadzania informacji do SIO – w przypadku dokumentu, o którym mowa w § 5 ust.1 pkt 1, 2 i 4.

§ 8. 1. Dokument zawierający informacje o policjancie lub pracowniku Policji przekazuje się, bez wprowadzania do SIO, do właściwej miejscowo komórki organizacyjnej Policji właściwej w sprawach wewnętrznych. O wprowadzeniu tej informacji do SIO decyduje kierownik wymienionej komórki organizacyjnej bądź upoważniony przez niego policjant.

2. Informacje, o których mowa w ust. 1, udostępnia się uprawnionym podmiotom za zgodą dyrektora biura KGP właściwego w sprawach wewnętrznych.

§ 9. Policjant sporządzający meldunek informacyjny dokonuje oceny wiarygodności źródła informacji, a wyniki tej oceny zaznacza w odpowiednich polach formularza meldunku w formie następujących kodów:

1) kod „A” – oznacza brak wątpliwości co do wiarygodności źródła informacji;

2) kod „B” – oznacza, że informacja pochodzi ze źródła, które w większości przypadków dotychczas było wiarygodne;

3) kod „C” – oznacza, że informacja pochodzi ze źródła, które w większości przypadków dotychczas nie było wiarygodne;

4) kod „X” – oznacza, że informacja pochodzi z nowego źródła, którego wiarygodność nie jest znana, bo źródło nie było sprawdzane lub sprawdzenie nie jest możliwe.

§ 10. Policjant sporządzający meldunek informacyjny dokonuje oceny prawdziwości i sposobu uzyskania informacji przekazywanej tym meldunkiem, a wyniki tej oceny wpisuje w odpowiednim polu formularza meldunku w formie następujących kodów:

1) kod „l” – oznacza, że informacja jest oceniana jako prawdziwa przez policjanta;

2) kod „2” – oznacza, że fakty wskazane w informacji są znane bezpośrednio źródłu przekazującemu informację;

3) kod „3” – oznacza, że fakty wskazane w informacji nie są znane bezpośrednio źródłu przekazującemu informację, ale zostały potwierdzone przez inne źródła informacji;

4) kod „4” – oznacza, że fakty wskazane w informacji nie są znane bezpośrednio źródłu przekazującemu informację i nie mogą być sprawdzone przez inne aktualnie dostępne źródła informacji.

§ 11. 1. Policjant sporządzający dokument, o którym mowa w § 5 ust. 1 pkt 1 i 2 lub jego bezpośredni przełożony określa w odpowiednim polu formularza dokumentu dopuszczalny sposób wykorzystania informacji, w formie następujących kodów:

1) kod „H1” – oznacza, że informacja nie może być wykorzystana w postępowaniu karnym bezpośrednio, bez uprzedniego dowodowego przetworzenia w sposób określony przepisami postępowania karnego;

2) kod „H2” – oznacza, że informacje można udostępnić tylko po uprzednim uzyskaniu zgody policjanta, który sporządził dokument lub jego bezpośredniego przełożonego;

3) kod „H3” – oznacza, że wykorzystanie informacji podlega ograniczeniom innym niż wymienione w pkt 1 i 2, wskazanym opisowo w polu „Uwagi” formularza dokumentu;

2. Kod „H1” wpisuje się do każdego dokumentu wprowadzanego do SIO, a kody „H2” i „H3” dodatkowo w przypadku uznania, że zachodzą określone powody do dalej idącego ograniczenia sposobu wykorzystania informacji, przy czym kod „H2” wpisuje się zawsze do dokumentów, o których mowa w § 5 ust. 1 pkt 3.

3. W przypadku przekazania lub przejęcia dokumentów objętych ochroną, o której mowa w ust. 1 i 2, decyzję o sposobie wykorzystania podejmuje funkcjonariusz przejmujący lub jego przełożony.

4. Sposób wykorzystania informacji ogranicza się kodem „H2” w przypadku konieczności szczególnej ochrony przebiegu prowadzonych czynności operacyjno-rozpoznawczych przed dekonspiracją, zapewnienia właściwego toku postępowania karnego albo ochrony zdrowia i życia policjantów lub innych osób uczestniczących w czynnościach służbowych.

5. Ograniczenie sposobu wykorzystania informacji kodem „H2” lub „H3” obowiązuje przez okres trzech miesięcy od daty wprowadzenia dokumentu do SIO. Okres ten może być przedłużany o kolejne trzymiesięczne okresy na pisemny wniosek kierownika komórki organizacyjnej Policji skierowany do komórki organizacyjnej właściwej do spraw wywiadu kryminalnego lub techniki operacyjnej.

6. W przypadku braku zgody, o której mowa w ust. 1 pkt 2, podmiot dokonujący sprawdzenia w SIO otrzymuje tylko informacje występujące w komunikacie systemowym.

§ 12. 1. Po wprowadzeniu informacji do SIO dokumenty, o których mowa w § 5 ust. 1 pkt 1 i 2, są zwracane sporządzającemu z adnotacją określającą datę wprowadzenia i numer identyfikacyjny nadany w SIO.

2. Kierownik komórki organizacyjnej właściwej w sprawach wywiadu kryminalnego w KGP, komendzie wojewódzkiej (Stołecznej) Policji albo policjant lub pracownik Policji upoważniony w tym zakresie, zwraca sporządzającemu dokument bez wprowadzenia do SIO jeżeli:

1) dokument został sporządzony niezgodnie z przepisami o ochronie informacji niejawnych;

2) informacje zawarte w dokumencie są powszechnie znane lub nieprzydatne w realizacji zadań ustawowych Policji;

3) dokument został wypełniony nieprawidłowo lub nieczytelnie;

4) dokument zawiera informacje, których przetwarzanie jest zabronione.

§ 13. 1. Na podstawie informacji zawartych w dokumentach, o których mowa w § 5 ust. 1, w SIO można tworzyć obiekty analityczne, z opisem ich wzajemnych powiązań:

1) „Adres" – informacje o miejscach;

2) „Dokument" – informacje o dokumentach;

3) „Firma" – informacje o podmiotach, które nie są osobami fizycznymi;

4) „Grupa" – informacje o grupach przestępczych, a w szczególności o ich charakterze, celach i obszarach działania oraz zachowaniach członków;

5) „Konto" – informacje o rachunkach w bankach lub innych instytucjach finansowych oraz o czynnościach bankowych;

6) „Osoba" – informacje o osobach fizycznych;

7) „Pojazd" – informacje o pojazdach oraz ich częściach składowych;

8) „Telefon" – informacje o numerach i abonentach telefonów, urządzeń telekopiowych, adresach (kontach) poczty elektronicznej lub innych adresach albo numerach urządzeń wykorzystywanych do przekazu informacji;

9) „Zdarzenie" – informacje o zdarzeniach oraz ich umiejscowieniu czasowym i terytorialnym.

2. Jeżeli treść dokumentu zawiera wszystkie informacje pozwalające na utworzenie obiektu analitycznego, utworzenie obiektu analitycznego jest obowiązkowe.

§ 14. 1. Dokumenty, o których mowa w § 5 ust. 1 pkt 1, grupuje się w podzbiorach tematycznych dotyczących poszczególnych czynów karalnych, metod działań przestępczych, grup przestępczych oraz innych zagadnień, uznanych za istotne w zakresie realizacji ustawowych zadań Policji. Każdy podzbiór tematyczny oznacza się nazwą „Sprawa" z indywidualnym numerem, nazwą lub symbolem identyfikacyjnym.

2. Obiekty analityczne wymienione w § 13 można grupować w podzbiorach tematycznych dotyczących poszczególnych czynów karalnych, metod działań przestępczych, grup przestępczych oraz innych zagadnień, uznanych za istotne w zakresie realizacji ustawowych zadań Policji.

3. Podzbiór tematyczny tworzy i usuwa w drodze decyzji dyrektor biura KGP właściwego w sprawach wywiadu kryminalnego, z własnej inicjatywy lub:

1) na polecenie Komendanta Głównego Policji lub Zastępcy Komendanta Głównego Policji nadzorującego komórki organizacyjne służby kryminalnej i śledczej KGP;

2) na wniosek komendantów jednostek organizacyjnych Policji albo kierowników komórek organizacyjnych KGP.

4. W decyzji, o której mowa w ust. 3, dyrektor biura KGP właściwego w sprawach wywiadu kryminalnego określa szczegółowo rodzaj informacji przetwarzanych w podzbiorze tematycznym, kategorie użytkowników uprawnionych do dostępu i zakres dostępu oraz warunki korzystania z podzbioru i sposób usuwania informacji przetwarzanych w podzbiorze.

5. Dyrektor biura KGP właściwego w sprawach wywiadu kryminalnego może odmówić wydania decyzji, o której mowa w ust. 3 pkt 2, jeżeli uzna wniosek o utworzenie podzbioru tematycznego za nieuzasadniony albo wniosek o usunięcie dotyczy podzbioru tematycznego utworzonego na wniosek innego podmiotu. W takim przypadku zwraca wniosek wnioskodawcy ze wskazaniem przyczyn jego nieuwzględnienia.

6. Decyzja i odmowa wydania decyzji, o których mowa w ust. 3 pkt 2 i ust. 5, podlega zatwierdzeniu przez Zastępcę Komendanta Głównego Policji nadzorującego komórki organizacyjne służby kryminalnej i śledczej KGP.

§ 15. 1. Policjant prowadzący czynności operacyjno-rozpoznawcze w odniesieniu do któregokolwiek z wyodrębnionych obiektów analitycznych może złożyć wniosek o zastrzeżenie koordynacyjne, w wyniku którego powinien być powiadamiany o każdym wprowadzeniu informacji do SIO, mającej związek z obiektem analitycznym objętym zastrzeżeniem.

2. Policjant prowadzący czynności operacyjno-rozpoznawcze lub jego przełożony podejmuje decyzję co do sposobu wykorzystania powiadomienia, o którym mowa w ust. l.

3. Zastrzeżenie koordynacyjne obowiązuje przez okres 3 miesięcy od daty objęcia zastrzeżeniem obiektu analitycznego w SIO.

4. Można przedłużać okres zastrzeżenia koordynacyjnego o kolejne trzymiesięczne okresy, na pisemny wniosek skierowany do kierowników komórek organizacyjnych Policji właściwych do spraw wywiadu kryminalnego lub techniki operacyjnej.

5. Wzór wniosku o zastrzeżenie koordynacyjne/przedłużenie okresu zastrzeżenia koordynacyjnego w SIO określa załącznik nr 3 do decyzji.

§ 16. 1. Dyrektor biura KGP właściwego w sprawach wywiadu kryminalnego zapewnia prowadzenie systematycznej weryfikacji informacji przetwarzanych w SMI, pod względem ich prawidłowości oraz przydatności do realizacji celów wymienionych w § 3 ust. 3.

2. Dyrektor biura KGP właściwego w sprawach techniki operacyjnej zapewnia, w porozumieniu z dyrektorem biura KGP właściwego w sprawach wywiadu kryminalnego, prowadzenie systematycznej weryfikacji informacji przetwarzanych w CBIU pod względem ich prawidłowości oraz aktualnej przydatności do realizacji celów wymienionych w § 3 ust. 3.

3. Informacje przetwarzane w SIO podlegają okresowej weryfikacji, o której mowa w art. 20 ust. 17 ustawy o Policji oraz w § 32 rozporządzenia.

4. Informacje uznane w wyniku weryfikacji za zbędne do realizacji ustawowych zadań Policji usuwa się z SIO w sposób trwały i udokumentowany protokolarnie, zgodnie z § 34 rozporządzenia.

§ 17. Policjant sporządzający dokument, w przypadku zmiany klauzuli tajności, jest zobowiązany do poinformowania o tym właściwej miejscowo komórki wywiadu kryminalnego, celem naniesienia zmian w oznaczeniu informacji wprowadzonych do systemu.

§ 18. 1. Informacje wprowadzone na podstawie dokumentów do SIO mogą być modyfikowane przez uprawnionych użytkowników SIO w celu poprawienia oczywistej omyłki pisarskiej.

2. Błędy ujawnione w obiektach analitycznych mogą być poprawiane przez każdego uprawnionego użytkownika systemu.

§ 19. 1. Sprawdzenia w SIO można dokonać:

1) w przypadku prowadzenia czynności operacyjno-rozpoznawczych w odniesieniu do osób, miejsc lub innych obiektów analitycznych;

2) w ramach czynności dochodzeniowo-śledczych, określonych decyzją dyrektora biura KGP właściwego w sprawach wywiadu kryminalnego w odniesieniu do miejsc;

3) na polecenie Komendanta Głównego Policji i Zastępcy Komendanta Głównego Policji nadzorującego komórki organizacyjne służby kryminalnej i śledczej KGP albo kierowników tych komórek organizacyjnych lub ich zastępców;

2. W wyniku sprawdzenia, jednostka organizacyjna Policji lub uprawniony podmiot pozapolicyjny otrzymuje dostępne w SIO informacje, z zastrzeżeniem § 8 ust. 2 i § 11 ust. 6.

3. Sprawdzenia dla zagranicznych organów ścigania wykonywane są za pośrednictwem biura KGP właściwego w sprawach międzynarodowej współpracy Policji.

4. Dopuszcza się kierowanie zapytań do SIO przez uprawnione podmioty pozapolicyjne na podstawie innych dokumentów, niż wymienione w § 5 ust. 1 pkt 2 zawierających niezbędne dane.

5. Sprawdzenia w SMI na wniosek uprawnionych podmiotów pozapolicyjnych są dokonywane przez policjantów i pracowników Policji z komórki organizacyjnej podległej dyrektorowi biura KGP właściwego w sprawach wywiadu kryminalnego.

6. Sprawdzeń w CBIU na podstawie zapytania/typowania dokonują:

1) dla komórek organizacyjnych właściwych w sprawach techniki operacyjnej – policjanci i pracownicy Policji pełniący służbę i zatrudnieni w tych komórkach organizacyjnych;

2) dla innych niż wymienione w pkt 1 komórek organizacyjnych służby kryminalnej i śledczej – policjanci lub pracownicy Policji komórek organizacyjnych właściwych w sprawach wywiadu kryminalnego, z zastrzeżeniem pkt 3;

3) dla komórek organizacyjnych właściwych w sprawach wewnętrznych – policjanci i pracownicy Policji wyznaczeni przez dyrektora biura KGP właściwego w sprawach wewnętrznych oraz centralni administratorzy merytoryczni wyznaczeni przez dyrektora biura KGP właściwego w sprawach wywiadu kryminalnego;

4) dla uprawnionych podmiotów pozapolicyjnych – policjanci i pracownicy Policji komórki organizacyjnej podległej dyrektorowi biura KGP właściwego w sprawach techniki operacyjnej, za pośrednictwem dyrektora KGP właściwego w sprawach wywiadu kryminalnego.

§ 20. 1. Sprawdzeń w formie zapytania/typowania i analizy dokonuje się na podstawie pisemnych wniosków kierowników komórek organizacyjnych służby kryminalnej i śledczej Policji lub komendantów powiatowych (miejskich, rejonowych) Policji, komendantów komisariatów i komisariatów specjalistycznych Policji.

2. Komendanci i kierownicy mogą upoważnić na piśmie podległych policjantów służby kryminalnej i śledczej do wykonywania czynności, o których mowa w ust. 1.

3. Wniosek o dokonanie sprawdzenia w formie analizy jest realizowany pod warunkiem potwierdzenia możliwości realizacji wniosku przez kierownika właściwej komórki organizacyjnej Policji do spraw wywiadu kryminalnego.

4. Sprawdzenie w formie analizy może być dokonane jedynie w celu:

1) rozpoznania lokalizacji, rodzaju działalności, składu osobowego i struktury organizacji przestępczych oraz sposobu wykorzystywania dochodów z działalności przestępczej;

2) ustalenia związków i zależności zachodzących pomiędzy poszczególnymi informacjami znajdującymi się w zbiorze, przydatnych do wspomagania działań wykrywczych i procesów decyzyjnych związanych z realizacją zadań Policji;

3) weryfikacji zgromadzonych informacji.

5. Wyniki zapytania/typowania i analizy mogą być przedstawione w formie opisowej i graficznej.

6. Do zapytania/typowania i analizy stosuje się odpowiednio przepisy § 11 i § 15.

§ 21. 1. Indywidualne uprawnienia dostępu do SIO są nadawane, odbierane lub zmieniane na podstawie pisemnego wniosku właściwego komendanta i kierownika jednostki lub komórki organizacyjnej Policji, według procedury określonej w dokumentacji bezpieczeństwa teleinformatycznego SIO.

2. Indywidualne uprawnienia dostępu do informacji przetwarzanych z wykorzystaniem MWD są nadawane i odbierane na podstawie pisemnego wniosku właściwego kierownika jednostki organizacyjnej Policji.

3. Wniosek o nadanie/odebranie uprawnień do aplikacji MWD należy przesłać do dyrektora biura KGP właściwego w sprawach wywiadu kryminalnego za pośrednictwem właściwej komórki wywiadu kryminalnego KGP, komend wojewódzkich (Stołecznej) Policji.

4. Komendant i kierownik, o którym mowa w ust. 1, lub upoważniony przez niego policjant, jest obowiązany przynajmniej raz w roku przeprowadzić weryfikację indywidualnych uprawnień dostępu do SIO, nadanych podległym policjantom i pracownikom Policji.

5. Wzór wniosku o nadanie/odebranie/zmianę uprawnień dostępu do SIO, o którym mowa w ust. 1, stanowi załącznik nr 4.

6. Wzór wniosku o nadanie/odebranie uprawnień dostępu do MWD stanowi załącznik nr 5 do decyzji.

§ 22. 1. Kontrolę i nadzór służbowy nad przetwarzaniem informacji w SIO wykonują:

1) dyrektor biura KGP właściwego w sprawach wywiadu kryminalnego;

2) Centralni Administratorzy Merytoryczni SIO wyznaczeni decyzją dyrektora KGP właściwego w sprawach wywiadu kryminalnego;

2. Zakres kontroli i nadzoru służbowego nad przetwarzaniem informacji w SIO obejmuje zgodność przetwarzania z zasadami ogólnymi określonymi w powszechnie obowiązujących przepisach oraz z uregulowaniami niniejszej decyzji i innych policyjnych przepisów wewnętrznych.

3. Centralny Administrator Merytoryczny SIO przeprowadza kontrolę w jednostkach i komórkach organizacyjnych Policji na podstawie pisemnego polecenia kontroli wskazującego zakres kontroli, wydanego przez dyrektora biura KGP właściwego w sprawach wywiadu kryminalnego.

4. W ramach nadzoru centralny administrator merytoryczny SIO zapewnia właściwe funkcjonowanie zestawu zbioru danych poprzez weryfikację, w jednostkach i komórkach organizacyjnych Policji, dokumentów stanowiących podstawę do wprowadzania informacji oraz bieżącą analizę zgromadzonych w zestawie zbiorów informacji.

5. W przypadku stwierdzonych uchybień w przetwarzaniu informacji dyrektor biura KGP właściwego w sprawach wywiadu kryminalnego wydaje zalecenia lub wytyczne celem ich usunięcia.

6. Kontrolowanych i nadzorowanych jednostek lub komórek organizacyjnych Policji nie informuje się wcześniej o planowanych czynnościach kontrolnych lub nadzorczych.

§ 23. 1. Dyrektora biura KGP właściwego w sprawach wywiadu kryminalnego upoważnia się do:

1) pełnienia funkcji administratora danych osobowych przetwarzanych w SIO;

2) kontroli dostępu do informacji przetwarzanych w SIO;

3) nadawania, odbierania i zmiany uprawnień dostępu do SIO;

4) wyznaczania centralnych administratorów merytorycznych SIO i określania zakresu ich zadań;

5) wydania wytycznych w sprawach szczegółowego sposobu wykonywania przez policjantów i pracowników jednostek organizacyjnych Policji czynności służbowych związanych z przetwarzaniem informacji w SIO.

2. Dyrektor biura KGP właściwego w sprawach wywiadu kryminalnego jest odpowiedzialny za merytoryczną jakość informacji przetwarzanych w SMI i ARCHIWUM.

3. Dyrektor biura KGP właściwego w sprawach techniki operacyjnej jest odpowiedzialny za merytoryczną jakość informacji przetwarzanych w CBIU.

4. Dyrektor biura KGP właściwego w sprawach łączności i informatyki jest odpowiedzialny za niezawodne funkcjonowanie SIO pod względem technicznym oraz bezpieczeństwa teleinformatycznego.

§ 24. Traci moc decyzja nr 773 Komendanta Głównego Policji z dnia 19 grudnia 2008 r. w sprawie prowadzenia w Policji zestawu zbiorów „System Informacji Operacyjnych” (Dz. Urz. KGP z 2009 r. Nr 1, poz. 3).

§ 25. Decyzja wchodzi w życie z dniem podpisania.

Komendant Główny Policji

nadinsp. Marek DZIAŁOSZYŃSKI

Załączniki do decyzji nr 126
Komendanta Głównego Policji
z dnia 5 kwietnia 2013 r.

Załącznik nr1

„WZÓR"

KLAUZULA TAJNOŚCI

Meldunek informacyjny		Nr URN*: HQMI
Jednostka, komórka Policji: *Kod jednostki:*	*Kategoria/rodzaj źródła informacji:*	*Miejsce, data wypełnienia:*
Sygnatura dokumentu: ...../.....	*Pseudonim/ID/nazwa źródła:*	*Egz. nr .....*
Osoba sporządzająca, nr telefonu kontaktowego Numer ID: *Data uzyskania informacji:*	*Temat:* Uzupełnienie MI nr: HQMI	Kod oceny źródła informacji: A B C X Kod ochrony informacji: H1 H2 H3
TREŚĆ**:		*Kod oceny informacji (1,2,3,4)*
Wykonano w ..... egz. Egz. nr 1 ..... Egz. nr 2 ..... Egz. nr 3 ..... Wyk./sporz.	Uwagi:	*Podpis policjanta* *Podpis przełożonego*

numer strony/liczba stron

** / wypełnia operator po wprowadzeniu do SMI*
***/ podczas wypełniania pamiętaj o odpowiedzi na pytania: kto?, co?, kiedy?, gdzie?, dlaczego?, w jaki sposób?, czym?*

KLAUZULA TAJNOŚCI

Załącznik nr 2

„WZÓR"

KLAUZULA TAJNOŚCI

HQZP .....

ZATWIERDZAM

....., dnia .....
(miejscowość, data)

.....
(jednostka, komórka organizacyjna Policji)
.....
(kod jednostki i komórki organizacyjnej)
.....
(numer sprawy operacyjnej)

Egz. nr .....

.....
(komórka właściwa w sprawach wywiadu kryminalnego)
w .....

ZAPYTANIE /TYPOWANIE*
DO SYSTEMU INFORMACJI OPERACYJNYCH
□SMI □CBIU

Proszę o sprawdzenie w zbiorze informacji: .....
.....
.....
.....
(wskazać przedmiot zapytania/typowania)*

UWAGI: .....
(np. ogólny opis sprawy (rodzaj przestępczości), oraz powiązania między obiektami, których dotyczy zapytanie, kryteria typowania)
.....
.....

Powód sprawdzenia**

- □ - przed zainteresowaniem operacyjnym
- □ - analiza

Kryterium ochrony**

- □ **- H1**
- □ **- H2**
- □ **- H3**

.....
(stopień, imię i nazwisko policjanta)
.....
(nr identyfikacyjny policjanta)
.....
(jednostka, komórka organizacyjna Policji)
.....
(nr telefonu kontaktowego)

* - niepotrzebne skreślić
** - zaznaczyć właściwe pole
Wyk. w ... egz.
Egz nr ... - .....
Egz. nr ... - .....
Wyk./Sporz. .....

.....
(numer stron/liczba stron)

Dane wymagane dla poszczególnych obiektów:

„**Adres**" – państwo, województwo, miejscowość, ulica, nr budynku;
„**Dokument**" – rodzaj, nr dokumentu;
„**Grupa**" – nazwa, charakterystyka, obszar działania;
„**Firma**" – nazwa pełna, REGON;
„**Konto**" – nr konta, nazwa banku;
„**Osoba**" – imię, nazwisko, PESEL;
„**Pojazd**" – marka, typ, nr rejestracyjny, kraj rejestracji;
„**Kontakt/Telefon**" – numer, rodzaj.

KLAUZULA TAJNOŚCI

Załącznik nr 3

„WZÓR"

KLAUZULA TAJNOŚCI

....., dnia .....
(miejscowość, data)

ZATWIERDZAM

Egz. nr .....

_____
(komórka właściwa w sprawach wywiadu kryminalnego)

w _____

WNIOSEK O ZASTRZEŻENIE KOORDYNACYJNE /PRZEDŁUŻENIE ZASTRZEŻENIA KOORDYNACYJNEGO W SYSTEMIE INFORMACJI OPERACYJNYCH

Wnoszę o:
- objęcie zastrzeżeniem koordynacyjnym od dnia .....*
- przedłużenie czasu zastrzeżenia koordynacyjnego od dnia .....*

w odniesieniu do następujących obiektów analitycznych:

.....
.....
.....
.....
.....

.....
(stopień, imię i nazwisko policjanta)

.....
(nr identyfikacyjny policjanta)

.....
(jednostka, komórka organizacyjna Policji)

.....
(nr telefonu kontaktowego)

* niepotrzebne skreślić

Wyk. w ... egz.
Egz. nr ... - .....
Egz. nr ... - .....

Wyk./Sporz. .....

.....
(numer strony/liczba stron)

Dane wymagane dla poszczególnych obiektów:
- „**Adres**" – państwo, województwo, miejscowość, ulica, nr budynku;
- „**Dokument**" – rodzaj, nr dokumentu;
- „**Grupa**" – nazwa, charakterystyka, obszar działania;
- „**Firma**" – nazwa pełna, REGON;
- „**Konto**" – nr konta, nazwa banku;
- „**Osoba**" – imię, nazwisko, PESEL;
- „**Pojazd**" – typ, nr rejestracyjny, kraj rejestracji;
- „**Kontakt/Telefon**" – numer, rodzaj.

KLAUZULA TAJNOŚCI

Załącznik nr 4

„WZÓR"

ZATWIERDZAM
(Dyrektor biura KGP
właściwego w sprawach
wywiadu kryminalnego)

_____
(komórka właściwa w sprawach wywiadu kryminalnego)

w _____

....., dnia .....
(miejscowość, data)

DYREKTOR
BIURA .....
KOMENDY GŁÓWNEJ POLICJI

WNIOSEK O NADANIE/ODEBRANIE/ZMIANĘ(1) UPRAWNIEŃ DOSTĘPU DO SYSTEMU INFORMACJI OPERACYJNYCH(2)

dla policjanta/pracownika *
.....
(nazwa jednostki, siedziba)

Lp.	Imię i nazwisko	Identyfikator kadrowy funkcjonariusza /pracownika Policji*	Rodzaj uprawnień**						
				SMI			CBIU		
			Centralny Administrator Merytoryczny(3)	Administrator Lokalny	Analityk	Wprowadzający dane (Operator stacji)	Administrator Lokalny	Analityk	Wprowadzający dane (Operator stacji)
			☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐

** niepotrzebne skreślić*
*** zaznaczyć właściwe pole*

Data przeszkolenia specjalistycznego szkolenia dla administratorów systemów.....
Nr zaświadczenia DBTI ABW.....
(Dot. nadania uprawnień dla administratora)

.....
Podpis przełożonego

.....
AKCEPTUJĘ *(dot. tylko CBŚ KGP, BSW KGP oraz komórek organizacyjnych właściwych ws. techniki operacyjnej)*

(1) - zaznaczyć w momencie przydziału nowych uprawnień lub zmiany jednostki.
(2) - wniosek należy przesłać do dyrektora KGP właściwego w sprawach wywiadu kryminalnego - bez pisma przewodniego.
(3) - uprawnienia Centralnego Administratora Merytorycznego wyłącznie dla funkcjonariuszy/pracowników biura KGP właściwego w sprawach wywiadu kryminalnego.

Załącznik nr 5

„WZÓR"

ZATWIERDZAM
(Dyrektor biura KGP
właściwego w sprawach
wywiadu kryminalnego)

.....
(jednostka/komórka Policji)

w..... dnia.....
(miejscowość, data)

DYREKTOR
BIURA .....
KOMENDY GŁÓWNEJ POLICJI

WNIOSEK O NADANIE/ODEBRANIE UPRAWNIEŃ
DOSTĘPU DO MODUŁU WPROWADZANIA DANYCH (1)

dla policjanta/pracownika *w.....
(nazwa jednostki/komórki policji, siedziba)

Lp.	Imię i Nazwisko	Identyfikator kadrowy funkcjonariusza/ pracownika policji	Nr klucza MWD	Rodzaj klucza MWD**(2)		Adres e-mail do karty EKD na urządzenie szyfrujące(3)
				Nadzorowany	Nadzorujący	

** niepotrzebne skreślić*
*** zaznaczyć właściwe pole*

.....
Podpis przełożonego

AKCEPTUJĘ
(naczelnik właściwej komórki wywiadu kryminalnego KGP/KWP/KSP)

(1) – wniosek o nadanie/odebranie uprawnień do MWD należy przesłać do dyrektora biura KGP właściwego w sprawach wywiadu kryminalnego za pośrednictwem właściwej jednostki/komórki wywiadu kryminalnego KGP/KWP/KSP bez pisma przewodniego.
(2) – klucz MWD nadzorowany przypisany jest do jednostek Policji KP, KMP, KRP, KPP i innych, klucz nadzorujący MWD przypisany jest do jednostek KWP/KSP/KGP.
(3) – należy podać adres skrzynki e-mail przyznawany wraz z kartą EKD do urządzenia szyfrującego.