

# Komenda Główna Policji

---

<http://kgp.bip.policja.gov.pl/kgp/centralny-organ-techni/46220,Centralny-Organ-Techniczny-Krajowego-Systemu-Informatycznego-Komendant-Glowny-Po.html>  
2026-03-10, 00:58

## Centralny Organ Techniczny Krajowego Systemu Informatycznego - Komendant Główny Policji

---

**COT KSI** - Komendant Główny Policji jako centralny organ techniczny Krajowego Systemu Informatycznego (KSI) - jest administratorem danych osobowych, przetwarzanych poprzez Krajowy System Informatyczny (KSI), zgodnie z art. 10 ustawy z dnia 24 sierpnia 2007 r. *o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym* (Dz. U. z 2023 r. poz. 1355, z późn. zm.), zwanej dalej "ustawą o SIS i VIS", tj. danych SIS przetwarzanych w Systemie Informacyjnym Schengen (SIS) w zakresie wpisów dokonanych przez organy, o których mowa w art. 3 ustawy o SIS i VIS, i danych VIS przetwarzanych w Wizowym Systemie Informacyjnym (VIS) w zakresie wpisów dokonanych przez organy, o których mowa w art. 5 ustawy o SIS i VIS oraz rozpatruje wnioski osób dotyczące przetwarzania ich danych osobowych w Systemie Informacyjnym Schengen (SIS) oraz Wizowym Systemie Informacyjnym (VIS).

### I. Administrator danych

Centralny organ techniczny KSI - Komendant Główny Policji

Dane kontaktowe:

ul. Puławska 148/150

02-624 Warszawa

tel. sekretariat: 47 72 148 79, 47 72 131 45

faks sekretariat: 47 72 129 21

e-mail: cot.admin.ksi@policja.gov.pl

ePUAP: /PolicjaKGP/skrytka (ePUAP)

e-Doręczenia: AE:PL-32148-68645-HUSFF-09

### II. Inspektor ochrony danych

Inspektor Ochrony Danych

Dane kontaktowe:

ul. Puławska 148/150

02-624 Warszawa

tel. 47 72 127 34

faks 47 72 128 73

e-mail: iod.kgp@policja.gov.pl

### III. Cel oraz podstawa prawna przetwarzania danych osobowych w SIS i VIS

#### 1. System Informacyjny Schengen (SIS)

Cele ogólne określają:

rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylecia decyzji Rady 2007/533/WSiSW oraz uchylecia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE (Dz. Urz. UE L 312 z 07.12.2018, str. 56, z późn. zm.), zwane dalej *rozporządzeniem 2018/1862*;

*rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylecia rozporządzenia (WE) nr 1987/2006 (Dz. Urz. UE L 312 z 07.12.2018, str. 14, z późn. zm.), zwane dalej rozporządzeniem 2018/1861;*

rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich (Dz. Urz. UE L 312 z 07.12.2018, str. 1), zwane dalej *rozporządzeniem 2018/1860*;

ustawa o SIS i VIS.

Ogólnie celem SIS jest zapewnienie przy wykorzystaniu informacji przekazywanych za pośrednictwem tego systemu - wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii, w tym utrzymywanie bezpieczeństwa publicznego i porządku publicznego oraz zagwarantowanie bezpieczeństwa na terytorium państw członkowskich, a także zapewnienie stosowania postanowień:

rozdziału 2 tytułu V części trzeciej TFUE w odniesieniu do przepływu osób na terytorium państw członkowskich (art. 1 *rozporządzenia 2018/1861*);

tytułu 4 i rozdziału 5 tytułu V części trzeciej TFUE w odniesieniu do przepływu osób na terytorium państw członkowskich (art. 1 *rozporządzenia 2018/1862*);

ustawy o SIS i VIS.

Dane osobowe zawarte we wpisach w SIS mogą być przetwarzane w celach innych niż te, w których wpisy te zostały dokonane, jeżeli jest to związane z konkretną sprawą i uzasadnione potrzebą w zakresie zapobiegania bezpośredniemu poważnemu zagrożeniu porządku publicznego oraz bezpieczeństwa publicznego, lub gdy jest to uzasadnione poważnymi względami bezpieczeństwa narodowego lub koniecznością zapobieżenia poważnym przestępstwom (art. 19 *rozporządzenia 2018/1860*, art. 41 ust. 5 *rozporządzenia 2018/1861* i art. 56 ust. 5 *rozporządzenia 2018/1862* ).

## 2. Wizowy System Informacyjny (VIS)

Cele ogólne określają:

rozporządzenie (WE) nr 767/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) (Dz. Urz. UE L 218 z 13.08.2008, str. 60-81) – *rozporządzenie ws. VIS*;

decyzja Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) (Dz. Urz. UE L 213, z 15.6.2004, s. 5-7);

decyzja Rady (WE) Nr 2008/633/WSiSW z dnia 23 czerwca 2008 r. w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądu, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania (Dz. Urz. UE L 218/129 z 2008 r.) – *decyzja ws. VIS*;

*ustawa o SIS i VIS.*

Ogólny cel VIS został wskazany w art. 2 *rozporządzenia ws. VIS*, do którego należy poprawa realizacji wspólnej polityki wizowej, poprawa współpracy konsularnej i procesu konsultacji pomiędzy centralnymi organami wizowymi poprzez ułatwienie wymiany danych pomiędzy państwami członkowskimi o wnioskach i związanych z nimi decyzjach, w celu m. in.:

1. uproszczenia procedury składania wniosków wizowych;
2. zapobieżenia omijaniu kryteriów służących do określania, które państwo członkowskie odpowiada za rozpatrzenie wniosku;
3. ułatwienia walki z nadużyciami;
4. ułatwienia odpraw w przejściach granicznych na granicach zewnętrznych państw członkowskich i na terytorium państw członkowskich;
5. pomocy w identyfikacji osób, które mogą nie spełniać warunków wjazdu, pobytu lub zamieszkania na terytorium państw członkowskich lub też przestały spełniać te warunki;
6. ułatwienia stosowania rozporządzenia (WE) nr 343/2003;
7. przyczynienia się do zapobiegania zagrożeniom bezpieczeństwa wewnętrznego każdego z państw członkowskich.

Dane VIS są przetwarzane w następujących celach szczegółowych, tj. w celu:

1. rozpatrzenia złożonych wniosków wizowych oraz podjęcia decyzji dotyczących tych wniosków, jak również decyzji o unieważnieniu, przedłużeniu, cofnięciu wizy - art. 15 *rozporządzenia VIS* rzenia złożonych wniosków wizowych oraz podjęcia decyzji dotyczących tych wniosków, jak również decyzji o unieważnieniu, przedłużeniu, cofnięciu wizy - art. 15 *rozporządzenia VIS* ;
2. przeprowadzania konsultacji między centralnymi organami wizowymi w sprawie wniosków

wizowych zgodnie z art. 22 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiającego Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz. Urz. UE L 243 z 15.09.2009, str. 1) - art. 16 *rozporządzenia VIS*;

3. sporządzania sprawozdań i statystyk - art. 17 *rozporządzenia VIS*;
4. sprawdzenia na przejściach granicznych tożsamości posiadacza wize, autentyczności wize lub spełnienia warunków wjazdu na terytorium Państw Członkowskich zgodnie z art. 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz. Urz. UE L 77/1 z 23.03.2016) - art. 18 *rozporządzenia VIS*;
5. sprawdzania na terytorium Rzeczypospolitej Polskiej tożsamości posiadacza wize, autentyczności wize lub spełniania warunków wjazdu lub pobytu na terytorium Państw Członkowskich - art. 19 *rozporządzenia VIS*;
6. zidentyfikowania osoby, która nie spełnia lub przestała spełniać warunki wjazdu lub pobytu na terytorium Państw Członkowskich - art. 20 *rozporządzenia VIS*;
7. określania Państwa Członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej zgodnie z art. 12 i art. 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca (wersja przekształcona) (Dz. Urz. UE L 180 z 29.06.2013) - art. 21 *rozporządzenia VIS*;
8. rozpatrzenia wniosku o udzielenie ochrony międzynarodowej - art. 22 *rozporządzenia VIS*;
9. realizacji obowiązku, o którym mowa w art. 25 ust. 2 *rozporządzenia VIS*.

Ponadto dane VIS mogą być przetwarzane w celu zapobiegania, wykrywania lub ścigania przestępstw wymienionych w art. 607w ustawy z dnia 6 czerwca 1997 r. - *Kodeks postępowania karnego* (Dz.U. z 2024 r. poz. 572 z późn. zm.), gdy jest to niezbędne w związku z określoną sprawą oraz gdy istnieją uzasadnione powody do uznania, że wgląd do danych VIS ma istotne znaczenie dla zapobiegania, wykrywania lub ścigania przestępstw, o których mowa w powyżej, zgodnie z *decyzją ws. VIS*.

#### **IV. Profilowanie w przypadku przetwarzania danych VIS**

Decyzje podejmowane przez właściwe organy w celu rozpatrzenia wniosku wizowego, sprawdzenia autentyczności wize lub spełnienia warunków wjazdu lub pobytu na terytorium Rzeczypospolitej Polskiej lub Państw Członkowskich mogą się opierać wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych (art. 11 ust. 2 *ustawy o SIS i VIS*).

#### **V. Ograniczenia w zakresie dostępu do danych osobowych przetwarzanych w SIS i VIS**

1. art. 11 ust. 1 *ustawy o SIS i VIS*

Przetwarzanie danych może następować bez wiedzy i zgody osób, których dane dotyczą, oraz bez

obowiązku ujawniania faktycznego celu zbierania danych.

2. art. 26 ustawy z dnia 14 grudnia 2018 r. o przetwarzaniu danych osobowych w związku zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. 125, z późn. zm.), zwanej dalej „ustawą p.d.o.z.p.”.

Nie przekazuje się żądanych informacji w odpowiedzi na wniosek oraz nie udostępnia danych osobowych, jeżeli mogłoby to powodować:

- ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;
- utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
- utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;
- zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;
- zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;
- istotne naruszenie dóbr osobistych innych osób.

Jednakże administrator może przekazać osobie, której dane dotyczą, informacje w przypadku gdy ich ujawnienie byłoby niezbędne do ochrony życia lub zdrowia ludzkiego.

3. art. 3 - 5 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781), zwana dalej *ustawą ODO* w związku z art. 23 ust. 1 lit. a, c, d i lit. i rozporządzenia 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 (Dz. Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.), zwanego dalej „*RODO*” oraz z uwzględnieniem art. 11 *ustawy o SIS i VIS*

Powyższe prawa do żądania od administratora dostępu do własnych danych osobowych, ich sprostowania, usunięcia, ograniczenia ich przetwarzania lub do wniesienia sprzeciwu wobec ich przetwarzania wynikające z *RODO* są realizowane z zastrzeżeniem ograniczeń dostępu do żądanych informacji oraz danych osobowych oraz z zastrzeżeniem ograniczeń związanych z przetwarzaniem danych osobowych wynikających z ww. przepisów.

4. art. 67 ust. 3 *rozporządzenia 2018/1862* oraz art. 53 ust. 3 *rozporządzenia 2018/1861*.

Państwo członkowskie podejmuje decyzję o nieprzekazywaniu całości lub części informacji osobie, której dane dotyczą, zgodnie z prawem krajowym, w zakresie – a także przez tak długi okres – w jakim takie częściowe lub całkowite ograniczenie stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, przy należyтым uwzględnieniu praw podstawowych i uzasadnionych interesów osoby, której dane dotyczą, po to aby:

- uniemożliwić utrudnianie prowadzenia urzędowych lub sądowych dochodzeń, postępowań przygotowawczych lub procedur;

uniemożliwić utrudnianie zapobiegania przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania lub wykonywania kar;

chronić bezpieczeństwo publiczne;

chronić bezpieczeństwo narodowe; lub

chronić prawa i wolności innych osób.

W przypadkach, o których mowa w akapicie pierwszym państwo członkowskie bez zbędnej zwłoki informuje na piśmie osobę, której dane dotyczą, o odmowie lub ograniczeniu dostępu oraz o powodach takiej odmowy lub takiego ograniczenia. Informacje takie można pominąć, jeżeli ich przekazanie godziłoby w którykolwiek z celów określonych powyżej, tj. w art. 67 ust. 3 w akapicie pierwszym lit. a-e rozporządzenia 2018/1862 lub w art. 53 ust. 3 w akapicie pierwszym lit. a-e rozporządzenia 2018/1861. Państwo członkowskie informuje osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub możliwości skorzystania ze środka ochrony prawnej przed sądem.

5. art. 14 ust. 4 decyzji ws. VIS

Odmawia się przekazywania informacji osobie, której dotyczą dane, jeżeli odmowa taka jest konieczna, by wykonać uprawnione działanie w związku z tymi danymi lub by chronić prawa i swobody osób trzecich;

## **VI. WARUNKI FORMALNE WNIOSKÓW DOTYCZĄCYCH REALIZACJI PRAW ZWIĄZANYCH Z PRZETWARZANIEM DANYCH OSOBOWYCH W SIS I VIS**

### **PRAWO OSÓB DO INFORMACJI - informacja ogólna**

1. Każdej osobie przysługuje prawo do:

- a. dostępu do własnych danych osobowych;
- b. sprostowania własnych nieprawidłowych danych/korekty błędnych danych;
- c. usunięcia własnych danych osobowych przetwarzanych niezgodnie z prawem;
- d. wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
- e. wystąpienia z roszczeniem o zapłatę, odszkodowanie lub zadośćuczynienie przeciwko podmiotowi (organowi), który ten wpis wprowadził i który za niego odpowiada w przypadku stwierdzenia naruszenia prawa osoby w związku z przetwarzaniem jej danych we wpisach danych SIS w SIS lub danych VIS w VIS;

Osobie pokrzywdzonej przywłaszczeniem jej tożsamości przez osobę poszukiwaną, której dotyczy wpis w SIS, w przypadku gdy dane osoby pokrzywdzonej przywłaszczeniem jej tożsamości za jej zgodą są przetwarzane w SIS w uzupełnieniu wpisu danych SIS jako dane osoby, której tożsamością posługuje się osoba poszukiwana na podstawie wpisu danych SIS oraz są przetwarzane w celu:

- a. umożliwienia właściwemu organowi odróżnienia osoby, której tożsamość została przywłaszczona, od osoby, której ma dotyczyć wpis, w tym uniknięcia ryzyka pomylenia osoby, której dotyczy lub ma dotyczyć wpis do tego systemu z osobą, której tożsamość została

przywłaszczona, w tym w celu zminimalizowania ryzyka niesłusznego zatrzymania i długotrwałych kontroli w kraju i za granicą osoby pokrzywdzonej przywłaszczeniem jej tożsamości, oraz

- b. umożliwienia osobie, której tożsamość została przywłaszczona, udowodnienia swojej tożsamości i wykazania, że jej tożsamość została przywłaszczona przysługuje również prawo do wycofania w dowolnym momencie zgody na uzupełnienie danych SIS o dodatkowe informacje dotyczące jej danych osobowych, w tym fotografie i odblaski linii papilarnych oraz na przetwarzanie dodanych danych osobowych w SIS w wymienionych celach.

2. Osoba składająca do COT KSI wnioski dotyczące realizacji jej praw, o których mowa powyżej, zwany dalej „wnioskiem”, może działać osobiście lub być reprezentowana przez pełnomocnika, chyba że charakter czynności wymaga jej osobistego działania.

Pełnomocnikiem osoby składającej wnioski może być osoba fizyczna posiadająca zdolność do czynności prawnych.

Pełnomocnictwo powinno być udzielone na piśmie i zawierać oświadczenie woli tego mocodawcy o udzieleniu pełnomocnictwa do działania w jego imieniu w danej sprawie objętej wnioskiem. Oryginał pełnomocnictwa lub urzędowo poświadczony odpis pełnomocnictwa powinien być przekazany wraz z wnioskiem składanym do COT KSI.

- a. Pełnomocnictwo udzielone na piśmie (na dokumencie w formie papierowej) przekazane drogą korespondencji tradycyjnej listowej (za pomocą usług operatora pocztowego), powinno zawierać własnoręczny podpis mocodawcy. Do wniosku należy dołączyć oryginał lub urzędowo poświadczony odpis pełnomocnictwa, którego zgodność z oryginałem została poświadczona przez notariusza albo przez występującego w sprawie pełnomocnika strony będącego adwokatem, radcą prawnym, rzecznikiem patentowym lub doradcą podatkowym;
- b. Pełnomocnictwo udzielone i przekazane w formie elektronicznej jako dokument na elektroniczną skrzynkę podawczą ePUAP KGP lub na adres do doręczeń elektronicznych Komendy Głównej Policji (usługi e-Doręczenia) powinno być opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym mocodawcy. Do wniosku przesłanego w formie elektronicznej należy dołączyć pełnomocnictwo w postaci dokumentu elektronicznego opatrzonego jednym z wymienionych powyżej elektronicznych podpisów mocodawcy lub złożyć uwierzytelniony elektronicznie odpis pełnomocnictwa poświadczony za zgodność z oryginałem przy użyciu kwalifikowanego podpisu elektronicznego, podpisu zaufanego albo podpisu osobistego przez notariusza albo przez występującego w sprawie pełnomocnika strony będącego adwokatem, radcą prawnym, rzecznikiem patentowym lub doradcą podatkowym.

Oryginałem nie jest skan czy też kopia pełnomocnictwa udzielonego na piśmie i przesłana drogą korespondencji tradycyjnej listowej (za pomocą usług operatora pocztowego) lub za pośrednictwem środków komunikacji elektronicznej, bez opatrzenia w tym przypadku dokumentu pełnomocnictwa podpisem własnoręcznym mocodawcy (na oryginale dokumentu) lub podpisem elektronicznym równoważnym w skutkach prawnych z podpisem własnoręcznym, tj. bez jego opatrzenia kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym mocodawcy.

# SYSTEM INFORMACYJNY SCHENGEN (SIS)

## 1. Wniosek o dostęp do własnych danych osobowych przetwarzanych w SIS

W tym celu należy złożyć pisemny wniosek w języku polskim, który obligatoryjnie powinien zawierać:

1. imię/imiona i nazwisko składającego wniosek;
2. obywatelstwo;
3. datę i miejsce urodzenia (miejscowość i kraj);
4. adres do korespondencji zwrotnej (kraj, miejscowość, kod pocztowy, powiat/rejon, województwo/obwód, ulica i numeru domu/mieszkania) - *w przypadku wniosku kierowanego drogą pocztową;*
5. przedmiot wniosku;
6. podpis osoby składającej wniosek (*w przypadku wniosku w formie pisemnej (dokumentu w formie papierowej) – zawierającego podpis własnoręczny, a w przypadku wniosku w formie elektronicznej (dokumentu w formie elektronicznej) zawierającego podpis elektroniczny równoważny w skutkach prawnych z podpisem własnoręcznym, tj. - kwalifikowany podpis elektroniczny, podpis zaufany lub podpis osobisty*)

Dodatkowo, w celu jednoznacznej identyfikacji danych, wnioskodawca może we wniosku podać:

1. nazwisko poprzednie/rodowe;
2. numer PESEL (jeżeli osoba posiada);
3. płeć;
4. miejsce zamieszkania (kraj, miejscowość, kod pocztowy, powiat/rejon, województwo/obwód, ulica i numeru domu/mieszkania);
5. dołączyć kserokopię strony dokumentu tożsamości zawierającej ww. dane osobowe.

W przypadku wątpliwości co do tożsamości osoby, która złożyła wniosek administrator może żądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby (art. 28 *ustawa p.d.o.z.p.* oraz art. 12 ust. 6 *RODO*).

## 2. Wniosek o sprostowanie własnych nieprawidłowych danych, usunięcie własnych danych osobowych przetwarzanych niezgodnie z prawem w SIS oraz wycofanie zgody na przetwarzanie dodanych danych osobowych (złożonej przez osobę pokrzywdzoną przywłaszczeniem tożsamości na uzupełnienie danych SIS).

W tym celu należy złożyć pisemny wniosek w języku polskim, który obligatoryjnie powinien zawierać:

1. imię/imiona i nazwisko składającego wniosek
2. obywatelstwo;
3. datę i miejsce urodzenia (miejscowość i kraj);

4. adres do korespondencji zwrotnej (kraj, miejscowość, kod pocztowy, powiat/rejon, województwo/obwód, ulica i numeru domu/mieszkania) - *w przypadku wniosku kierowanego drogą pocztową*;
5. przedmiot wniosku z uzasadnieniem:
  - w przypadku sprostowania własnych nieprawidłowych danych przetwarzanych w SIS, proszę podać, jakie dane należy sprostować lub jakie są nieprawdzie i podać dane poprawne oraz wskazać uzasadnienie potwierdzające zasadność wniosku;
  - w przypadku usunięcia własnych danych osobowych przetwarzanych niezgodnie z prawem w SIS proszę podać, jakie dane należy usunąć oraz wskazać uzasadnienie potwierdzające zasadność usunięcia tych danych;
  - w przypadku wycofania przez osobę pokrzywdzoną przywłaszczeniem jej tożsamości zgody na przetwarzanie w SIS jej danych osobowych jako osoby pokrzywdzonej przywłaszczeniem tożsamości w uzupełnieniu wpisu danych SIS jako danych osoby, której tożsamością posługuje się osoba poszukiwana na podstawie wpisu danych SIS, - proszę we wniosku wyraźnie wskazać, że zgoda na przetwarzanie ww. danych z SIS została wycofana;
6. podpis osoby składającej wniosek *w przypadku wniosku w formie pisemnej (dokumentu w formie papierowej) - zawierającego podpis własnoręczny, a w przypadku wniosku w formie elektronicznej (dokumentu w formie elektronicznej) zawierającego podpis elektroniczny równoważny w skutkach prawnych z podpisem własnoręcznym, tj. kwalifikowany podpis elektroniczny, podpis zaufany lub podpis osobisty.*

Dodatkowo, w celu jednoznacznej identyfikacji danych, wnioskodawca może we wniosku podać:

1. nazwisko poprzednie/rodowe;
2. numer PESEL (jeżeli osoba posiada);
3. płeć;
4. miejsce zamieszkania (kraj, miejscowość, kod pocztowy, powiat/rejon, województwo/obwód, ulica i numeru domu/mieszkania);
5. dołączyć kserokopię strony dokumentu tożsamości zawierającej ww. dane osobowe.

W przypadku wątpliwości co do tożsamości osoby, która złożyła wniosek administrator może żądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby (art. 28 *ustawa p.d.o.z.p.* oraz art. 12 ust. 6 *RODO*).

### **3. Wniosek do COT KSI można kierować:**

a) w formie papierowej (*wniosek musi zawierać własnoręczny podpis osoby składającej wniosek lub działającego w jej imieniu pełnomocnika wraz z dokumentem pełnomocnictwa spełniającym wymogi, o których mowa powyżej w pkt VI*) drogą pocztową na adres:

Centralny Organ Techniczny KSI  
Komenda Główna Policji

ul. Puławska 148/150  
02-624 Warszawa  
Polska

b) w formie elektronicznej (*wniosek musi zawierać podpis elektroniczny równoważny w skutkach prawnych z podpisem własnoręcznym tj.. kwalifikowany podpis elektroniczny, podpis zaufany lub podpis osobisty osoby składającej wniosek albo działającego w jej imieniu pełnomocnika wraz z dokumentem pełnomocnictwa spełniającym wymogi, o których mowa powyżej w pkt VI)*) za pomocą następujących środków komunikacji elektronicznej:

przez [elektroniczną skrzynkę podawczą \(ePUAP\)](#) (tylko do dnia 31 grudnia 2025 r.)

publiczną usługą rejestrowanego doręczenia elektronicznego (e-Doręczenia) na adres:  
AE:PL-32148-68645-HUSFF-09

za pośrednictwem poczty elektronicznej na adres: [cot.admin.ksi@policja.gov.pl](mailto:cot.admin.ksi@policja.gov.pl)

#### **4. Wzór wniosku:**

W celu złożenia wniosku można skorzystać z [formularza wniosku dotyczącego przetwarzania danych osobowych w SIS](#)

## **WIZOWY SYSTEM INFORMACYJNY (VIS)**

### **1. Wniosek o dostęp do własnych danych osobowych przetwarzanych w VIS**

W tym celu należy złożyć pisemny wniosek w języku polskim, który obligatoryjnie powinien zawierać:

- a. imię/imiona i nazwisko składającego wniosek;
- b. obywatelstwo;
- c. datę i miejsce urodzenia (miejscowość i kraj);
- d. adres do korespondencji zwrotnej (kraj, miejscowość, kod pocztowy, powiat/rejon, województwo/obwód, ulica i numeru domu/mieszkania) - *w przypadku wniosku kierowanego drogą pocztową;*
- e. przedmiot wniosku;
- f. podpis osoby składającej wniosek *w przypadku wniosku w formie pisemnej (dokumentu w formie papierowej) – zawierającego podpis własnoręczny, a w przypadku wniosku w formie elektronicznej (dokumentu w formie elektronicznej) zawierającego podpis elektroniczny równoważny w skutkach prawnych z podpisem własnoręcznym, tj. kwalifikowany podpis elektroniczny, podpis zaufany lub podpis osobisty).*

Dodatkowo, w celu jednoznacznej identyfikacji danych, wnioskodawca może we wniosku podać:

- a. nazwisko poprzednie/rodowe;
- b. numer PESEL (jeżeli osoba posiada);

- c. płeć;
- d. dołączyć kserokopię strony dokumentu tożsamości zawierającej dane osobowe.

W przypadku wątpliwości co do tożsamości osoby, która złożyła wniosek administrator może żądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby (art. 28 ustawy p.d.o.z.p. oraz art. 12 ust. 6 RODO).

## **2. Wniosek o korektę błędnych danych przetwarzanych w VIS i usunięcie własnych danych osobowych bezprawnie przetwarzanych w VIS**

W tym celu należy złożyć pisemny wniosek w języku polskim, który obligatoryjnie powinien zawierać:

- a. imię/imiona i nazwisko składającego wniosek;
- b. obywatelstwo;
- c. datę i miejsce urodzenia (miejscowość i kraj);
- d. adres do korespondencji zwrotnej (kraj, miejscowość, kod pocztowy, powiat/rejon, województwo/obwód, ulica i numeru domu/mieszkania) - *w przypadku wniosku kierowanego drogą pocztową;*
- e. przedmiot wniosku z uzasadnieniem:
  - w przypadku korekty błędnych danych przetwarzanych w VIS, niezgodnych ze stanem faktycznym, proszę podać, jakie dane należy sprostować lub jakie są nieprawdzie i podać dane poprawne oraz wskazać uzasadnienie potwierdzające zasadność wniosku;
  - w przypadku usunięcia danych osobowych bezprawnie przetwarzanych w VIS proszę podać, jakie dane należy usunąć oraz wskazać uzasadnienie potwierdzające zasadność usunięcia tych danych;
- f. podpis osoby składającej wniosek *w przypadku wniosku w formie pisemnej (dokumentu w formie papierowej) - zawierającego podpis własnoręczny, a w przypadku wniosku w formie elektronicznej (dokumentu w formie elektronicznej) zawierającego podpis elektroniczny równoważny w skutkach prawnych z podpisem własnoręcznym, tj. kwalifikowany podpis elektroniczny, podpis zaufany lub podpis osobisty).*

Dodatkowo, w celu jednoznacznej identyfikacji danych, wnioskodawca może we wniosku podać

- a. nazwisko poprzednie/rodowe;
- b. numer PESEL (jeżeli osoba posiada);
- c. płeć;
- d. dołączyć kserokopię strony dokumentu tożsamości zawierającej dane osobowe.

W przypadku wątpliwości co do tożsamości osoby, która złożyła wniosek administrator może żądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby (art. 28 ustawy p.d.o.z.p. oraz art. 12 ust. 6 RODO).

### **3. Wniosek do COT KSI można skierować:**

**a.** w formie papierowej (*wniosek musi zawierać własnoręczny podpis osoby składającej wniosek lub działającego w jej imieniu pełnomocnika wraz z dokumentem pełnomocnictwa spełniającym wymogi, o których mowa powyżej w pkt VI*)) drogą pocztową na adres:

Centralny Organ Techniczny KSI  
Komenda Główna Policji  
ul. Puławska 148/150  
02-624 Warszawa  
Polska

**b.** w formie elektronicznej (*wniosek musi zawierać podpis elektroniczny równoważny w skutkach prawnych z podpisem własnoręcznym tj. kwalifikowany podpis elektroniczny, podpis zaufany lub podpis osobisty osoby składającej wniosek albo działającego w jej imieniu pełnomocnika wraz z dokumentem pełnomocnictwa spełniającym wymogi, o których mowa powyżej w pkt VI*)) tj. kwalifikowany podpis elektroniczny, podpis zaufany, podpis osobisty) za pomocą następujących środków komunikacji elektronicznej:

przez [elektroniczną skrzynkę podawczą \(ePUAP\)](#) (tylko do dnia 31 grudnia 2025 r.)

publiczną usługą rejestrowanego doręczenia elektronicznego (e-Doręczenia) na adres:  
AE:PL-32148-68645-HUSFF-09

za pośrednictwem poczty elektronicznej na adres: [cot.admin.ksi@policja.gov.pl](mailto:cot.admin.ksi@policja.gov.pl)

### **4. Wzór wniosku:**

W celu złożenia wniosku można skorzystać z [formularza wniosku dotyczącego przetwarzania danych osobowych w VIS](#).

## **DANE KONTAKTOWE**

### **W PRZYPADKU DODATKOWYCH PYTAŃ DOTYCZĄCYCH ZASAD SKŁADANIA WNIOSKÓW DO COT KSI**

Telefon :

[47 72 153 11](tel:477215311)

[47 72 153 36](tel:477215336)

[47 72 137 67](tel:477213767)

[47 72 138 04](tel:477213804)

### **PRAWO DO WNIESIENIA SKARGI I DO WYSTĄPIENIA Z ROSZCZENIEM O ZAPŁATĘ, ODSZKODOWANIE LUB ZADOŚĆUCZYNIENIE**

Każdej osobie, której dane są przetwarzane w Systemie Informacyjnym Schengen i Wizowym Systemie

Informacyjnym przysługuje prawo:

**1)** złożenia skargi do Prezesa Urzędu Ochrony Danych osobowych w przypadku stwierdzenia, że przetwarzanie danych osobowych w SIS lub VIS odbywa się z naruszeniem przepisów prawa o ochronie danych osobowych dotyczących przetwarzania danych osobowych w SIS lub VIS, w tym z naruszeniem odpowiednio przepisów *rozporządzenia 2018/1862, rozporządzenia 2018/1861 oraz rozporządzenia 2018/1860* lub *rozporządzenia ws. VIS i decyzji ws. VIS*.

Skargę można skierować:

- a. w formie pisemnej tradycyjnej na adres: Prezes Urzędu Ochrony Danych Osobowych, ul. Moniuszki 1A, 00-014 Warszawa, Polska
- b. w formie elektronicznej: przez elektroniczną skrzynkę podawczą dostępną na stronie:  
<https://www.uodo.gov.pl>

Szczegółowe informacje: [www.uodo.gov.pl](http://www.uodo.gov.pl)

**2)** wystąpienia z roszczeniem o zapłatę, odszkodowanie lub zadośćuczynienie jeżeli roszczenie wiąże się z naruszeniem jej praw w związku z wpisem jej danych w SIS lub VIS lub szkodą wyrządzoną naruszeniem tych praw, przeciwko podmiotowi (organowi), który ten wpis wprowadził do SIS lub VIS i który za niego odpowiada.

Takie roszczenie można skierować:

- a. w przypadku powództwa o roszczenie przeciwko podmiotom lub organom, będącym jednostkami organizacyjnymi Skarbu Państwa, które mają siedzibę w Rzeczypospolitej Polskiej, do sądu okręgowego na terytorium Rzeczypospolitej Polskiej właściwego według siedziby tego podmiotu (organu), tj. właściwego według siedziby państwowej jednostki organizacyjnej, z której działalnością wiąże się dochodzone roszczenie (art. 17 pkt 4<sup>5</sup> i art. 29 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego)
  - b. w przypadku powództwa o roszczenie przeciwko podmiotowi (organowi) mającemu siedzibę w innym państwie członkowskim UE do sądu właściwego według przepisów prawa krajowego tego państwa, w którym podmiot (organ), który dokonał wpisu w SIS lub VIS i którego dotyczy roszczenie, ma siedzibę.
-

## Akty prawne

[KONWENCJA WYKONAWCZA DO UKŁADU Z SCHENGEN z dnia 14 czerwca 1985 roku między Rządami Państw Unii Gospodarczej Beneluxu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach](#)

[ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY \(UE\) NR 265/2010 z dnia 25 marca 2010 r. zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenie \(WE\) nr 562/2006 w zakresie dotyczącym przepływu osób posiadających wizy długoterminowe](#)

[ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY \(UE\) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich](#)

[ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY \(UE\) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen \(SIS\) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia \(WE\) nr 1987/2006](#)

[ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY \(UE\) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen \(SIS\) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady \(WE\) nr 1986/2006 i decyzji Komisji 2010/261/UE](#)

[ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY \(WE\) NR 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego \(VIS\) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych \(rozporządzenie w sprawie VIS\)](#)

[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 \(ogólne rozporządzenie o ochronie danych\)](#)

[USTAWA z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym](#)

[USTAWA z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości](#)

[USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych](#)

[ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 3 marca 2023 r. w sprawie wzorów kart wpisu i wzorów kart zapytania o dane w Systemie Informacyjnym Schengen oraz sposobu ich wypełniania](#)

[ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 3 marca 2023 r. w sprawie dostępu i wzoru upoważnienia do dostępu do Krajowego Systemu Informatycznego \(KSI\) oraz przetwarzania danych poprzez Krajowy System Informatyczny \(KSI\)](#)

[ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 3 marca 2023 r. w sprawie trybu przekazywania Policji osób lub przedmiotów odnalezionych na skutek wglądu](#)

[do danych SIS, procedury postępowania w przypadkach ujawnienia tożsamości przywłaszczonej oraz sposobu i trybu współpracy organów z biurem SIRENE](#)

[ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 27 lutego 2023 r. w sprawie szkoleń osób mających dostęp do Krajowego Systemu Informatycznego \(KSI\) oraz kwalifikacji osób uprawnionych do przeprowadzania tych szkoleń](#)

[ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 6 marca 2023 r. w sprawie warunków technicznych dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny \(KSI\)](#)

[ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 3 marca 2023 r. w sprawie przetwarzania danych biometrycznych Systemu Informacyjnego Schengen](#)

[ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 27 czerwca 2011 r. w sprawie sposobu wykorzystywania Krajowego Systemu Informatycznego jako krajowego interfejsu Wizowego Systemu Informacyjnego](#)

## **Formularze**

[formularz wniosku dotyczącego przetwarzania danych osobowych w SIS](#)

[formularz wniosku dotyczącego przetwarzania danych osobowych w VIS](#)

### **Metryczka**

---

Data publikacji : 16.09.2025  
Data modyfikacji : 19.09.2025  
[Rejestr zmian](#)

Podmiot udostępniający informację:  
Komenda Główna Policji

Osoba udostępniająca informację:  
Renata Przesmycka Biuro Prawne KGP

Osoba modyfikująca informację:  
Renata Przesmycka