

Warszawa, dnia wtorek, 5 lipca 2022 r.

Poz. 209

**ZARZĄDZENIE NR 80
KOMENDANTA GŁÓWNEGO POLICJI**

z dnia 30 czerwca 2022 r.

w sprawie Systemu Informacyjnego Interpolu I-24/7

Na podstawie art. 7 ust. 1 pkt 2 w związku z art. 1 ust. 2 pkt 7 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2021 r. poz. 1882, 2333, 2447 i 2448 oraz z 2022 r. poz. 655 i 1115), w związku z § 2 ust. 4 pkt 1 oraz § 18 ust. 2 pkt 8 zarządzenia nr 2 Komendanta Głównego Policji z dnia 1 kwietnia 2016 r. w sprawie regulaminu Komendy Głównej Policji (Dz. Urz. KGP z 2016 r. poz. 13, z późn. zm.¹⁾) zarządza się, co następuje:

**Rozdział 1
Przepisy ogólne**

§ 1. Zarządzenie określa metody i formy wykonywania zadań związanych z obsługą Systemu Informacyjnego Interpolu I-24/7, zwanego dalej „SII I-24/7”, w tym:

- 1) zadania Krajowego Biura Interpolu w zakresie przetwarzania informacji, w tym danych osobowych, w SII I-24/7;
- 2) procedury nadawania, zmiany, cofania lub utraty uprawnień do dostępu do SII I-24/7;
- 3) procedury wykonywania kontroli i nadzoru nad przetwarzaniem informacji, w tym danych osobowych, w SII I-24/7;
- 4) podział zadań administratora oraz upoważnienia do wykonywania zadań administratora w odniesieniu do informacji, w tym danych osobowych, przetwarzanych w SII-I-24/7.

§ 2. Użyte w zarządzeniu określenia i skróty oznaczają:

- 1) bazy danych Interpolu – policyjne bazy danych, o których mowa w art. 36 Regulaminu Interpolu oraz w specyfikacjach baz danych Interpolu „INTERPOL Database Identification Form”, publikowanych na stronie intranetowej Sekretariatu Generalnego Interpolu;
- 2) dyrektor biura KGP – dyrektora biura Komendy Głównej Policji lub kierownika równorzędnej komórki organizacyjnej Komendy Głównej Policji;
- 3) dostęp bezpośredni – wprowadzanie i pozyskiwanie danych w SII I-24/7 przez osoby uprawnione przez użycie środków automatycznych oraz bez pomocy Sekretariatu Generalnego Interpolu, zgodnie z art. 1 Regulaminu Interpolu;
- 4) dostęp pośredni – wprowadzanie i pozyskiwanie danych w SII I-24/7 za pośrednictwem Sekretariatu Generalnego Interpolu, zgodnie z art. 1 Regulaminu Interpolu;

¹⁾Zmiany wymienionego zarządzenia zostały ogłoszone w Dz. Urz. KGP z 2016 r. poz. 69, z 2017 r. poz. 44, z 2018 r. poz. 2, 106 i 126, z 2019 r. poz. 105 i 126, z 2020 r. poz. 16, z 2021 r. poz. 15, 57 i 101 oraz z 2022 r. poz. 88 i 199.

- 5) formularz rejestracyjny – wnioski i formularze, których wzory zostały określone w zarządzeniu nr 5 Komendanta Głównego Policji z dnia 4 lutego 2021 r. w sprawie not i dyfuzji Międzynarodowej Organizacji Policji Kryminalnej – Interpol (Dz. Urz. KGP poz. 9);
- 6) Interpol – Międzynarodową Organizację Policji Kryminalnej – Interpol;
- 7) KAB SII I-24/7 – Krajowy Administrator Bezpieczeństwa SII I-24/7 – osobę odpowiedzialną za administrowanie kontami INSYST I-24/7 i uprawnieniami krajowych użytkowników SII I-24/7;
- 8) KBI Warszawa – Krajowe Biuro Interpolu w Warszawie – komórkę organizacyjną Komendy Głównej Policji, wyznaczoną do wykonywania zadań polskiego krajowego biura Interpolu w zakresie koordynowania i prowadzenia międzynarodowej wymiany informacji o charakterze kryminalnym oraz strategicznym, pomiędzy podmiotami krajowymi, KBI innych państw oraz Sekretariatem Generalnym Interpolu;
- 9) konto INSYST I-24/7 – imienne konto dostępne utworzone na stanowisku dostępowym obsługującym Policijną Sieć Transmisji Danych, za pomocą którego uzyskuje się dostęp do SII I-24/7 zgodnie z przyznanym zakresem uprawnień;
- 10) oficer kontaktowy – policjanta lub pracownika Policji pełniących funkcję oficera kontaktowego do spraw międzynarodowej wymiany informacji kryminalnych, wyznaczonego zgodnie z przepisami Komendanta Głównego Policji w sprawie ustanowienia oficerów kontaktowych do spraw międzynarodowej wymiany informacji kryminalnych;
- 11) organ uprawniony – sąd, prokuraturę, ministra właściwego w sprawach kultury i dziedzictwa narodowego oraz podmioty wymienione w art. 1 ust. 2 ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz. U. z 2020 r. poz. 158);
- 12) Regulamin Interpolu – Regulamin Interpolu dotyczący przetwarzania danych (INTERPOL's Rules on the Processing of Data) – przyjęty Rezolucją nr AG-2011-RES-07 podczas 80. sesji Zgromadzenia Ogólnego Interpolu w Hanoi w dniach 31 października - 3 listopada 2011 r., wraz ze zmianami;
- 13) rozporządzenie PE i Rady (UE) 2016/679 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.²⁾);
- 14) Statut Interpolu – Statut Międzynarodowej Organizacji Policji Kryminalnej – Interpol, przyjęty w Wiedniu dnia 13 czerwca 1956 r. (Dz. U. z 2015 r. poz. 1758);
- 15) STBS – system teleinformatyczny wspomagający zarządzanie, koordynację i czynności Policji podejmowanych w celu wykonywania zadań ustawowych i zobowiązań międzynarodowych w obszarze międzynarodowej współpracy Policji;
- 16) system łączności I-24/7 – system komunikacji, o którym mowa w Karcie Bezpieczeństwa I-24/7 (I-24/7 Security Charter), zatwierdzonej Rezolucją nr AG-2003-RES-04 podczas 72 Sesji Zgromadzenia Ogólnego Interpolu w Benidrom w dniach 29 września - 2 października 2013 r., przeznaczony do przekazywania informacji, w tym danych osobowych, przez bezpieczną i szyfrowaną sieć, w ramach współpracy międzynarodowej pomiędzy poszczególnymi KBI oraz Sekretariatem Generalnym Interpolu, w celu zwalczania przestępczości;
- 17) trener SII I-24/7 – oficer kontaktowy lub osoba wyznaczona w upoważnionym podmiocie krajowym do przeprowadzenia szkolenia z zakresu dostępu do SII I-24/7;
- 18) upoważniony podmiot krajowy – podmiot posiadający uprawnienia do bezpośredniego dostępu do SII I-24/7 nadane przez Krajowe Biuro Interpolu na podstawie porozumienia, zawartego przez ten podmiot z Komendantem Głównym Policji, w celu sprawdzania lub bezpośredniego rejestrowania, modyfikowania oraz usuwania informacji, w tym danych osobowych;
- 19) uprawnienia dostępu do SII I-24/7 – zakres uprawnień do poszczególnych baz danych i narzędzi Interpolu;

²⁾Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

- 20) ustawa ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości – ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);
- 21) użytkownik końcowy – osobę posiadającą konto INSYST I-24/7 w celu realizacji powierzonych zadań;
- 22) wniosek o dostęp do SII I-24/7 – wniosek o nadanie, zmianę lub cofnięcie uprawnień oraz upoważnienia do przetwarzania informacji, w tym danych osobowych, w SII I-24/7.

Rozdział 2

Zadania KBI Warszawa w zakresie przetwarzania informacji, w tym danych osobowych, w SII I-24/7

§ 3. 1. SII I-24/7 jest systemem międzynarodowym, określonym w art. 1 pkt 4 Regulaminu Interpolu.

2. Sekretariat Generalny Interpolu jest administratorem SII I-24/7 oraz realizuje zadania w tym zakresie, określone w przepisach tytułu 2 rozdziału II Regulaminu Interpolu.

3. Zadania administratora, o których mowa w ust. 2 oraz w rozumieniu art. 4 pkt 1 ustawy ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, w odniesieniu do informacji, w tym danych osobowych, przetwarzanych przez KBI oraz w ramach dostępu bezpośredniego, realizuje KBI Warszawa poprzez dyrektora biura KGP właściwego w sprawach współpracy międzynarodowej lub inną osobę upoważnioną w tym zakresie przez Komendanta Głównego Policji.

§ 4. 1. SII I-24/7 umożliwia przetwarzanie informacji, w tym danych osobowych, w bazach danych Interpolu.

2. KBI Warszawa przetwarza w SII I-24/7 informacje, w tym dane osobowe, o których mowa w:

- 1) ustawie z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi;
- 2) Regulaminie Interpolu;
- 3) specyfikacjach baz danych Interpolu „INTERPOL Database Identification Form” publikowanych na stronie intranetowej Sekretariatu Generalnego Interpolu.

3. Informacje, w tym dane osobowe, z baz danych Interpolu uzyskuje się w ramach:

- 1) dostępu bezpośredniego do SII I-24/7:
 - a) poprzez systemy teleinformatyczne Krajowego Systemu Informacyjnego Policji, w sposób określony w przepisach Komendanta Głównego Policji w sprawie Krajowego Systemu Informacyjnego Policji, zwanego dalej „KSIP”,
 - b) poprzez konto INSYST I-24/7;
- 2) dostępu pośredniego do SII I-24/7 poprzez KBI Warszawa.

4. SII I-24/7 umożliwia przekazywanie informacji, w tym danych osobowych, do baz danych Interpolu w sposób:

- 1) częściowo zautomatyzowany;
- 2) zautomatyzowany;
- 3) manualny.

5. Informacje, w tym dane osobowe, o których mowa w ust. 2, przetwarza się w SII I-24/7 w celu:

- 1) poszukiwania osoby w celu jej zatrzymania, aresztowania lub ograniczenia jej swobody przemieszczania się;
- 2) ustalenia miejsca pobytu osoby lub przedmiotu będących przedmiotem zainteresowania Policji;
- 3) dostarczenia lub uzyskania informacji związanych ze śledztwem lub z działalnością przestępczą danej osoby;
- 4) ostrzeżenia o osobie, zdarzeniu, przedmiocie lub modus operandi związanych z działalnością przestępczą;
- 5) zidentyfikowania osoby lub zwłok ludzkich;

- 6) przeprowadzenia badań kryminalistycznych;
- 7) przeprowadzenia kontroli bezpieczeństwa;
- 8) identyfikacji zagrożeń, tendencji w przestępczości oraz grup przestępczych.

§ 5. 1. KBI Warszawa wykonuje w SII I-24/7 następujące operacje przetwarzania informacji, w tym danych osobowych:

- 1) rejestrację, modyfikowanie i usuwanie informacji, w tym danych osobowych, bezpośrednio w bazach danych Interpolu poprzez:
 - a) system not i dyfuzji Interpolu, o którym mowa w art. 8 i 73 Regulaminu Interpolu,
 - b) usługi dostarczone w ramach SII I-24/7;
- 2) bezpośrednio sprawdzanie w bazach danych Interpolu z zachowaniem warunków ustalonych dla każdej bazy danych, a także ograniczeń i zasad poufności ustalonych przez KBI Warszawa, które dokonało rejestracji informacji, w tym danych osobowych;
- 3) weryfikowanie zarejestrowanych informacji oraz pozytywnych wyników zapytań;
- 4) przekazywanie informacji, w tym danych osobowych, organom ścigania, krajowym biurom Interpolu innych państw oraz Sekretariatowi Generalnemu Interpolu.

2. Operacje przetwarzania informacji, w tym danych osobowych, mogą być wykonywane przez KBI Warszawa na wniosek jednostek organizacyjnych Policji, otrzymany za pośrednictwem oficerów kontaktowych oraz organów uprawnionych, niemających bezpośredniego dostępu do SII I-24/7.

3. Za prawidłowe i poprawne wykonanie operacji przetwarzania informacji, w tym danych osobowych, odpowiadają policjanci lub pracownicy Policji w KBI Warszawa, uprawnieni do przetwarzania informacji, w tym danych osobowych, w SII I-24/7, a za prawidłowe i poprawne wypełnienie formularza rejestracyjnego – odpowiada wnioskujący o wykonanie operacji przetwarzania informacji.

Rozdział 3

Procedury nadawania, zmiany i cofania uprawnień dostępu do SII I-24/7

§ 6. 1. KBI Warszawa jest upoważnione do nadawania uprawnień dostępu do SII I-24/7 użytkownikom końcowym:

- 1) w KBI, jednostkach organizacyjnych Policji i komórkach organizacyjnych Komendy Głównej Policji, zgodnie z art. 111 Regulaminu Interpolu;
- 2) w upoważnionych podmiotach krajowych oraz do ustalania zakresu uprawnień tych podmiotów, zgodnie z art. 21 Regulaminu Interpolu.

2. KBI Warszawa jest odpowiedzialne za udzielenie praw dostępu do stanowisk dostępowych działających w systemie łączności I-24/7 i zapewnienie ochrony dostępu, zgodnie z ustawą ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz rozporządzeniem PE i Rady (UE) 2016/679. Za konfigurację stanowiska dostępowego odpowiada administrator lokalny, natomiast za nadawanie uprawnień dostępu do SII I-24/7 odpowiada administrator systemu.

§ 7. 1. Uprawnienia dostępu do SII I-24/7 w zakresie przetwarzania informacji, w tym danych osobowych, mogą być nadane w zakresie:

- 1) dostępu do baz danych Interpolu;
- 2) wykonywania określonych operacji przetwarzania informacji, w tym danych osobowych, w SII I-24/7.

2. Dostęp do baz danych Interpolu posiadają, zgodnie z zakresem realizowanych zadań na stanowisku służbowym:

- 1) użytkownicy końcowi w KBI Warszawa w oparciu o uprawnienia do:
 - a) przetwarzania informacji, w tym danych osobowych, w SII I-24/7 w ramach konta INSYST I-24/7,
 - b) przetwarzania informacji, w tym danych osobowych, w KSIP,
 - c) przetwarzania informacji, w tym danych osobowych, w STBS;

2) użytkownicy końcowi w jednostkach organizacyjnych Policji i komórkach organizacyjnych Komendy Głównej Policji w oparciu o uprawnienia do przetwarzania informacji, w tym danych osobowych, w SII I-24/7 w ramach konta INSYST I-24/7;

3) użytkownicy końcowi w jednostkach i komórkach organizacyjnych Policji w oparciu o uprawnienia do przetwarzania informacji, w tym danych osobowych, w KSIP.

3. KBI Warszawa przetwarza informacje, w tym dane osobowe, przy pomocy STBS oraz konta INSYST I-24/7.

§ 8. 1. W KBI Warszawa czynności administrowania, w tym nadania uprawnień do SII I-24/7 w ramach konta INSYST I-24/7, wykonuje dyrektor biura KGP właściwego w sprawach współpracy międzynarodowej. W imieniu dyrektora biura KGP właściwego w sprawach współpracy międzynarodowej wyznaczenia użytkowników końcowych dokonuje kierownik komórki organizacyjnej tego biura właściwej w sprawach współpracy strategicznej.

2. Uprawnienia dostępu do SII I-24/7 w zakresie przetwarzania informacji, w tym danych osobowych, o których mowa w § 7 ust. 1 oraz ust. 2 pkt 1 lit. a i pkt 2, nadaje się na pisemny wniosek kierownika jednostki lub komórki organizacyjnej Policji.

3. Wniosek o dostęp do SII I-24/7, o którym mowa w ust. 2, zawiera:

- 1) imię i nazwisko, identyfikator kadrowy, stanowisko policjanta lub pracownika Policji oraz dane kontaktowe;
- 2) określenie okresu obowiązywania uprawnień oraz upoważnienia do przetwarzania informacji, w tym danych osobowych w SII I-24/7, w tym dostępu do danych osobowych, wraz ze wskazaniem daty nadania, zmiany lub cofnięcia tego uprawnienia oraz upoważnienia;
- 3) nazwę jednostki i komórki organizacyjnej Policji, w której pełni służbę lub wykonuje pracę policjant lub pracownik Policji;
- 4) zakres przedmiotowy uprawnienia oraz upoważnienia ze wskazaniem bazy danych Interpolu, której to uprawnienie lub upoważnienie dotyczy;
- 5) rodzaj danych osobowych i sposób ich przetwarzania.

4. Wzór wniosku o dostęp do SII I-24/7 określa załącznik do zarządzenia.

5. Wniosek o dostęp do SII I-24/7 przesyła się w 1 egzemplarzu drogą elektroniczną do dyrektora biura KGP właściwego w sprawach współpracy międzynarodowej.

6. Dyrektor biura KGP właściwego w sprawach współpracy międzynarodowej lub osoba przez niego upoważniona weryfikuje zakres wskazanych uprawnień, akceptuje wniosek i przekazuje go do KAB SII I-24/7, w celu:

- 1) przeprowadzenia szkolenia z dostępu do SII I-24/7;
- 2) założenia konta INSYST I-24/7 i nadania uprawnień;
- 3) przekazania użytkownikowi końcowemu danych do logowania.

7. W przypadku użytkowników końcowych spoza Komendy Głównej Policji szkolenie, o którym mowa w ust. 6 pkt 1, przeprowadza trener SII I-24/7 przed złożeniem wniosku do dyrektora biura KGP właściwego w sprawach współpracy międzynarodowej.

§ 9. 1. Kierownik jednostki lub komórki organizacyjnej Policji, o którym mowa w § 8 ust. 2, jest obowiązany:

- 1) dokonywać na bieżąco weryfikacji nadanych uprawnień w zakresie:
 - a) zgodności posiadanych uprawnień z realizowanymi zadaniami służbowymi,
 - b) aktualności zawartych we wniosku danych, o których mowa w § 8 ust. 3,
 - c) zgodności faktycznego zakresu przetwarzania informacji w SII I-24/7 z zakresem posiadanych uprawnień;

- 2) złożyć wniosek o odpowiednią zmianę zakresu nadanych uprawnień do przetwarzania informacji, w tym danych osobowych, w SII I-24/7, jeżeli nastąpi zmiana zakresu lub rodzaju czynności służbowych realizowanych przez użytkownika końcowego;
- 3) niezwłocznie złożyć wniosek o cofnięcie nadanych uprawnień do przetwarzania informacji, w tym danych osobowych, w SII I-24/7, jeżeli użytkownik końcowy:
 - a) został zawieszony w czynnościach służbowych lub w pełnieniu obowiązków,
 - b) został przeniesiony do pełnienia służby lub wykonywania pracy w innej jednostce lub komórce organizacyjnej,
 - c) zmarł lub został uznany za zaginionego;
- 4) złożyć wniosek o cofnięcie wszystkich uprawnień do przetwarzania informacji, w tym danych osobowych, w SII I-24/7, w związku ze zwolnieniem ze służby lub ustaniem stosunku pracy.

2. Zmiana oraz cofnięcie uprawnień do przetwarzania informacji, w tym danych osobowych, w SII I-24/7 odbywa się odpowiednio w sposób określony w § 8.

§ 10. 1. Ewidencję osób uprawnionych do przetwarzania informacji, w tym danych osobowych, w SII I-24/7 w ramach konta INSYST I-24/7, zwaną dalej „ewidencją uprawnień” oraz ewidencję osób upoważnionych do przetwarzania informacji, w tym danych osobowych, w SII I-24/7, zwaną dalej „ewidencją upoważnień”, prowadzi dyrektor biura KGP właściwego w sprawach współpracy międzynarodowej lub osoba przez niego wyznaczona.

2. Ewidencja uprawnień i ewidencja upoważnień zawiera informacje, o których mowa w art. 42 ust. 1 ustawy ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

3. Ewidencję uprawnień można prowadzić łącznie z ewidencją upoważnień. Ewidencja uprawnień i upoważnień może być prowadzona w postaci elektronicznej.

Rozdział 4 Przywracanie dostępu do SII I-24/7

§ 11. 1. W stosunku do użytkowników końcowych, którzy utracili dostęp do SII I-24/7, przywraca się go w następujący sposób:

- 1) w przypadku zablokowania dostępu do konta INSYST I-24/7 lub po wygaśnięciu hasła użytkownik końcowy przesyła drogą elektroniczną do KAB SII I-24/7 prośbę o reset hasła, podając:
 - a) nazwę użytkownika,
 - b) nazwę jednostki, w której pełni służbę lub wykonuje pracę;
- 2) KAB SII I-24/7 generuje nowe hasło dostępowe do konta INSYST I-24/7 i przesyła je drogą elektroniczną użytkownikowi końcowemu;
- 3) użytkownik końcowy zmienia hasło wygenerowane przez KAB SII I-24/7 na nowe podczas pierwszego logowania do konta INSYST I-24/7.

2. W stosunku do użytkowników końcowych konto INSYST I-24/7 jest automatycznie usuwane przez Interpol w przypadku braku aktywności przez okres 90 dni.

Rozdział 5 Procedury wykonywania kontroli i nadzoru nad przetwarzaniem informacji, w tym danych osobowych, w SII I-24/7

§ 12. 1. W odniesieniu do informacji, w tym danych osobowych, przetwarzanych w SII I-24/7, w celu zapewnienia zgodności trybu gromadzenia informacji z celem ich przetwarzania, zapewnienia integralności i bezpieczeństwa informacji, monitorowania działalności dotyczącej przetwarzania informacji w SII I-24/7 oraz w celu weryfikacji zgodności przetwarzania z prawem, a także jako jeden ze środków zapewnienia ochrony przetwarzanych danych osobowych w zakresie kontroli, o której mowa w art. 39 pkt 3-7 ustawy ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, wykonuje się czynności kontroli i nadzoru służbowego w zakresie:

- 1) dostępu do baz danych Interpolu oraz do informacji, w tym danych osobowych, w nich przetwarzanych;

- 2) przetwarzania informacji, w tym danych osobowych, w bazach danych Interpolu;
- 3) uprawnienia do przetwarzania informacji, w tym danych osobowych, w SII I-24/7.

2. Czynności, o których mowa w ust. 1, realizuje się w szczególności przez:

- 1) weryfikację, typowanie i analizę informacji, w tym danych osobowych, przetwarzanych w bazach danych Interpolu;
- 2) sprawdzanie zakresu dostępu do baz danych Interpolu, zakresu i rodzaju operacji przetwarzania wykonanych na informacjach, w tym danych osobowych, oraz ocenę, analizę lub weryfikację wyników tego sprawdzenia;
- 3) kontrolę rejestrów czynności (logowań) odnotowywanych w SII I-24/7 – Sekretariat Generalny Interpolu udostępnia rejestr na wniosek KBI Warszawa;
- 4) kontrolę i ocenę legalności, poprawności, kompletności i celowości przetwarzania informacji, w tym danych osobowych, a także przeprowadzenie analizy w tym zakresie;
- 5) sprawdzanie dokumentacji stanowiącej podstawę do wprowadzenia informacji, w tym danych osobowych, do bazy danych, a także stanowiącej podstawę ich sprawdzenia, wykorzystania, modyfikacji lub usunięcia;
- 6) usuwanie informacji, w tym danych osobowych, wobec których stwierdzono brak przesłanek ich przetwarzania przez Policję.

3. Czynności, o których mowa w ust. 1 i 2, wykonuje dyrektor biura KGP właściwego w sprawach współpracy międzynarodowej lub osoby przez niego upoważnione.

4. Dyrektor biura KGP właściwego w sprawach współpracy międzynarodowej może wydawać zalecenia lub wytyczne w celu usunięcia stwierdzonych uchybień w przetwarzaniu informacji, w tym danych osobowych, w SII I-24/7.

Rozdział 6

Przepis końcowy

§ 13. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Komendant Główny Policji

gen. insp. Jarosław SZYMCZYK

Załącznik do zarządzenia nr 80
 Komendanta Głównego Policji
 z dnia 30 czerwca 2022 r.

WZÓR

.....
 miejscowość, data

ZATWIERDZAM

*Dyrektor biura KGP właściwego
 w sprawach współpracy międzynarodowej*

egz. pojedynczy

.....
 (data nadania, pieczęć i podpis osoby upoważnionej)

NR EWIDENCYJNY

WNIOSEK O NADANIE, ZMIANĘ LUB COFNIĘCIE

uprawnień oraz upoważnienia do przetwarzania informacji, w tym danych osobowych w Systemie Informacyjnym Interpolu I-24/7

<input type="checkbox"/>	NADANIE*	<input type="checkbox"/>	ZMIANA*	<input type="checkbox"/>	COFNIĘCIE*	
..... (WNIOSKOWANA DATA: DZIEŃ, MIESIĄC I ROK)	 (WNIOSKOWANA DATA: DZIEŃ, MIESIĄC I ROK)	 (WNIOSKOWANA DATA: DZIEŃ, MIESIĄC I ROK)		
NAZWISKO:		IMIĘ:		TELEFON/E-MAIL:		
NAZWA JEDNOSTKI / KOMÓRKI ORGANIZACYJNEJ:			IDENTYFIKATOR KADROWY/ STANOWISKO SŁUŻBOWE:			
okres, na który przyznaje się uprawnienie/upoważnienie:		<input type="checkbox"/>	czas oznaczony do: (dzień – miesiąc – rok)**			
		<input type="checkbox"/>	do odwołania*			

ZAKRES UPRAWNIENIA/UPOWAŻNIENIA		REJESTRACJA, MODYFIKACJA, USUWANIE, WGLĄD* (KBI Warszawa oraz Koordynator KWP/KSP ds. dóbr kultury)	WGLĄD*
01	Access Rights Management	Zarządzanie kontami użytkowników	
02	Address Book	Książka adresowa Interpolu	

ZAKRES UPRAWNIENIA/UPOWAŻNIENIA		REJESTRACJA, MODYFIKACJA, USUWANIE, WGLĄD* (KBI Warszawa oraz Koordynator KWP/KSP ds. dóbr kultury)	WGLĄD*
03	Afisgw	Baza odbitek linii papilarnych	
04	Child Alerts System	System ostrzegania o uprowadzeniach dzieci	
05	Daily News	Wiadomości dnia	
06	Dial-Doc	Baza ostrzeżeń o wykrytych sposobach fałszowania dokumentów podróży (paszporty)	
07	Diffusions	Informacje o dyfuzjach	
08	DISCS	Baza wzorców dokumentów stanu cywilnego (akty urodzenia, zgonu, małżeństwa, prawa jazdy)	
09	DNA Admin	Baza danych DNA (administrator)	
10	DNA Forms	Baza danych DNA (formularze)	
11	eASF2 Nominal	Baza danych osób poszukiwanych i zaginionych (Nominal)	
12	eASF2 Stolen Documents	Baza skradzionych i zagubionych dokumentów podróży (SLTD)	
13	eASF2 Stolen Vehicles	Baza skradzionych pojazdów (SMV) i dokumentów administracyjnych (SAD)	
14	eASF2 Training Nominal	Baza szkoleniowa osób poszukiwanych i zaginionych	
15	eASF2 Training Stolen Documents	Baza szkoleniowa skradzionych i zagubionych dokumentów podróży	
16	eASF2 Training Stolen Vehicles	Baza szkoleniowa skradzionych pojazdów i dokumentów administracyjnych	
17	eASF2 Training Works of Art	Baza szkoleniowa skradzionych dzieł sztuki	
18	eASF2 Works of Art	Baza skradzionych dzieł sztuki (WoA).	
19	EdisonTD	Baza wzorców dokumentów (paszporty, dowody osobiste, dokumenty wystawiane cudzoziemcom)	
20	European Committee	Komitet Europejski	
21	European Contact Officers	Europejscy Oficerowie Kontaktowi	
22	Executive Committee	Komitet Wykonawczy	
23	Fada Research International	Międzynarodowa grupa robocza dot. zwalczania przestępczości samochodowej	
24	Fusion Task Force	Informacje dla jednostek zwalczających terroryzm	
25	Genuine Currency	Baza wzorców walut	
26	Heads Contact Details	Dane kontaktowe Szefów Krajowych Biur	
27	I-247 AGFM	Dostęp wyłącznie dla Członków Grupy Doradczej ds. Finansowych	
28	I-247 Corruption	Korupcja, odzyskiwanie mienia (grupy robocze, akademia antykorupcyjna, punkty kontaktowe)	
29	I-247 Crime Intelligence Analysis	Analizy kryminalne	
30	I-247 Dashboard	Niepubliczna strona Interpolu	
31	I-247 Drugs	Przestępczość narkotykowa (alerty, projekty i operacje).	
32	I-247 Environmental Crime	Przestępczość przeciwko środowisku naturalnemu (alerty, grupy robocze, konferencje i wydarzenia, operacje)	
33	I-247 Financial Crime	Przestępczość finansowa (karty płatnicze, pranie pieniędzy, podrabianie środków płatniczych, alerty)	
34	I-247 Forensic	Działania Interpolu w zakresie kryminalistyki	
35	I-247 Human Traffic	Informacje związane z handlem i przemytem ludzi	
36	I-247 Information	Najnowsze informacje i noty prasowe na temat działalności Interpolu	
37	I-247 IT Crime	Cyberprzestępczość (operacje, wydarzenia, punkty kontaktowe)	
38	I-247 Maritime Piracy	Baza danych o piractwie morskim	

ZAKRES UPRAWNIENIA/UPOWAŻNIENIA			REJESTRACJA, MODYFIKACJA, USUWANIE, WGLAD* (KBI Warszawa oraz Koordynator KWP/KSP ds. dóbr kultury)	WGLAD*
39	I-247 Network of NCB Legal Advisers	Sieć doradców prawnych Krajowych Biur Interpolu		
40	I-247 Notices Requests	Wnioski o noty Interpolu		
41	I-247 Pharmaceutical Crime	Przestępczość farmaceutyczna (operacje, punkty kontaktowe)		
42	I-247 Region Activities	Informacje regionalne na temat działalności państw europejskich		
43	I-247 Share	Wirtualny dysk twardy		
44	I-247 Terrorism	Terroryzm (Fusion Task Force, CBRNE, szkolenia i wydarzenia)		
45	I-247 Trafficking in illicit goods	Przemysł podrabianych towarów (operacje, wydarzenia, wsparcie prawne, szkolenia i wydarzenia)		
46	I-247 Vehicle Crime	Przestępczość samochodowa (statystyki, projekty i operacje)		
47	I-247 Wanted	Osoby poszukiwane (operacje, raporty, wydarzenia).		
48	I-247 Weapon Explosive	Broń palna (encyklopedyczna baza broni palnej, alerty, publikacje)		
49	I-247 Works of Art	Dzieła sztuki (konferencje, zasoby prawne)		
50	iARMS	Baza skradzionej / nielegalnej broni palnej		
51	I-Checkit	Informacje nt. usługi checkit		
52	ICSEDB users of the production version	Baza wizerunków dzieci wykorzystywanych seksualnie (użytkownicy wersji produkcyjnej)		
53	ICSEDB users who can only have access to a limited version	Baza wizerunków dzieci wykorzystywanych seksualnie (użytkownicy wersji ograniczonej)		
54	ICSETDBU	Baza wizerunków dzieci wykorzystywanych seksualnie		
55	IGCI Working Group	Grupa robocza Centrum Innowacji w Singapurze		
56	I-le@rn Management System	Platforma przeznaczona do samokształcenia		
57	i-Link: test application	Platforma szkoleniowa do tworzenia not i dyfuzji		
58	I-link Portal ***	Platforma do tworzenia not i dyfuzji		
59	International Crime Statistics	Dane statystyczne dot. największych baz Interpolu (SLTD, SMV)		
60	INTERPOL Travel Document	Informacje nt. baz danych Interpolu dot. dokumentów podróży		
61	Millennium Analysis File	Analizy dot. Projektu Millennium		
62	Millennium Project	Projekt Millennium dot. euroazjatyckich grup przestępczych		
63	Notices Published	Katalog opublikowanych not poszukiwawczych Interpolu		
64	NSOGUIDE ***	Przewodnik dla Krajowego Administratora Bezpieczeństwa		
65	Organised Crime	Przestępczość zorganizowana (alerty, projekty, grupy robocze)		
66	Periodic Assessment of Data	Okresowa ocena danych		
67	Project BI & DATAVIZ	Statystyki baz danych, not, dyfuzji i produktów Interpolu		
68	Project Stadia	Projekt Stadia		
69	PSYCHE	Aplikacja do wprowadzania/usuwania utraconych dzieł sztuki w bazie Works of Art		
70	reftables	Zestawienia		
71	Security Alert	Alerty bezpieczeństwa		
72	Stolen Vessels Database	Baza skradzionych jednostek pływających (SVD)		
73	Test	Portal testowy - dostęp wyłącznie dla Członków Grupy Doradczej ds. Technicznych		
74	TESTIPSGT	Portal testowy Sekretariatu Generalnego		
75	Users Of Test Forum	Użytkownicy forum testowego		

ZAKRES UPRAWNIENIA/UPOWAŻNIENIA		REJESTRACJA, MODYFIKACJA, USUWANIE, WGLĄD* (KBI Warszawa oraz Koordynator KWP/KSP ds. dóbr kultury)	WGLĄD*
76	War Crimes	Ludobójstwo, przestępstwa wojenne, przestępstwa przeciwko ludzkości (wydarzenia, raporty, szkolenia)	
77	Inne ...		

Zakres niniejszego upoważnienia wynika z zakresu zadań realizowanych na danym stanowisku, zgodnie z zakresem obowiązków oraz kartą opisu pracy na stanowisku.

Z chwilą zatwierdzenia, wniosek o dostęp do SII I-24/7 stanowi upoważnienie do przetwarzania danych osobowych w Systemie Informacyjnym Interpolu I-24/7, w rozumieniu art. 41 ust. 1 zdanie drugie ustawy ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

OŚWIADCZENIE

Ja, niżej podpisany/a, zapoznałem/am się z zakresem nadanego mi upoważnienia do przetwarzania danych osobowych i przyznanych mi uprawnień w Systemie Informacyjnym Interpolu I-24/7 oraz zobowiązuję się do zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Systemie Informacyjnym Interpolu I-24/7, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem.

.....
data i czytelny podpis osoby, której dotyczy wniosek

.....
data szkolenia i czytelny podpis osoby szkolącej

.....
data i czytelny podpis osoby wnioskującej

- * - w wybranym polu zaznaczyć „X”
- ** - w przypadku zaznaczenia pola – wpisać daty
- *** - dostęp wyłącznie dla KBI Warszawa

wykonano w 1 egzemplarzu