GRUPA KOORDYNUJĄCA NADZÓR NAD SIS II

SYSTEM INFORMACYJNY SCHENGEN

PRZEWODNIK DOTYCZĄCY KORZYSTANIA Z PRAWA DOSTĘPU

Sekretariat – adres korespondencyjny: rue Wiertz 60 - B-1047 Brussels
Biuro: rue Montoyer 30
E-mail : EDPS-sis@edps.europa.eu
Tel.: 02-283 19 13 - Fax : 02-283 19 50

Przewodnik ten został opracowany przez Grupę koordynującą nadzór nad SIS II

Adres: rue Wiertz 60 - B-1047 Brussels

Biuro: rue Montoyer 30

E-mail : EDPS-sis@edps.europa.eu

Tel.: 02-283 19 13

Fax : 02-283 19 50

SPIS TREŚCI

Osobom, których dane osobowe są gromadzone, przechowywane lub w inny sposób przetwarzane w systemie informacyjnym Schengen drugiej generacji (zwanym dalej „SIS II"), przysługuje prawo dostępu do danych, korekty nieścisłości oraz usunięcia danych wprowadzonych niezgodnie z prawem[1]. W niniejszym przewodniku opisano warunki korzystania z tych praw.

I. INFORMACJE OGÓLNE DOTYCZĄCE SYSTEMU INFORMACYJNEGO SCHENGEN DRUGIEJ GENERACJI (SIS II)

SIS II jest wielkoskalowym systemem informatycznym, który stworzono jako środek wyrównawczy w związku ze zniesieniem kontroli na granicach wewnętrznych i który ma na celu zapewnienie wysokiego poziomu bezpieczeństwa w obszarze wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej, między innymi, poprzez utrzymanie bezpieczeństwa i porządku publicznego oraz zagwarantowanie bezpieczeństwa na terytoriach państw członkowskich. SIS II został wprowadzony we wszystkich państwach członkowskich UE, z wyjątkiem Chorwacji, Cypru i Irlandii[2], a także w czterech państwach stowarzyszonych: Islandii, Norwegii, Szwajcarii i Liechtensteinie.

SIS II jest systemem informacyjnym umożliwiającym krajowym organom ścigania, sądowym i administracyjnym wykonywanie określonych zadań poprzez wymianę istotnych danych. Ograniczone prawa dostępu do systemu mają również europejskie agencje EUROPOL i EUROJUST.

Kategorie przetwarzanych informacji

SIS II zawiera dwie szeroko rozumiane kategorie informacji w postaci wpisów, które dotyczą, po pierwsze, *osób* poszukiwanych w celu aresztowania, zaginionych, poszukiwanych do celów postępowania sądowego, kontroli niejawnych lub szczególnych kontroli, bądź też obywateli państw trzecich podlegających odmowie pozwolenia na wjazd lub pobyt w strefie Schengen, i po drugie, *przedmiotów* - takich jak pojazdy, dokumenty, karty kredytowe przeznaczone do zajęcia lub wykorzystania jako dowód w postępowaniu karnym bądź niezbędne do kontroli niejawnych lub

[1] Prawa te przysługują na mocy art. 41 rozporządzenia (WE) nr 1987/2006 z dnia 20 grudnia 2006 w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) i art. 58 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania systemu informacyjnego Schengen drugiej generacji (SIS II).

[2] Informacje z lipca 2015 r. W Bułgarii i Rumunii utrzymano granice wewnętrzne, mimo że kraje te stosują SIS. Zjednoczone Królestwo ma dostęp do SIS, z wyjątkiem wpisów dokonanych w związku z odmową pozwolenia na wjazd na terytorium Schengen.

szczególnych kontroli.

Podstawa prawna

W zależności od rodzaju wpisu SIS II jest regulowany bądź rozporządzeniem (WE) 1987/2006 Parlamentu i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji – w odniesieniu do procedur dokonywania wpisów ujętych w tytule IV Traktatu ustanawiającego Wspólnotę Europejską - dawny pierwszy filar (zwanym dalej „rozporządzeniem SIS II"), bądź decyzją Rady 2007/533/JHA z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania systemu informacyjnego Schengen drugiej generacji w zakresie procedur ujętych w tytule VI Traktatu Unii Europejskiej - dawny trzeci filar (zwaną dalej „decyzją SIS II").

Kategorie przetwarzanych danych osobowych

Jeżeli wpis dotyczy osoby, informacja zawsze zawiera imię, nazwisko oraz pseudonimy, płeć, odesłanie do decyzji będącej powodem wpisu, a także działania, jakie należy podjąć. Wpis może również zawierać, w miarę dostępności, takie informacje jak wszelkie obiektywne szczególne cechy fizyczne niepodlegające zmianom; miejsce i data urodzenia; fotografie; odciski palców; obywatelstwo (obywatelstwa); informacja, czy dana osoba jest uzbrojona, agresywna lub czy jest uciekinierem; powód wpisu; organ dokonujący wpisu; odsyłacze do innych wpisów dokonanych w SIS II zgodnie z art. 37 rozporządzenia SIS II lub art. 52 decyzji SIS II.

Architektura systemu

SIS II składa się z (1) systemu centralnego (zwanego dalej „centralnym SIS II"), (2) systemu krajowego (zwanego dalej „N.SIS II") w każdym państwie członkowskim, który łączy się z centralnym SIS II oraz (3) infrastruktury łączności między systemem centralnym a systemami krajowymi zapewniającej zaszyfrowaną sieć wirtualną dedykowaną dla danych SIS II oraz umożliwiającą wymianę danych między organami odpowiedzialnymi za wymianę informacji dodatkowych (SIRENE Bureaux)[3].

II. PRAWA PRZYSŁUGUJĄCE OSOBOM, KTÓRYCH DANE SĄ PRZETWARZANE W SIS II

Zgodnie z zasadami ochrony danych wszystkim osobom, których dane są przetwarzane w systemie

[3] Dane w SIS II wprowadza się, aktualizuje, usuwa i wyszukuje za pośrednictwem poszczególnych systemów krajowych. System centralny, wykonujący funkcje nadzorcze i administracyjne, mieści się w Strasburgu, we Francji. System ten zapewnia usługi konieczne do wprowadzania i przetwarzania danych SIS II. Rezerwowy system centralny, zdolny do zapewnienia wszystkich funkcji głównego systemu centralnego w przypadku jego awarii, mieści się niedaleko Salzburga, w Austrii. Każde państwo członkowskie odpowiada za budowę, eksploatację i utrzymanie własnego systemu krajowego oraz za przyłączenie go do systemu centralnego. Ponadto każde państwo członkowskie wyznacza organ, krajowy urząd SIS II („urząd N.SIS II"), który na szczeblu centralnym odpowiada za system krajowy tego państwa. Organ ten odpowiada za sprawne działanie i bezpieczeństwo systemu krajowego.

SIS II, przysługują określone prawa wynikające z rozporządzenia SIS II i decyzji SIS II[4], które omówiono poniżej. Każdy, kto korzysta z dowolnego z tych praw, może złożyć wniosek do właściwego organu w wybranym przez siebie państwie, w którym funkcjonuje SIS II. Jest to możliwe, ponieważ wszystkie krajowe bazy danych (N.SIS II) są identyczne względem bazy danych systemu centralnego[5]. Z praw tych można zatem korzystać w dowolnym państwie używającym SIS II, niezależnie od państwa członkowskiego, w którym dokonano wpisu.

W przypadku gdy dana osoba korzysta z swojego prawa dostępu do danych, korekty nieścisłości oraz usunięcia danych wprowadzonych niezgodnie z prawem, składając stosowny wniosek, właściwe organy mają obowiązek odpowiedzi w ściśle określonym terminie. Oznacza to, że dana osoba jest informowana niezwłocznie, a w każdym razie nie później niż 60 dni od daty złożenia przez nią wniosku o uzyskanie dostępu, bądź też wcześniej, jeżeli prawo krajowe przewiduje krótszy okres[6]. Dana osoba jest również informowana o działaniach podjętych po skorzystaniu przez nią z prawa do korekty i usunięcia danych, niezwłocznie, a w każdym razie nie później niż trzy miesiące od daty złożenia przez nią wniosku o korektę lub usunięcie danych, bądź też wcześniej, jeżeli prawo krajowe przewiduje krótszy okres[7].

II.1. **Prawo dostępu**

Prawo dostępu oznacza możliwość uzyskania przez każdą osobę, która tego zażąda, wiedzy na temat informacji przechowywanych o niej w kartotece zgodnie z prawem krajowym. Jest to jedna z podstawowych zasad ochrony danych umożliwiająca osobom, których dane dotyczą, sprawowanie kontroli nad danymi osobowymi przechowywanymi przez strony trzecie. Prawo to jest określone wprost w art. 41 rozporządzenia SIS II i art. 58 decyzji SIS II.

Prawo dostępu jest wykonywane zgodnie z przepisami państwa członkowskiego, w którym składany jest wniosek. Procedury różnią się w zależności od kraju oraz przepisów dotyczących przekazywania danych wnioskodawcom. W przypadku gdy dane państwo członkowskie otrzyma wniosek o dostęp do wpisu, którego samo nie dokonało, musi umożliwić państwu, które dokonało wpisu, zajęcie stanowiska w sprawie możliwości udostępnienia danych wnioskodawcy[8]. Informacje nie są przekazywane osobie, której dotyczą dane, jeżeli jest to konieczne do realizacji uprawnionych działań w związku z wpisem lub dla ochrony praw i wolności innych osób.

[4] Zobacz w szczególności art. 41 rozporządzenia SIS II i art. 58 decyzji SIS II.
[5] Zobacz art. 4 ust. 1 lit. b) rozporządzenia i decyzji SIS II.
[6] Zobacz art. 41 ust. 6 rozporządzenia SIS II i art. 58 ust. 6 decyzji SIS II.
[7] Zobacz art. 41 ust. 7 rozporządzenia SIS II i art. 58 ust. 7 decyzji SIS II.
[8] Zobacz art. 41 ust. 3 rozporządzenia SIS II i art. 58 ust. 3 decyzji SIS II.

Obecnie istnieją dwa rodzaje systemu dostępu do danych przetwarzanych przez organy ścigania, a tym samym do danych SIS. W niektórych państwach członkowskich dostęp jest bezpośredni, w innych pośredni.

W przypadku **bezpośredniego dostępu** dana osoba składa wniosek bezpośrednio do organów posługujących się danymi (policji, *gendarmerie*, organów celnych itp.). O ile zezwala na to prawo krajowe, właściwy organ może przesłać wnioskodawcy dotyczące go informacje.

W przypadku **pośredniego dostępu** dana osoba przesyła swój wniosek o dostęp krajowemu organowi ds. ochrony danych państwa, w którym przedkładany jest wniosek. Organ ten rozpatruje wniosek przeprowadzając niezbędne weryfikacje i przesyła odpowiedź wnioskodawcy.

II.2. Prawo do korekty nieścisłości i usunięcia danych

Prawo dostępu jest uzupełnione prawem do korekty danych osobowych niezgodnych ze stanem faktycznym lub niekompletnych oraz prawo do żądania ich usunięcia, jeżeli są przechowywane niezgodnie z prawem (art. 41 ust. 5 rozporządzenia SIS II i 58 ust. 5 decyzji SIS II).

Zgodnie z przepisami Schengen, w ramach SIS II, do zmiany lub usunięcia wprowadzonych danych uprawnione jest wyłącznie państwo członkowskie, które dokonało wpisu (zob. art. 34 ust. 2 rozporządzenia SIS II i art. 49 ust. 2 decyzji SIS II). Jeżeli wniosek jest składany w państwie członkowskim, które nie dokonało wpisu, wówczas zainteresowane państwa członkowskie współpracują ze sobą w celu znalezienia rozwiązania poprzez wymianę informacji i dokonanie odpowiednich weryfikacji. Wnioskodawca powinien przedstawić uzasadnienie wniosku o wprowadzenie korekty lub usunięcie danych i zebrać wszelkie istotne informacje na jego poparcie.

II.3. Środki odwoławcze: prawo do złożenia skargi do organu ds. ochrony danych lub wszczęcia postępowania sądowego

Artykuł 43 rozporządzenia SIS II i art. 59 decyzji SIS II przewidują środki odwoławcze przysługujące osobom fizycznym w przypadku nieuwzględnienia ich wniosku. Każdy może wystąpić do sądów lub organów właściwych na mocy prawa krajowego dowolnego z państw członkowskich z wnioskiem o dostęp do informacji, skorygowanie, usunięcie lub uzyskanie informacji bądź o odszkodowanie w związku z dotyczącym go wpisem.

W przypadku otrzymania skargi o charakterze transgranicznym krajowe organy ds. ochrony danych powinny współpracować ze sobą w celu zagwarantowania praw osób, których dotyczą dane.

III. OPIS OBOWIĄZUJĄCYCH PROCEDUR W POSZCZEGÓLNYCH KRAJACH

Obowiązujące procedury w każdym państwie stosującym acquis Schengen, które powinny być stosowane przez osoby, które pragną skorzystać ze swoich praw dostępu do danych, ich poprawienia lub usunięcia, zostały opisane w rozdziałach IV - XXXII.

IV. AUSTRIA

1. Charakter gwarantowanego dostępu (bezpośredni, pośredni lub mieszany)

W Austrii przepisy o ochronie danych przewidują zasadniczo bezpośredni dostęp do informacji, innymi słowy wniosek o informacje należy kierować do organu odpowiadającego za przetwarzanie danych (tzw. *Auftraggeber*, czyli zleceniodawca), a organ ten musi udzielić odpowiedzi na wniosek. Zasada ta ma w myśl austriackiej ustawy o ochronie danych powszechne zastosowanie, zatem odnosiłaby sie też do informacji zawartych w SIS we wpisach dokonanych na podstawie art. 24 rozporządzenia SIS II i art. 26, 32, 34, 36 oraz 38 Decyzji SIS II.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wniosek o informacje zainteresowany powinien kierować do organu policji (jako zleceniodawcy), od którego pragnie sie dowiedzieć, czy przetwarzał jego dane.

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

W myśl §26 ustawy o ochronie danych z roku 2000 (*Datenschutzgesetz (DSG) 2000*) zleceniodawca musi udzielić zainteresowanemu informacji:

– jeżeli zainteresowany wystąpił z pisemnym (lub – za zgoda zleceniodawcy – ustnym) żądaniem oraz

– jeżeli zainteresowany w odpowiedniej formie potwierdzi swoja tożsamość (np. kopia dowodu osobistego).

Udzielając informacji, zleceniodawca musi wskazać w ogólnie zrozumiałej formie:

– przetwarzane dane

– źródło ich pochodzenia

– wszystkich odbiorców lub wszystkie kręgi odbiorców je otrzymujących

– cel wykorzystania danych

– podstawy prawne

– na żądanie zainteresowanego – także nazwy i adresy usługodawców przetwarzających dane.

Informacji nie udziela sie:

– jeżeli ze szczególnych powodów wymaga tego ochrona samego zainteresowanego

– jeżeli przeszkoda jest wyższej wagi uzasadniony interes zleceniodawcy lub osoby trzeciej

– jeżeli przeszkoda jest wyższej wagi interes publiczny wynikający z potrzeby, aby:

• chronić konstytucyjne instytucje Republiki Austrii lub

• zapewnić gotowość operacyjną federalnych sił zbrojnych lub

• chronić interes szeroko pojętej obrony kraju lub
• chronić ważne interesy Republiki Austrii lub Unii Europejskiej w dziedzinie polityki zagranicznej, gospodarczej lub finansowej lub
• uprzedzać, uniemożliwiać lub ścigać czyny zabronione.

Ilekroć odmawia sie udzielenia informacji przez wzgląd na interes publiczny w dziedzinie ochrony porządku publicznego (lub ponieważ w rzeczywistości żadne dane nie są wykorzystywane), należy w odpowiedzi stwierdzić, że nie wykorzystuje sie żadnych danych zainteresowanego objętych obowiązkiem udzielenia informacji (pkt 5).

Odmowy udzielenia informacji podlegają kontroli ze strony organu ochrony danych (*Datenschutzbehörde*) i specjalnej procedurze odwoławczej.

Informacji można nie udzielać, jeżeli zainteresowany nie pomaga w procedurze informacyjnej lub nie uiścił prawnie należnej opłaty.

Zainteresowany musi w rozsądnym zakresie pomagać w procedurze informacyjnej, udzielając koniecznych wyjaśnień.

W terminie 8 tygodni zleceniodawca musi udzielić informacji lub na piśmie uzasadnić częściową lub całkowita odmowę ich udzielenia.

Informacji należy udzielić nieodpłatnie, jeżeli zapytanie dotyczy aktualnego zbioru danych i jeżeli jest pierwszym zapytaniem zgłoszonym przez zainteresowanego w danym roku.

W innych przypadkach można pobrać ryczałtowa opłatę w wysokości 18,89 EUR, która może sie zmienić w razie faktycznie większych kosztów. Pobrana opłatę należy zwrócić, jeżeli w wyniku udzielenia informacji doszło do sprostowania danych.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Datenschutzbehörde
Hohenstaufengasse 3
A - 1010 Vienna
Tel.: +43 1 531 15/2525
Fax: +43 1 531 15/2690
E-mail:
dsb@dsb.gv.at

Jeżeli organ policji nie dotrzyma 8-tygodniowego terminu (tzn. zainteresowany nie uzyska odpowiedzi) lub jeżeli zainteresowany otrzyma odpowiedź informującą go, że nie wykorzystuje sie

żadnych jego danych objętych obowiązkiem udzielenia informacji, może odwołać sie do organu ochrony danych zgodnie z §31 pkt 1 i 4 ustawy o ochronie danych z roku 2000.

Jeżeli w postępowaniu odwoławczym toczącym sie w myśl §31 pkt 4 ww. ustawy zleceniodawca powoła sie na konieczność zachowania tajemnicy z uwagi na wyższej wagi interes publiczny, organ ochrony danych musi sprawdzić, czy zachowanie tajemnicy było konieczne, a jeżeli względem zainteresowanego nie było ono uzasadnione, musi nakazać udzielenie mu informacji.

Odnośny organ może jednak odwołać sie do Naczelnego Sadu Administracyjnego (*Verwaltungsgerichtshof*). Jeżeli tego nie robi, musi w terminie 8 tygodni wypełnić decyzję organu ochrony danych, inaczej organ sam udzieli zainteresowanemu żądanych informacji.

5. Najważniejsze przepisy krajowe

§26 ustawy o ochronie danych z roku 2000 (DSG 2000), Federalny Dziennik Urzędowy (*Bundesgesetzblatt*) I, nr 165/1999.

§26 (1) każdej osobie, która o to wystąpi na piśmie i w odpowiedniej formie wykaże swoją tożsamość, zleceniodawca musi udzielić informacji o danych przetwarzanych w związku z jej osobą. Za zgoda zleceniodawcy żądanie informacji może mieć formę ustną. Udzielając informacji, należy w ogólnie zrozumiałej formie wskazać przetwarzane dane, źródło ich pochodzenia, wszystkich odbiorców lub wszystkie kręgi odbiorców je otrzymujących, cel ich wykorzystania i podstawy prawne. Na żądanie zainteresowanego należy także podać nazwy i adresy podmiotów wykonujących usługę przetwarzania danych. Za zgoda zainteresowanego można udzielić informacji nie na piśmie, ale ustnie, zapewniając jednak możliwość wglądu, wykonania odpisu lub kserokopii.

(2) Informacji nie udziela sie, jeżeli ze szczególnych powodów wymaga tego ochrona samego zainteresowanego lub jeżeli przeszkoda jest wyższej wagi uzasadniony interes zleceniodawcy lub osoby trzeciej, a zwłaszcza wyższej wagi interes publiczny. Taki wyższej wagi interes publiczny może wynikać z potrzeby, aby:

1. chronić konstytucyjne instytucje Republiki Austrii lub
2. zapewnić gotowość operacyjna federalnych sił zbrojnych lub
3. chronić interes szeroko pojętej obrony kraju lub
4. chronić ważne interesy Republiki Austrii lub Unii Europejskiej w dziedzinie polityki zagranicznej, gospodarczej lub finansowej lub
5. uprzedzać, zapobiegać lub ścigać czyny zabronione.

Słuszność odmowy udzielenia informacji z powyższych powodów podlega kontroli ze strony organu ochrony danych na mocy §30 pkt 3 i może być kwestionowana przed tym organem w specjalnej procedurze odwoławczej na mocy §31 pkt 4.

(3) Zainteresowany musi w rozsądnym zakresie pomagać w procedurze informacyjnej, udzielając koniecznych wyjaśnień, aby zaoszczędzić zleceniodawcy nieuzasadnionego i nieproporcjonalnego nakładu pracy.

(4) W terminie 8 tygodni od otrzymania żądania należy udzielić informacji lub na piśmie uzasadnić częściową lub całkowita odmowę ich udzielenia. Informacji można także nie udzielać, jeżeli wbrew pkt 3 zainteresowany nie pomaga w procedurze informacyjnej lub jeżeli nie uiścił prawnie należnej opłaty.

(5) W dziedzinach ochrony porządku publicznego, które obejmują zadania wskazane w pkt 2 pkt 1–5, należy – o ile jest to konieczne do ochrony wspomnianego interesu publicznego, który nakazuje odmówić udzielenia informacji – postępować następująco: ilekroć odmawia sie udzielenia jakichkolwiek informacji – także z tego powodu, że w rzeczywistości żadne dane nie są wykorzystywane – należy zamiast podawać merytoryczne uzasadnienie, stwierdzić, że nie wykorzystuje sie żadnych danych zainteresowanego objętych obowiązkiem udzielenia informacji. Słuszność takiego postępowania podlega kontroli ze strony organu ochrony danych na mocy §30 pkt 3 i może być kwestionowana przed tym organem w specjalnej procedurze odwoławczej na mocy §31 pkt 4.

(6) Informacji należy udzielić nieodpłatnie, jeżeli zapytanie dotyczy aktualnego zbioru danych i jeżeli jest pierwszym zapytaniem w danej materii zgłoszonym zleceniodawcy przez zainteresowanego w bieżącym roku. W innych przypadkach można pobrać ryczałtowa opłatę w wysokości 18,89 EUR, która może sie zmienić w razie faktycznie większych kosztów. Każda uiszczona opłata podlega zwrotowi, niezależnie od jakichkolwiek roszczeń odszkodowawczych, jeżeli dane zostały wykorzystane nielegalnie lub jeżeli w wyniku udzielenia informacji doszło do sprostowania danych.

(7) Od momentu gdy zleceniodawca dowiaduje sie o żądaniu udzielenia informacji, nie wolno mu przez 4 miesiące niszczyć danych dotyczących zainteresowanego, a jeżeli następuje odwołanie do organu ochrony danych w myśl §31 – nie wolno ich niszczyć, dopóki postępowanie sie nie zakończy.

(8) Jeżeli z mocy przepisów zbiory danych są dostępne do publicznego wglądu, zainteresowani maja prawo do informacji w takim stopniu, w jakim zachodzi prawo do wglądu. Wgląd możliwy jest w trybie określonym szczegółowymi przepisami ustawy o utworzeniu rejestru publicznego.
(9) Udzielanie informacji z rejestru karnego jest regulowane specjalnymi przepisami ustawy o rejestrze karnym z roku 1968 dotyczącej wyciągów z tego rejestru.
(10) Jeżeli usługodawca zgodnie z §6 pkt 4 decyduje samodzielnie na podstawie przepisów lub zasad postępowania, by posłużyć się zgodnie z §4 pkt 4 zdanie 3 określoną aplikacją do przetwarzania danych, to zainteresowany może początkowo wystąpić z żądaniem informacji do zlecającego wykonanie tej aplikacji. Zlecający musi bezzwłocznie i nieodpłatnie podać zainteresowanemu – o ile nie posiada on jeszcze tych informacji – nazwę i adres faktycznego samodzielnego usługodawcy, tak by zainteresowany mógł dochodzić swoich praw wobec niego zgodnie z pkt 1.

6. Wymagany język

W myśl przepisów austriackich zainteresowany musi do wszczęcia postępowania o dostęp użyć języka niemieckiego.

V. BELGIA

1. Charakter gwarantowanego prawa dostępu

Każdy ma prawo do pośredniego dostępu do swoich danych osobowych przetwarzanych przez organy policji. Aby skorzystać z tego prawa, należy skierować wniosek do komisji ochrony prywatności.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Commissie voor de bescherming van de persoonlijke levenssfeer

Drukpersstraat 35, 1000 Brussel

Commission de la protection de la vie privée

Rue de la Presse, 35, 1000 Bruxelles

+32 (0)2 274 48 00

+32 (0)2 274 48 35

commission@privacycommission.be

Website: http://www.privacycommission.be

3. Kwestie formalne: potrzebne informacje i dokumenty

Wnioski należy przesyłać komisji pismem opatrzonym datą i podpisem. W piśmie należy podać nazwisko i imię, datę urodzenia oraz obywatelstwo zainteresowanego oraz załączyć kserokopie jego dowodu osobistego.

Należy podać (jeżeli znane) nazwę go organu lub odnośnych służb oraz wszelkie istotne informacje na temat kwestionowanych danych: ich rodzaj, okoliczności ich wykrycia oraz źródło, a także wskazać, jakich działań się oczekuje.

Procedura jest bezpłatna.

4. Oczekiwany skutek. Treść podawanych informacji

Po otrzymaniu wniosku o pośredni dostęp do danych osobowych przetwarzanych przez organ policji komisja dokonuje niezbędnych kontroli w odnośnym organie.

Po ich zakończeniu komisja informuje zainteresowanego o ich przeprowadzeniu. W odpowiednich

przypadkach – jeżeli organ policji przetwarzał dane w celu kontroli tożsamości – po konsultacji z odnośnym organem komisja przesyła zainteresowanemu wszelkie informacje, jakie uzna za stosowne.

5. Najważniejsze przepisy krajowe

– ustawa z dnia 8 grudnia 1992 r. o ochronie prywatności w przetwarzaniu danych osobowych, zmieniona ustawa z dnia 11 grudnia 1998 r., która przeniosła do prawa krajowego dyrektywę 95/46/WE z dnia 24 października 1995 r., zwłaszcza jej art. 13

– dekret królewski z dnia 13 lutego 2001 r. wdrążający ustawę z dnia 8 grudnia 1992 r. o ochronie prywatności w przetwarzaniu danych osobowych, zwłaszcza jej art. 36–46.

VI. BUŁGARIA

1. Charakter gwarantowanego prawa dostępu

Każda osoba ma prawo dostępu do danych osobowych jej dotyczących, zbieranych bez jej wiedzy i przetwarzanych przez Ministerstwo Spraw Wewnętrznych (MSW) lub w SIS, i powinna skierować wniosek o dostęp do krajowego Biura SIRENE, ustanowionego w ramach Dyrektoratu ds. Międzynarodowej współpracy operacyjnej w MSW.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Ministerstwo Spraw Wewnętrznych Republiki Bułgarii
Sofia, 1000
29 "6-th September" str.
Tel.: + 359 2/9825000 – Kancelaria MSW
Strona internetowa: http://www.mvr.bg/contactus.htm

3. Kwestie formalne: potrzebne informacje i dokumenty – potencjalne koszty

Każdy ma prawo korzystania ze swoich praw poprzez złożenie pisemnego wniosku (osobiście lub poprzez wyraźnie upoważnioną osobę z notarialnym potwierdzeniem pełnomocnictwa) do administrator danych (w tym wypadku Ministerstwa Spraw Wewnętrznych).

Wniosek może być także złożony mailem na podstawie procedury wskazanej w ustawie o dokumencie elektronicznym i elektronicznym podpisie.
Minister Spraw Wewnętrznych obowiązany jest do podjęcia decyzji w ciągu 14 dni od otrzymania wniosku. Kopia przetwarzanych danych osobowych może zostać przekazana na wniosek osoby, której dane dotyczą.
Złożenie wniosku o dostęp do danych w SIS jest bezpłatne.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Komisja Ochrony Danych Osobowych (ang. Commission for Personal Data Protection)

Sofia 1592, 2 “Prof. Tsvetan Lazarov” blvd.

Informacja - Tel.: + 3592/91-53-518

Rejestry:

Tel.: + 3592/91-53-515, 02/91-53-519

Fax: +3592/91-53-525

E-mail: kzld@cpdp.bg

Strona internetowa: www.cpdp.bg

Każdy ma prawo zwrócić się do CPDP z wnioskiem o sprawdzenie dotyczących go danych, które są przetwarzane w SIS II, a także ma prawo otrzymać informacje o ich wykorzystaniu. Jeśli dane zostały wprowadzone przez inne państwo członkowskie, CPDP przeprowadzi sprawdzenie we współpracy z organem nadzorczym danego państwa.

- Jeśli administrator (MSW) nie rozpatrzył wniosku osoby o dostęp i uważa ona, że doszło naruszenia LPPD poprzez przetwarzanie danych jej dotyczących (np. utrudnianie korzystania z przysługujących praw), może ona złożyć skargę do CPDP (w ramach postępowania administracyjnego). Jeśli osoba, której dane dotyczą, nie złoży skargi do CPDP, może ona złożyć odwołanie od decyzji (o odmowie dostępu lub przekazania informacji lub utrudnianie realizacji prawa do usunięcia, poprawienia lub zablokowania danych) do sądu. Komisja Ochrony Danych Osobowych rozpatruje skargi i podejmuje decyzje, które po ich wejściu w życie są wiążące dla administratorów danych. Jeśli przedmiotem skargi była odmowa dostępu do danych, decyzja CPDP może zobowiązać administratora do wykonania dostępu i udzielać wskazówek w tym zakresie.

- Jeśli wykryto naruszenie przetwarzania danych osobowych, CPDP może nakładać kary administracyjne – kary lub sankcje materialne, na administrator danych.

5. Oczekiwany skutek. Treść podawanych informacji

W ustawie o Ministerstwie Spraw Wewnętrznych (MIA) przewidziano, że każdy ma prawo do dostępu do dotyczących go danych osobowych, zbieranych bez jego wiedzy i przetwarzanych przez MSW w swoich zasobach. Administrator zobowiązany jest do odpowiedzi w ciągu 14 dni od otrzymania wniosku o dostęp. Jeśli osoba wyrazi taką wolę, może otrzymać papierową kopię danych jej dotyczących. MSW odmawia całkowicie lub częściowo odmawia przekazania danych:

- jeśli zagraża to bezpieczeństwu narodowemu lub porządkowi publicznemu; - dla ochrony informacji oklauzulowanych jako państwowa lub urzędowa tajemnica; jeśli źródło informacji lub powiązane metody i środki ich pozyskania mogłyby zostać ujawnione; - jeśli przekazanie tych danych może stanowić odstępstwo od zadań MSW wykonywanych na podstawie prawa; - informacje zostały wprowadzone do SIS przez inne państwo, które nie wyraziło zgody. Osoby, których dane dotyczą, są informowane pisemnie o podstawach prawnych odmowy. Jeśli odpowiedź nie zostanie przesłane w ramach czasowych przewidzianych prawem jest to odbierane jako odmowa. Zgodnie z art. 161 MIA, odmowa może być przedmiotem odwołania w ramach procedury przewidzianej w Administracyjnym Kodeksie Karny.

6. Najważniejsze akty prawne

- Ustawa o Ministerstwie Spraw Wewnętrznych SG 17/24.02.2006, z późn. zm. z dnia 70/09.08.2013, w mocy od 09.08.2013.

- rozporządzenia wdrażające ustawę o Ministerstwie Spraw Wewnętrznych – przyjęte Dekretem Rady Ministrów 126/02.06.2006, SG 47/09.06.2006, z późn. zm. z dnia 10/04.02.2014.

- Zarządzenie 2727 z dnia 16 listopada 2010 w sprawie organizacji i funkcjonowania Krajowego Systemu Informacyjnego Schengen Republiki Bułgarii – wydany przez MSW, w mocy od dnia 30.11.2010, zmieniony SG 28/19.03.2013.

- Zarządzenie zmieniające i uzupełniające Zarządzenie 2727 dnia 16 listopada 2010 w sprawie organizacji i funkcjonowania Krajowego Systemu Informacyjnego Schengen Republiki Bułgarii – wydany przez MSW, w mocy od dnia 30.11.2010, zmieniony SG 28/19.03.2013
- Ustawa o ochronie danych osobowych SG 1/04.01.2002, zmieniony SG 15/15.02.2013.

6. Wymagany język

Wniosek o dostęp do danych przetwarzanych w Systemie Informacyjnym Schengen powinien zostać złożony po bułgarsku.

VII. CZECHY

1. Charakter gwarantowanego dostępu

Osoba, której dotyczą dane, ma prawo do bezpośredniego dostępu. Swoich praw względem danych przechowywanych w SIS powinna ona dochodzić zasadniczo przed administratorem tych danych, czyli Policja Republiki Czeskiej.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Police Presidium of the Czech Republic [*prezydium policji Republiki Czeskiej*]
P. O. Box 62/K-SOU
Strojnická 27
170 89 Praha 7

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Tryb występowania o informacje na temat danych lub o sprostowanie bądź usuniecie danych (w tym formularze) przedstawiono na stronie Urzędu Ochrony Danych Osobowych (www.uoou.cz). Informacje można też znaleźć na stronach policji (www.policie.cz) i Ministerstwa Spraw Wewnętrznych (http://www.mvcr.cz/eu-schengen.aspx), jak również na czeskich stronach poświeconych ogólnie sprawom europejskim (www.euroskop.cz).

W ramach prawa do informacji i do żądania sprostowania lub usunięcia swoich danych przetwarzanych w SIS każdy zainteresowany może wysłać pisemny wniosek do Policji Republiki Czeskiej (na podany wyżej adres). Informacje o przetwarzaniu danych osobowych w SIS są ujawniane wyłącznie osobie, której te dane dotyczą (lub jej zastępcy prawnemu). We wniosku należy określić swoja tożsamość, podając pełne imię (imiona), nazwisko, datę i miejsce urodzenia oraz adres. Policja ma obowiązek zareagować w ciągu 60 dni. Korzystanie z prawa do dostępu jest bezpłatne.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

The Office for Personal Data Protection
Pplk. Sochora 27
170 00 Praha 7

Urząd Ochrony Danych Osobowych jest organem właściwym, by na wniosek zainteresowanego skontrolować przetwarzanie danych osobowych w krajowym module SIS, jeżeli zachodzi podejrzenie o nielegalność procedur lub jeżeli administrator danych (Policja Republiki Czeskiej) nie udzielił zadowalającej odpowiedzi.

5. Oczekiwany skutek. Treść podawanych informacji

Policja powinna w odpowiedzi określić, czy i jakie dane osobowe zainteresowanego są przechowywane w SIS, dlaczego (w jakim celu) zostały wprowadzone do systemu i przez jaki organ.

Zgodnie z art. 83/4 ustawy o policji policja nie przychyla sie do wniosku, jeżeli jego realizacja mogłaby narazić na niepowodzenie czynności policyjne prowadzone w ramach postępowania karnego, zagrozić bezpieczeństwu narodowemu lub zaszkodzić uzasadnionym interesom osoby trzeciej.

6. Najważniejsze przepisy krajowe

Ustawa nr 101/2000 Zb. o ochronie danych osobowych i o zmianie niektórych ustaw (art. 12 i 21).

Ustawa nr 273/2008 Zb. o Policji Republiki Czeskiej (art. 83 i 84).

7. Wymagany język

Jedynym urzędowym językiem komunikacji z organami czeskimi jest czeski. Niemniej z czeskim urzędem ochrony danych można też porozumiewać sie po angielsku. Także po angielsku są podane na jego stronach podstawowe informacje o trybie występowania o dostęp.

VIII. DANIA

1. Charakter gwarantowanego dostępu

Osoba, której dotyczą dane, ma prawo do bezpośredniego dostępu.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski o dostęp należy kierować do policji, która jest administratorem danych:

Rigspolitiet [*policja panstwowa*]

Polititorvet 14

DK-1780 København V

Tel.: +45 33 14 88 88

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Nie ma szczególnych wymogów formalnych co do wysyłanych wniosków.

Reakcja na wniosek powinna nastąpić maksymalnie szybko, a jeżeli wyjątkowo nie można udzielić odpowiedzi w ciągu 4 tygodni, administrator danych musi o tym powiadomić zainteresowanego. Powinien wtedy określić, dlaczego decyzja nie może zapaść w terminie 4 tygodni oraz kiedy można sie jej spodziewać.

Zasadniczo, jeżeli zażąda tego zainteresowany, odpowiedzi są udzielane na piśmie. Jeżeli zainteresowany stawi sie u administratora danych osobiście, należy ustalić, czy pragnie on pisemnej czy tylko ustnej informacji na temat treści danych.

Wnioski o dostęp rozpatrywane są bezpłatnie.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Datatilsynet [*inspekcja danych*]

Borgergade 28, 5. sal

DK-1300 København K

Tel.: +45 3319 3200

Faks: +45 3319 3218

E-mail: dt@datatilsynet.dk

www.datatilsynet.dk

W urzędzie tym można składać skargi na decyzje policji w sprawie dostępu. Rozpatrując je, urząd

analizuje sprawę i sprawdza, czy żadnych danych nie wprowadzono do systemu wbrew postanowieniom rozporządzenia i decyzji SIS II.

5. Oczekiwany skutek. Treść podawanych informacji

Zgodnie z sekcją 31 (1) ustawy o przetwarzaniu danych osobowych administrator (w tym przypadku policja) musi poinformować zainteresowanego, czy jego dane są przetwarzane. Jeżeli są, należy go w sposób zrozumiały poinformować, jakie dane są przetwarzane, w jakim celu, jakim kategoriom odbiorców są przekazywane oraz (maksymalnie wyczerpująco) z jakich źródeł pochodzą.

Zgodnie z sekcją 32 (1) w związku z sekcja 30 (2) ustawy obowiązek ten nie ma zastosowania, jeżeli stwierdzi sie, że interes wnioskodawcy polegający na uzyskaniu informacji jest podrzędny względem istotnego interesu publicznego dotyczącego m.in.:

(1) bezpieczeństwa narodowego

(2) ……

(3) bezpieczeństwa publicznego

(4) uprzedzania, ścigania, wykrywania i karania przestępstw oraz naruszeń etyki zawodowej w zawodach regulowanych

(5) …….

(6) ……..

6. Najważniejsze przepisy krajowe

Ustawa nr 429 z dnia 31 maja 2000 r. o przetwarzaniu danych osobowych.

7. Wymagany język

Duński jest językiem oficjalnym w komunikacji z duńskimi urzędami. Tym niemniej istnieje także możliwość komunikacji w języku angielskim.

IX. ESTONIA

1. Charakter prawa dostępu

Bezpośredni, ale jeśli osoba złoży wniosek do organu ochrony danych osobowych, nie jest odsyłana do przetwarzającego dane, ale to organ prosi o informacje I następnie przekazuje je osobie, której dane dotyczą.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Zarząd Policji i Straży Granicznej (ang. Police and Border Guard Board)

Pärnu mnt 139

15060 TALLINN

tel. 612 3300

fax +372 612 3009

ppa@politsei.ee

www.politsei.ee

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Wniosek/prośba podpisana cyfrowo lub ręcznie, kopia dowodu osobistego lub paszportu. Złożenie wniosku jest bezpłatne.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Data Protection Inspectorate

Väike-Ameerika 19, 10129

Tallinn, Estonia

info@aki.ee

www.aki.ee

Organ ochrony danych ma prawo nadzorowania wpisów i stanowiących ich podstawę dokumentów, próśb o dostęp, usunięcie lub poprawienie danych osobowych poprzez właściwe postępowanie w sprawie wykroczeń. Przedstawiciele organu ochrony danych osobowych mają prawo do wejścia dla celów inspekcji, bez przeszkód, do siedziby przetwarzającego dane osobowe, do dostępu do

dokumentów i urządzeń, jak też zarejestrowanych danych i oprogramowania wykorzystywanego do przetwarzania danych osobowych.

5. Oczekiwany skutek. Treść podawanych informacji

Oczekiwanym skutkiem jest udzielenie dostępu, o ile jest to przewidziane przez prawo. W wypadku ochrony postępowań karnych itp. dostęp do danych jest ograniczony. Organ ochrony danych może sprawdzić słuszność takiego ograniczenia. Krajowy termin to 30 dni.

6. Najważniejsze przepisy krajowe

Ustawa o ochronie danych

Ustawa o Policji i Strazy Granicznej

Statuty dot. utrzymania krajowego rejestru Systemu Informacyjnego Schengen

7. Wymagany język

Akceptowane są wnioski po estońsku, angielsku i rosyjsku, które są najczęściej używanymi językami. Odpowiedzi udzielane są po estońsku i angielsku.

X. FINLANDIA

1. Charakter gwarantowanego dostępu

Osoba, której dotyczą dane, ma prawo do bezpośredniego dostępu.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wniosek należy składać osobiście w miejscowej komendzie policji.

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Wniosek należy złożyć na policji osobiście, okazując dowód tożsamości.

Za korzystanie z prawa do wglądu opłata należy sie tylko wtedy, gdy od poprzedniego razu, kiedy zainteresowany korzystał z tego prawa, nie minął rok.

Administrator rejestru musi bez zbędnej zwłoki umożliwić zainteresowanemu wgląd do przechowywanych danych, a na żądanie – udzielić informacji na piśmie.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Albertinkatu 25 A
PL 315,
FIN - 00181 Helsinki
Tel.: ++358 (0)10 36 66700
Faks: ++358 (0)10 36 66735
E-mail: tietosuoja@om.fi
Strona internetowa: www.tietosuoja.fi

Jeżeli na podstawie sekcji 27 ustawy o danych osobowych policja odmówi zgody na wgląd do danych przechowywanych w SIS, musi wydać odpowiednie zaświadczenie i poinstruować zainteresowanego, by skontaktował sie z urzędem ochrony danych. Wtedy zainteresowany będzie mógł przedstawić sprawę do rozpatrzenia urzędowi.

W kwestiach dotyczących prawa do wglądu urząd ochrony danych wydaje wiążące decyzje. Od jego decyzji można sie odwołać do właściwego sadu administracyjnego, a dalej do Naczelnego Sądu Administracyjnego (sekcja 28 i 29 ustawy o danych osobowych).

5. Najważniejsze przepisy krajowe

Ustawa o ochronie danych (523/1999)

Ustawa o ochronie danych policyjnych (761/2003).

XI. FRANCJA

1. Charakter gwarantowanego dostępu

Dostęp ma charakter mieszany. Dostęp jest bezpośredni dla osób poszukiwanych (art. 32 decyzji 2007/533) lub dla osób wskazanych lub zidentyfikowanych we wpisach dotyczących przedmiotów (art. 38 ww. decyzji).

We wszystkich pozostałych przypadkach dostęp do danych w SIS jest pośredni i może być wykonywany tylko poprzez Krajową Komisję Informatyki i Wolności (CNIL).

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski w wymienionych przypadkach, w których zachodzi prawo do dostępu bezpośredniego, należy kierować bezpośredni pod adres:

Direction générale de la police nationale [*dyrekcja generalna policji krajowej*]

Ministère de l'Intérieur [*ministerstwo spraw wewnętrznych*]

11 rue des Saussaies

F - 75008 Paris

Tel.: +33(0)1.49.27.49.27

Faks: ---

E-mail: ---

Internet: www.interieur.gouv.fr

We wszystkich pozostałych przypadkach wnioski należy adresować:

Commission nationale de l'informatique et des libertés [*krajowa komisja informatyki i wolności*]

8, rue Vivienne – CS 30223

F - 75083 PARIS CEDEX 02

Tel.: ++33 1 53 73 22 22

Faks: ++33 1 53 73 22 00

E-mail: bmonegier@cnil.fr

Internet: www.cnil.fr

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Z prawa do dostępu można korzystać jedynie osobiście. Wnioski musza być składane osobiście przez samych zainteresowanych (w żadnym wypadku przez krewnego) lub przez prawników działających z ich ramienia.

Nie ma szczególnych wymogów formalnych. Zainteresowany musi jedynie podać swoje nazwisko, imię, datę i miejsce urodzenia oraz dołączyć do wniosku czytelna kserokopie dokumentu tożsamości. Dołączyć należy też kopie wszelkich odnośnych dokumentów (zawiadomienie o odmowie wydania wizy na podstawie wpisu do SIS, korzystną dla zainteresowanego decyzję sadowa uchylającą nakaz wydalenia).

Procedura uzyskiwania dostępu jest bezpłatna.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Commission nationale de l'informatique et des libertés [*krajowa komisja informatyki i wolnosci*]

8, rue Vivienne – CS 30223

F - 75083 PARIS CEDEX 02

Tel.: ++33 1 53 73 22 22

Faks: ++33 1 53 73 22 00

E-mail: bmonegier@cnil.fr

Internet: www.cnil.fr

5. Oczekiwany skutek. Treść podawanych informacji

Po dokonaniu sprawdzenia, jego wynik jest przekazywany wnioskującemu, który jest przedmiotem wpisu, jeśli członek Komisji stwierdzi, w porozumieniu z administratorem, że ujawnienie danych nie osłabia jego celów, bezpieczeństwa państwa, obrony oraz bezpieczeństwa publicznego.

Jeśli administrator danych sprzeciwia się ujawnieniu informacji (np. osoba jest poddawana kontroli niejawnej, wydano nakaz aresztowania wobec niej, wydano zakaz wjazdu do kraju ze względu na porządek publiczny), Komisja informuje wnioskującego, że niezbędne sprawdzenia zostały wykonane, ale dalsze informacje nie mogą zostać mu przekazane (*Artykuł 88 Dekretu nr 2005-1309 w dniu 20 października 2005 wprowadzone do stosowania ustawą nr 78-17 w sprawie technologii informacyjnych, zbiorów danych i swobód obywatelskich*). Komisja informuje również wnioskującego o środkach i okresie, w jakim może złożyć swój sprzeciw.

Jeśli wnioskujący, jest przedmiotem wpisu, wprowadzonego przez inne państwo, CNIL będzie współpracował z organem ochrony danych osobowych tego państwa.

Jeśli sprawdzenia doprowadzą do usunięcia wpisu dot. wnioskującego, wnioskujący zostanie o tym poinformowany, jeśli nie sprzeciwi się temu administrator.

Średni czas rozpatrzenia wniosku waha się od jednego do czterech miesięcy, w zależności od tego, czy wnioskujący jest przedmiotem wpisu oraz czy nie ma potrzeby przeprowadzania dalszego postępowania, takiego jak współpraca pomiędzy organami ochrony danych osobowych, w celu weryfikacji zasadności wpisu.

6. Przepisy krajowe

Artykuł 41 ustawy nr 78-17 z dnia 6 stycznia 1978 w sprawie technologii informacyjnych, zbiorów danych i swobód obywatelskich.

Artykuł 86 I następne Dekretu nr 2005-1309 z dnia 20 października 2005 wprowadzone do stosowania ww. ustawą nr 78-17.

7. Wymagany język

Zainteresowany może złożyć wniosek w języku francuskim lub angielskim.

XII. NIEMCY

1. Charakter gwarantowanego dostępu

W Niemczech obowiązuje dostęp bezpośredni. Można z niego skorzystać bezpośrednio po zwróceniu sie do organu odpowiadającego za rejestrowanie danych. Z prawa do dostępu zainteresowany może na swoje życzenie skorzystać za pośrednictwem urzędu ochrony danych.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Bundeskriminalamt [*federalny urzad sledczy*]

– SIRENE Büro –

D – 65173 Wiesbaden

Tel.: ++611 551 65 11

Faks: ++611 551 65 31

E-mail: sirenedeutschland@bka.bund.de

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Zainteresowany powinien podać swoje nazwisko (nazwisko panieńskie, jeżeli dotyczy), imię oraz dla ścisłości datę urodzenia. Poza tym nie ma _żadnych szczególnych wymogów formalnych. Sama procedura jest bezpłatna.

Określanie dalszego przebiegu procedury leży w gestii właściwego organu (*Bundeskriminalamt*).

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

W dochodzeniu praw może zainteresowanego wesprzeć krajowy urząd ochrony danych: przekazuje on wniosek o informacje organowi odpowiadającemu za rejestracje danych (np. *Bundeskriminalamt*) lub na żądanie wszczyna inspekcje tego organu pod katem ochrony danych.

Adres urzędu jest następujący:

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [*federalny inspektor ochrony danych i wolnosci informacji*]

Husarenstraße 30

D - 53117 Bonn

Tel.: ++49-228-997799-0

Faks: ++49-228-997799-550
E-mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Jeżeli wniosek dotyczy wpisu dokonanego na podstawie art. 24 rozporządzenia SIS II, informacje z reguły sie ujawnia.
Jeżeli wniosek dotyczy wpisu dokonanego na podstawie art. 26 lub art. 36 decyzji SIS II, udzielenia informacji można odmówić, gdy zachodzi przynajmniej jedna z przesłanek generalnie uzasadniających taka odmowę (określonych w § 19 pkt 4 federalnej ustawy o ochronie danych), tzn.: gdyby ujawnienie informacji mogło narazić na szwank prawidłowe wykonywanie zadań leżących w kompetencjach danego organu rejestrującego, gdyby ujawnienie mogło zagrozić bezpieczeństwu lub porządkowi publicznemu lub gdyby dane lub fakt ich rejestracji należało w myśl prawa lub z uwagi na ich charakter utrzymać w tajemnicy (zwłaszcza z uwagi na wyższej wagi uzasadniony interes strony trzeciej) – a w związku z tym interes wnioskodawcy polegający na uzyskaniu informacji należałoby potraktować jako niższej wagi.
Jeżeli wpisu dokonał zagraniczny organ na podstawie art. 26 decyzji SIS II, należy uwzględnić stanowisko tego organu zgodnie z art. 41 ust. 3 zdanie trzecie rozporządzenia SIS II i art. 58 ust 3 decyzji SIS II. Informacji zwykle udziela *Bundeskriminalamt* – biuro SIRENE. Jeżeli zainteresowany wystąpił do krajowego urzędu ochrony danych, informacji udziela federalny inspektor ochrony danych. W odpowiedzi zwykle podawana jest podstawa prawna wpisu, data jego dokonania, prawdopodobny termin jego
przechowywania oraz nazwa organu, który go dokonał.

5. Najważniejsze przepisy krajowe

Najważniejsze obowiązujące przepisy krajowe to art. 43 ust 1 rozporzadzenia SIS II i art. 58 ust 3 decyzji SIS II w powiązaniu z art. 19 federalnej ustawy o ochronie danych lub z odnośnymi przepisami o prawie do informacji zawartymi w aktach państw związkowych (*Länder*) o ochronie danych.

6. Wymagany język

Zgodnie z przepisami krajowymi (§23 federalnej ustawy o postępowaniu administracyjnym – *Verwaltungsverfahrensgesetz*) językiem urzędowym jest niemiecki, ale jeżeli chodzi o obywateli

Unii Europejskiej, o których mowa w art. 17 i następnych traktatu WE, przyjmowane są także podania i wnioski w innych językach UE

XIII. GRECJA

1. Charakter gwarantowanego dostępu

Zgodnie z art. 12 ustawy 2472/1997 dostęp jest bezpośredni (zainteresowani składają wnioski bezpośrednio do biura SIRENE). Jeżeli wniosek wpłynie do organu ochrony danych osobowych, zainteresowanego poucza sie, by zwrócił sie bezpośrednio do biura SIRENE.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Według przepisów wnioski należy kierować do biura SIRENE, którego pełny adres jest następujący:

Ministry of Citizen Protection [*ministerstwo ochrony obywateli*]

Greek Police [*policja grecka*]

International Police Cooperation Division [*wydział międzynarodowej współpracy policyjnej*]

3d Division SIRENE

Kanellopoulou 4

GR-101 77 Athens

Tel.: ++301 69 81 957

Faks: ++301 69 98 264/5

E-mail: info@sirene-gr.com

Internet: ---

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

We wniosku zainteresowany musi podać nazwisko i imię, imię ojca, pełna datę urodzenia i obywatelstwo. Podawanie innych danych, np. numeru indentyfikacyjnego, numeru paszportu, adresu, numeru telefonu i imienia matki, nie jest obowiązkowe. Należy dołączyć kopię paszportu. Aby skorzystać z prawa do dostępu na mocy art. 12 ustawy 2472/1997, zainteresowany musi wpłacić 5 EUR na rzecz administratora danych (biura SIRENE), natomiast korzystanie z prawa do odwołania na mocy art. 13 wspomnianej ustawy oraz decyzji 122 przyjętej przez urząd ochrony danych osobowych w dniu 9 października 2001 r. – kosztuje 60 EUR. Należy dodać, że w rzeczywistości symboliczna kwota 5 EUR za dostęp do danych przechowywanych w SIS nigdy nie jest pobierana.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Dane teleadresowe greckiego organu ochrony danych osobowych są następujące:

Hellenic Data Protection Authority [*grecki urząd ochrony danych*]

Kifisias 1–3, 1st floor

GR – 115 23 Athens

Tel.: ++30 210 6475600

Faks: ++ 301 210 6475628

E-mail: contact@dpa.gr

Krajowy urząd ochrony danych osobowych sprawdza, czy wpis zawarty w SIS na temat zainteresowanego jest legalny i uzasadniony.

5. Oczekiwany skutek. Treść podawanych informacji

Jeżeli wpis ma za podstawę art. 24 rozporządzenia SIS II, zainteresowany otrzyma informacje o dotyczących go danych.

Jeżeli wpis ma za podstawę art. 26 i art. 36 decyzji SIS II, zainteresowany najprawdopodobniej otrzyma odmowę ujawnienia dotyczących go danych. Ponadto, zgodnie z art. 12 ust. 5 ustawy 2472/1997, dane nie zostaną ujawnione, jeżeli były przetwarzane ze względów bezpieczeństwa narodowego lub podczas dochodzenia dotyczącego szczególnie poważnych czynów zabronionych.

Jeżeli wpisu mającego za podstawę art. 26 decyzji SIS II dokonał zagraniczny organ, jego stanowisko będzie uwzględnione podczas podejmowania decyzji o ewentualnym ujawnieniu danych zainteresowanemu.

W odpowiedzi podaje sie zainteresowanemu prawna podstawę wpisu, datę jego wprowadzenia do SIS, nazwę departamentu go wprowadzającego oraz termin jego przechowywania.

6. Najważniejsze przepisy krajowe

Zastosowanie mają: art. 41 rozporządzenia SIS II oraz art. 12 (korzystanie z prawa do dostępu) i 13 (korzystanie z prawa do odwołania) ustawy 2472/1997.

Uwaga

Jeżeli dane zainteresowanego zostały wprowadzone do SIS przez grecką policję, wnioski dotyczące prawa do dostępu i wnioski odwoławcze mające za podstawę at. 12 i 13 ustawy 2472/1997 należy kierować bezpośrednio do administratora danych.

Jeżeli chodzi o system językowy, oficjalnym językiem jest grecki, jednak rozpatrywane są też wnioski po angielsku.

XIV. WĘGRY

1. Charakter gwarantowanego dostępu

Dostęp może być pośredni lub bezpośredni.

2. Dane teleadresowe organu, do którego należy kierować wniosek

The SIRENE Office of the National Police Headquarters [*biuro SIRENE przy Komendzie Głównej Policji*]

H-1139 Budapest, Teve utca 4–6.

Tel.: +36 1 443 5861

E-mail: sirene@nebek.police.hu

Nemzeti Adatvédelmi és Információszabadság Hatóság

Postal address: 1530 Budapest, Pf.: 5.

Office address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Tel: +36 1 391-1400

Fax: +36 1 391-1410

Email: ugyfelszolgalat@naih.hu

Web: http://naih.hu

Wnioski o dostęp można składać osobiście w:

- każdym urzędzie publicznym, (http://www.kormanyhivatal.hu/hu),
- każdej placówce policji http://www.police.hu/magyarendorseg/szervezetif) na terytorium Węgier,
- w każdej placówce dyplomatycznej Republiki Węgierskiej (http://www.kormany.hu/hu/kovetsegek-konzulatusok).

Zostaną one przekazane biuru SIRENE.

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Zainteresowany musi przedstawić wiarygodny dowód swojej tożsamości. Wnioski należy sporządzać po węgiersku, angielsku, niemiecku lub francusku. Odpowiedzi udziela sie na piśmie w możliwie krótkim terminie, najpóźniej w ciągu 30 dni od daty złożenia wniosku. Złożenie wniosku jest bezpłatne. Jeżeli jednak w danym roku kalendarzowym zainteresowany składa kolejny wniosek, ponosi on koszty udzielenia informacji.

4. **Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji**

   Węgierski organ ochrony danych osobowych upoważniony jest do prowadzenia dochodzeń i postępowań administracyjnych w sprawie ochrony danych osobowych na wnioski składane na podstawie odpowiednich przepisów (§52-61) ustawy CXII z 2011 r. o prywatności.

   Ponadto zainteresowany może się zwrócić do organu ochrony danych osobowych, jeżeli ma wątpliwości co do odpowiedzi otrzymanej z biura SIRENE, lub jeżeli nie otrzymał on stamtąd żadnej odpowiedzi.

5. **Najważniejsze przepisy krajowe**

   Ustawa CXII z roku 2001 o prywatności

   Ustawa CLXXXI z roku 2012 o wymianie informacji w Systemie Informacyjnym Schengen drugiej generacji

   Dekret rządowy nr. 15/2013. (28/I) o szczegółowej procedurze wymiany informacji w ramach Systemu Informacyjnym Schengen drugiej generacji

XV. ISLANDIA

1. Charakter gwarantowanego dostępu

Obowiązuje bezpośredni dostęp do informacji, co oznacza, że osoby, których dane dotyczą, powinny kierować wniosek o informację, poprawienie lub usunięcie danych do Biura SIRENE, które zdecyduje, czy zapewnić dostęp do danych.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski należy kierować do islandzkiego biura SIRENE, prowadzonego przez Komendanta Islandzkiej Policji Państwowej:

Ríkislögreglustjórinn
SIRENE-skrifstofa
Skúlagata 21
101 Reykjavík
ICELAND
Tel.: ++354 444 2500
Fax: ++354 444 2501
E-mail: rls@rls.is
Internet: www.rls.is

Odpowiedni formularz wniosku można wypełnić w lokalnym posterunku policji lub w urzędzie komisarza. Decyzje o ewentualnym udzieleniu informacji podejmuje biuro SIRENE.

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Zainteresowany musi okazać dowód tożsamości i wypełnić formularz w obecności funkcjonariusza policji. Może wystąpić o dostęp do informacji dotyczących tylko niego samego. Jednakże opiekun prawny może wystąpić o dostęp do informacji o osobie, nad która sprawuje opiekę. Korzystanie z prawa do wglądu jest bezpłatne, ale możliwe tylko raz w ciągu roku, chyba że częstszy dostęp podyktowany jest szczególnymi okolicznościami. W takich sytuacjach biuro SIRENE zasięga opinii organu ochrony danych.

Wniosek musi być złożony osobiście. Wymagany jest dowód potwierdzający tożsamość. Informacje są udzielane bezpłatnie.

4. **Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji**

Jeżeli zainteresowanemu wysyła się standardową odpowiedź: „Brak informacji w systemie/Zakaz ujawniania przechowywanych informacji" (zob. pkt 5), biuro SIRENE musi go poinstruować o możliwości odwołania sie od tej decyzji do Ministerstwa Sprawiedliwości i Praw Człowieka. W sprawie decyzji biura SIRENE ministerstwo może zasięgnąć opinii organu ochrony danych.

[*ministerstwo sprawiedliwości i praw człowieka*:]
The Ministry of Justice and Human Rights:
Dómsmála- og mannréttindaráduneytid
Skuggasund
IS - 150 Reykjavík
Tel.: ++354 545 9000.
Fax: ++354.552.7340
E-mail: postur@dmr.stjr.is
Internet: www.domsmalaraduneyti.is

Adres organu ochrony danych jest następujący:

Persónuvernd
Rauðarárstígur 10
IS - 105 Reykjavík
Tel.: ++354 510 9600.
Fax: ++354 510.9606
E-mail: postur@personuvernd.is
Internet: www.personuvernd.is

Jeśli odmówiono dostępu, organ ochrony danych może wydać opinię w sprawie praw osób, których dane dotyczą. Tym niemniej, aktualnie organ ochrony danych nie ma uprawnień władczych względem SIS II.

5. **Oczekiwany skutek. Treść podawanych informacji**

Biuro SIRENE musi udzielić odpowiedzi bez zbędnej zwłoki, najpóźniej w ciągu miesiąca od otrzymania wniosku. Jeżeli zainteresowany figuruje w systemie, otrzyma on informacje o celu i powodach wpisu. Zainteresowany nie ma prawa zapoznać sie z przechowywanymi danymi, jeżeli

należy je zachować w tajemnicy, po to by mógł sie zrealizować zamysł organu dokonującego wpisu do systemu informacyjnego lub by chronić interes osób trzecich, lub by nie udaremniać trwającej obserwacji niejawnej. Zainteresowany otrzymuje wtedy taka sama standardowa odpowiedz, jak osoba niefigurująca w systemie: „Brak informacji w systemie/Zakaz ujawniania przechowywanych informacji".

Artykuły 13 i 15 ustawy o Systemie Informacyjnym Schengen w Islandii (http://www.personuvernd.is/information-in-english/greinar/nr/440):

Art. 13
Każda osoba, której dane zostały wprowadzone do system powinna mieć prawo do informacji o danych jej dotyczących przetwarzanych w systemie.
Prawo osoby, której dane dotyczą, do informacji na podstawie § 1 nie ma zastosowania, jeśli jest to niezbędne do zachowania tajemnicy w celu realizacji celu związanego z wjazdem lub ze względu na interes innych osób. Jeśli niejawna obserwacja jest prowadzona na podstawie art. 7, osoba, której dane dotyczą, nie powinna być informowana o swoich danych. Jeśli wnioskujący zwraca się o informacje o danych, które zostały wprowadzone do system przez inny organ, państwo to powinno mieć możliwość wyrażenia swojego stanowisko przed ujawnieniem informacji.

Art. 15
Jeśli Komendant Główny Policji Islandii otrzymuje wniosek złożony na podstawie art. 13 lub 14, powinien udzielić odpowiedzi bez zbędnej zwłoki. Uzasadnienie decyzji powinno w możliwie najszerszym zakresie, oprócz informacji, które nie powinny zostać ujawnione.

6. Najważniejsze przepisy krajowe

Najważniejsze przepisy krajowe to: ustawa nr 16/2000 o systemie informacyjnym Schengen w Islandii oraz rozporządzenie nr 112/2001 o systemie informacyjnym Schengen w Islandii

7. Wymagany język

Choć nie ma odnośnych przepisów prawnych, językiem administracji w Islandii jest islandzki. Jeżeli jednak organ islandzki otrzyma zapytanie w innym języku, udzieli na nie odpowiedzi. Jeżeli

wniosek składa osoba, która nie będzie w stanie zrozumieć odpowiedzi po islandzku (np. cudzoziemiec, którego interesu nie reprezentuje żaden islandzki podmiot, np. adwokat), otrzyma odpowiedz w języku dla niej zrozumiałym.

Broszury informacyjne po angielsku i islandzku zostały wydrukowane i udostępnione na międzynarodowym lotnisku w Keflaviku. Osoba, której dane dotyczą, jest uprawniona do otrzymania informacji w zrozumiałym dla niej języku.

XVI. WŁOCHY

1. Charakter gwarantowanego dostępu

Można korzystać tylko z dostępu bezpośredniego, zwracając sie do administratora – Departament Bezpieczeństwa Publicznego w Ministerstwie Spraw Wewnętrznych.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Zgodnie ze wskazówkami wspomnianego Departamentu Bezpieczeństwa Publicznego wszystkie wnioski o dostęp i weryfikacje należy kierować na następujący adres:

Ministero dell'interno [*ministerstwo spraw wewnętrznych*]
Dipartimento della pubblica sicurezza [*departament bezpieczeństwa publicznego*]
Ufficio coordinamento e pianificazione delle forze di polizia [*biuro koordynacji i planowania sił policji*]
Divisione N.SIS
Via di Torre di Mezza Via 9/121 - 00173 Roma

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Składanie wniosku (poczta lub faksem) nie wiąże sie z żadnymi specjalnymi wymogami, nie ma też za to żadnych opłat. Obowiązujące przepisy nie określają jednoznacznie, jak należy ustalać tożsamość zainteresowanego dostępem do N-SIS. Niemniej aby przyśpieszyć rozpatrywanie skargi, zainteresowany powinien ją sporządzić po włosku, angielsku, francusku lub niemiecku, **podpisać**, wskazać w skrócie powody jej złożenia oraz dołączyć do niej **kserokopie swojego dowodu osobistego**.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Jeżeli uzyskana odpowiedz jest niezadowalająca, zainteresowany może skierować skargę do *Garante per la protezione dei dati personali* (inspektora ochrony danych osobowych) na następujący adres:

Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121
00186 Roma

Aby dokumenty były dobrze czytelne, skargi lepiej wysyłać poczta niż faksem. Należy w nich podać odpowiednie dane teleadresowe zainteresowanego – w miarę możliwości jego adres – by ułatwić korespondencje.

5. Oczekiwany skutek. Treść podawanych informacji

Odpowiedź powinna zostać udzielona w ciągu 30 dni.

6. Najważniejsze przepisy krajowe

Najważniejsze przepisy krajowe to:

a) ustawa nr 388 z dnia 30 września 1993 r. dotyczącą ratyfikacji i wdrożenia układu z Schengen i j konwencji wykonawczej (zob. zwłaszcza art. 9, 10, 11 i 12)

b) dekret legislacyjny nr 196 z roku 2003.

7. Wymagany język

Wniosek powinien być sporządzony, w miarę możliwości, po włosku, angielsku, francusku lub niemiecku.

XVII. ŁOTWA

1. Charakter gwarantowanego dostępu

Każdy (zarówno obywatel, jak i osoba nie będąca obywatelem państwa strefy Schengen) ma prawo bezpośredniego dostępu do swoich danych osobowych przechowywanych w SIS. (Określa to rozporządzenie Rady Ministrów nr 622 „*Instrukcja, jak osoba, której dotyczą dane, powinna występować o informacje na temat danych przechowywanych w systemie informacyjnym Schengen i systemie informacyjnymi SIRENE oraz jak należy jej udzielać takich informacji*".) Odpowiedź zainteresowany otrzymuje w ciągu jednego miesiąca.

Zainteresowany, którego wniosek o sprawdzenie jego danych osobowych spotkał sie z odmowa lub pozostał bez odpowiedzi, może odwołać sie do Państwowego Inspektoratu Danych, który jest też właściwym organem nadzorującym realizacje prawa do żądania sprostowania nieścisłych danych lub prawa do żądania usunięcia danych nielegalnych.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wniosek (pisemny) o bezpośredni dostęp należy kierować do policji państwowej lub placówki dyplomatycznej bądź konsularnej Republiki Łotewskiej.

State Police [*policja państwowa*]
Ciekurkalna 1.linija 1, k-4
Riga, LV-1026
Tel.: +371 67075212; faks: +371 67371227
E-mail: kanc@vp.gov.lv

Dane teleadresowe placówek dyplomatycznych i konsularnych Republiki Łotewskiej można znaleźć na stronie Ministerstwa Spraw Zagranicznych (pod linkiem: http://www.mfa.gov.lv/lv/Ministrija/mission).

3. Kwestie formalne: potrzebne informacje i dokumenty

Wnioski opatrzone data i podpisem należy składać osobiście lub elektronicznie w biurze Policji Państwowej lub w łotewskiej placówce dyplomatycznej bądź konsularnej. Składając wniosek osobiście, zainteresowany musi potwierdzić swoja tożsamość dowodem tożsamości. Wnioski składane elektronicznie powinny być opatrzone bezpiecznym podpisem elektronicznym.

We wniosku zainteresowany podaje swoje nazwisko i imię, datę urodzenia, numer identyfikacyjny

(jeżeli zainteresowany go posiada), miejsce urodzenia, państwo pochodzenia, rodzaj (jeżeli dotyczy) i numer dokumentu tożsamości, nazwę organu wydającego, datę wydania i termin ważności, zakres żądanych informacji (informacje o zainteresowanym, o odbiorcach jego danych), oczekiwany sposób otrzymania odpowiedzi (osobiście w biurze Policji Państwowej lub w łotewskiej placówce dyplomatycznej bądź konsularnej albo poczta – należy wtedy wskazać odpowiedni adres).

Procedura jest bezpłatna.

4. Oczekiwany skutek. Treść podawanych informacji

Otrzymawszy od zainteresowanego wniosek o informacje, przedstawiciele Policji Państwowej lub łotewskiej placówki dyplomatycznej bądź konsularnej weryfikują tożsamość zainteresowanego i kierują wniosek do jednostki Policji Państwowej – łotewskiego biura SIRENE.

Dokonuje ono niezbędnych kontroli w związku z otrzymanym wnioskiem i w ciągu miesiąca udziela zainteresowanemu odpowiedzi lub odmawia ujawnienia informacji. W tym celu wysyła pismo pod wskazany przez zainteresowanego adres lub do wskazanej instytucji (adres własny, Policji Państwowej albo łotewskiej placówki dyplomatycznej bądź konsularnej).

5. Najważniejsze przepisy krajowe

– ustawa o ochronie danych osobowych

– ustawa o użytkowaniu systemu informacyjnego Schengen

– rozporządzenie Rady Ministrów nr 622 (z 11.9.2007) „Instrukcja, jak osoba, której dotyczą dane, powinna występować o informacje na temat danych przechowywanych w systemie informacyjnym Schengen i systemie informacyjnym SIRENE oraz jak należy jej udzielać takich informacji".

6. Wymagany język

Jeżeli chodzi o wymogi językowe, wszelkie czynności względem organów łotewskich należy prowadzić po łotewsku (zgodnie z ustawa o urzędowym języku Republiki Łotewskiej), co dotyczy również prawa dostępu do SIS. Natomiast ustawa o petycjach (art. 7 sekcja 1 ust. 4) przewiduje, że petycja lub skarga mogą pozostać bez odpowiedzi, jeżeli obiektywnie rzecz biorąc, nie można ich odczytać lub zrozumieć. Łotewskie biuro SIRENE poinformowało, że rozpatruje też wnioski po angielsku i rosyjsku.

XVIII. LUKSEMBURG

1. **Charakter gwarantowanego dostępu**

   Dostęp jest pośredni w tym sensie, że z prawa do niego można korzystać tylko za pośrednictwem organu nadzorczego.

2. **Dane teleadresowe organu, do którego należy kierować wniosek**

   Organ nadzorczy ustanowiony na mocy art. 17 ustawy z dnia 2 sierpnia 2002 r. o ochronie osób w związku z przetwarzaniem danych osobowych, zmienionej ustawa z dnia 31 lipca 2006 r., ustawa z dnia 22 grudnia 2006 r. i ustawa z dnia 27 lipca 2007 r.

   Parquet Général du Grand-Duché de Luxembourg
   [*prokuratura generalna Wielkiego Księstwa Luksemburga*]
   BP 15
   L-2010 Luxembourg
   Tel.: ++352 47 59 81–331
   Faks: ++352 47 05 50
   E-mail: parquet.general@mj.etat.lu

3. **Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty**

   Ustawa z roku 2002 nie przewiduje żadnych specjalnych wymogów w odniesieniu do wniosku. Procedura jest bezpłatna.

   Na mocy art. 17 ustawy z roku 2002 organ nadzorczy przeprowadzi odpowiednie sprawdzenia i dochodzenie oraz spowoduje konieczne zmiany.

4. **Oczekiwany skutek. Treść podawanych informacji**

   Organ nadzorczy poinformuje zainteresowanego, że przetwarzane dane nie zawierają żadnych danych, które oznaczałyby naruszenie traktatów, przepisów ustawowych i wykonawczych.

   Nie ujawnia sie żadnych informacji o treści danych zainteresowanego.

5. **Najważniejsze przepisy krajowe**

   Ustawa z dnia 2 sierpnia 2002 r., ze zmianami, o ochronie osób w związku z przetwarzaniem danych osobowych.

Rozporządzenie Wielkiego Księstwa Luksemburga z dnia 9 sierpnia 1993 r. o zgodzie na ustanowienie i wykorzystywanie bazy danych będącej krajowym modułem systemu informacyjnego Schengen (N.SIS) (rozporządzenie nie obejmuje prawa do dostępu).

6. Wymagany język

Do wszczęcia postępowania o dostęp zainteresowany może użyć języka:

- luksemburskiego
- francuskiego
- niemieckiego
- angielskiego.

XIX. LIECHTENSTEIN

1. Charakter prawa dostępu

Osoba, której dane dotyczą, może korzystać z bezpośredniego prawa dostępu.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Landespolizei des Fürstentums Liechtenstein (Krajowa policja)
Kommando
Gewerbeweg 4
Postfach 684
9490 Vaduz
FÜRSTENTUM LIECHTENSTEIN

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Wniosek o dostęp powinien być skierowany pisemnie do Policji Krajowej. Wnioskodawca musi przedstawić dowód tożsamości. Jeśli wniosek nie jest składany osobiście, wnioskodawca musi przedstawić uwierzytelnioną kopię swojego paszportu.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Data Protection Office **(***Biuro Ochrony Danych Osobowych***)**
Kirchstrasse 8
Postfach 684
9490 Vaduz
Liechtenstein
Tel. +423 / 236 60 90
info.dss@llv.li

5. Oczekiwany skutek. Treść podawanych informacji

Co do zasady odpowiedź jest udzielana w ciągu 30 dni. Jeśli nie może zostać udzielona w tym terminie wnioskodawca zostanie o tym poinformowany. Jednakże, odpowiedź musi zostać udzielona nie później niż w ciągu 60 dni w ciągu złożenia wniosku.

6. Najważniejsze przepisy krajowe

Art. 11 i 12 ustawy o ochronie danych osobowych;

Art. 34g ustawy o Policji krajowej (LGBl. 1989 Nr. 48);

Art. 47-49 zarządzenie w sprawie Systemu Informacyjnego Schengen (SIS) i Biura SIRENE (LGBl. 2011 Nr. 140).

7. Wymagany język

Wniosek powinien zostać sporządzony po niemiecku.

XX. LITWA

1. Charakter gwarantowanego dostępu

Osoba, której dotyczą dane, ma prawo do bezpośredniego dostępu.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski o dostęp, sprostowanie lub usuniecie należy kierować do Ministerstwa Spraw Wewnętrznych Republiki Litewskiej, które jest administratorem danych:

Ministry of the Interior of the Republic of Lithuania [*ministerstwo spraw wewnętrznych Republiki Litewskiej*]
Šventaragio str. 2, LT-01510 Vilnius
Lithuania
Phone +370 5 271 7130, fax +370 5 271 8551
Email bendrasisd@vrm.lt

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Wniosek musi mieć formę pisemną i zawierać podpis zainteresowanego. Zainteresowany dostępem do swoich danych lub żądający ich sprostowania czy usunięcia musi we wniosku określić swoją tożsamość: podać nazwisko(-a) i imię (imiona), osobisty numer identyfikacyjny (jeżeli go nie ma – datę urodzenia), miejsce zamieszkania, dane kontaktowe (telefon lub e-mail). Musi też dostarczyć administratorowi danych dokument potwierdzający tożsamość. Korzystanie z tych praw jest bezpłatne.

4. Oczekiwany skutek. Treść podawanych informacji

Zainteresowany ma prawo otrzymać informacje o źródłach i rodzaju zgromadzonych o nim danych, celu ich przetwarzania oraz odbiorcach, którym te dane sie ujawnia lub ujawniono, przynajmniej w ostatnim roku.

Na zapytanie zainteresowanego dotyczące przetwarzania jego danych osobowych administrator danych musi odpowiedzieć, precyzując, czy dane osobowe zainteresowanego są przetwarzane, oraz ujawnić mu żądane dane najpóźniej w terminie 30 dni kalendarzowych od otrzymania zapytania (Art. 25 ustawy o ochronie prawnej danych osobowych).

Jeżeli zapoznawszy sie ze swoimi danymi osobowymi, zainteresowany stwierdzi, że są one nieprawdziwe, niekompletne lub nieścisłe lub że są przetwarzane nielegalnie lub niesprawiedliwie, i zwróci sie na piśmie do administratora danych – wtedy administrator danych musi bezzwłocznie zweryfikować wskazane dane oraz sprostować nieprawdziwe, niekompletne lub nieścisłe dane osobowe i (lub) wstrzymać ich przetwarzanie (nie dotyczy przechowywania). Jeżeli stwierdzi, że dane osobowe przetwarza się nielegalnie lub niesprawiedliwie, musi bezzwłocznie zniszczyć dane zgromadzone nielegalnie lub niesprawiedliwie albo wstrzymać ich przetwarzanie (nie dotyczy przechowywania).

Administrator danych musi na żądanie zainteresowanego bezzwłocznie poinformować jego oraz odbiorców danych osobowych o sprostowaniu, zniszczeniu lub zawieszeniu przetwarzania tych danych (art. 26 ustawy o prawnej ochronie danych osobowych).

W myśl art. 23 ustawy o ochronie prawnej danych osobowych administrator danych musi umożliwić zainteresowanemu korzystanie z przysługujących mu praw, z wyjątkiem sytuacji określonych prawem, w których przeważa wzgląd na:

1) bezpieczeństwo lub obronę państwa

2) porządek publiczny, zapobieganie przestępstwom, prowadzenie odnośnych dochodzeń, wykrywanie i karanie przestępstw

3) ważny państwowy interes gospodarczy lub finansowy

4) zapobieganie naruszeniom etyki urzędowej lub zawodowej, prowadzenie odnośnych dochodzeń oraz wykrywanie takich naruszeń

5) ochronę praw i swobód osób, których dotyczą dane, i innych osób.

Zainteresowanemu odmawia sie udzielenia informacji o jego danych osobowych, jeżeli jest to konieczne do wykonania czynności żądanych we wpisie lub do ochrony praw i swobód stron trzecich. Informacji o jego danych osobowych nie ujawnia sie mu również w okresie ważności wpisu dotyczącego obserwacji niejawnej.

Odmowę przychylenia sie do wniosku zainteresowanego administrator danych musi oprzeć na odpowiednich przesłankach. O swojej odmowie administrator danych powiadamia zainteresowanego najpóźniej w terminie 30 dni kalendarzowych od dnia otrzymania wniosku.

Regulacje o litewskim krajowym systemie informacyjnym Schengen, zatwierdzone rozporządzeniem Ministra Spraw Wewnętrznych Republiki Litewskiej nr 1V-324 z dnia 17 września 2007 r., przewidują, że jeżeli wpisu o zainteresowanym dokonała inna umawiająca się strona, to informacje o jego danych osobowych przetwarzanych w krajowym SIS administrator danych N.SIS może ujawnić zainteresowanemu tylko za zgoda umawiającej się strony, która tego

wpisu dokonała.

Otrzymawszy od zainteresowanego pisemny wniosek o sprostowanie nieprawdziwych, niekompletnych lub nieścisłych danych osobowych, o zniszczenie danych przetwarzanych nielegalnie czy o wstrzymanie przetwarzania danych osobowych, administrator danych N.SIS musi bezzwłocznie wniosek ten przekazać właściwej instytucji umawiającej sie strony i poinformować o tym zainteresowanego. Gdy właściwa instytucja umawiającej sie strony sprostuje nieprawdziwe i nieścisłe dane, uzupełni dane niekompletne, zniszczy dane przechowywane nielegalnie lub zawiesi ich przetwarzanie, administrator danych N.SIS musi bezzwłocznie poinformować o tym zainteresowanego oraz odbiorców danych N.SIS, którym przekazano dane nieprawdziwe, nieścisłe lub niekompletne.

5. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

State Data Protection Inspectorate [*panstwowy inspektorat ochrony danych*]
A.Juozapavičiaus str. 6 , LT-09310 Vilnius
Lithuania
Phone +370 5 279 1445, fax +370 5 261 9494
E-mail: ada@ada.lt
Internet: www.ada.lt

Jeżeli odpowiedź administratora danych nie satysfakcjonuje zainteresowanego (gdy administrator nie przychylił sie do jego wniosku o dostęp do danych, o sprostowanie lub zniszczenie danych czy zawieszenie dalszego ich przetwarzania albo nie udzielił odpowiedzi w terminie 30 dni kalendarzowych od dnia otrzymania wniosku), zainteresowany może zaskarżyć czynności (niedopatrzenia) administratora do Państwowego Inspektoratu Ochrony Danych w terminie 3 miesięcy od daty otrzymania odpowiedzi lub w terminie 3 miesięcy od daty, z która wygasł termin na odpowiedź. Na poparcie faktów przytoczonych w skardze zainteresowany może załączyć ewentualne dokumenty (odpowiedz administratora danych na wniosek zainteresowanego itp.), tak by zapewnić optymalne rozpatrzenie skargi.

Po otrzymaniu skargi zainteresowanego Państwowy Inspektorat Ochrony Danych kontroluje legalność przetwarzania odnośnych danych osobowych i podejmuje decyzje w sprawie faktów opisanych w skardze.

6. Najważniejsze przepisy krajowe

Ustawa o prawnej ochronie danych osobowych

Regulacje o litewskim krajowym systemie informacyjnym Schengen, zatwierdzone rozporządzeniem Ministra Spraw Wewnętrznych Republiki Litewskiej nr 1V-324 z dnia 17 września 2007 r.

7. Wymagany język

Wnioski o dostęp, sprostowanie lub usunięcie należy składać w języku państwowym (litewskim).

Wnioski otrzymane w jakimkolwiek innym języku zostaną rozpatrzone zgodnie z procedura ogólna.

Wnioski w języku innym niż język państwowy muszą zostać przetłumaczone na litewski.

Odpowiedz zostanie zainteresowanemu udzielona w języku państwowym (litewskim).

Ochrony Danych w języku innym niż język państwowy musi zostać przetłumaczona na litewski.

Decyzja w sprawie skargi zostanie przyjęta, a odpowiedz na skargę udzielona w języku państwowym (litewskim).

XXI. MALTA

1. Charakter gwarantowanego dostępu

Osoba, której dotyczą dane, ma prawo do bezpośredniego dostępu.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski o dostęp, sprostowanie lub usuniecie należy kierować do właściwego organu krajowego pod następujący adres:

Data Protection Officer Insp. [*inspektor ochrony danych*]

Legal Unit

Police Headquarters

Floriana

Tel.: 21224001

E-mail: sandro.camilleri@gov.mt

3. Kwestie formalne

W myśl prawa maltańskiego zainteresowany powinien złożyć wniosek na piśmie i opatrzyć go swoim podpisem. Wniosek powinien sformułować po maltańsku lub angielsku, które to języki są językami urzędowymi uznanymi w konstytucji maltańskiej. Odpowiedz powinna nastąpić w tym samym języku, którym posłużył sie zainteresowany we wniosku. Informacji należy udzielić bezpłatnie i bez zbytniej zwłoki.

4. Procedura

Rozporządzenie SIS II i decyzja SIS II przewidują, że osoby występujące o dostęp do swoich danych osobowych wprowadzonych do systemu informacyjnego Schengen korzystają z tego prawa zgodnie z przepisami państwa, w którym złożono wniosek do właściwego krajowego organu.

Po złożeniu wniosku zainteresowany ma prawo do otrzymania pisemnej odpowiedzi zgodnej z ogólnymi przepisami o ochronie danych zawartymi w maltańskiej ustawie o ochronie danych (rozdział 440). Odpowiedz powinna być zrozumiała i informować o faktycznie przetwarzanych danych osobowych, źródle ich pochodzenia, celu przetwarzania oraz ewentualnych ich odbiorcach.

Odmowa lub ograniczenie prawa dostępu mogą nastąpić tylko wtedy, gdy są one uzasadnione walką z przestępczością lub gdy są konieczne do ochrony osób, których dotyczą dane, lub swobód osób trzecich.

W razie odmowy lub ograniczenia dostępu zainteresowany jest informowany na piśmie o zapadłej

decyzji, w tym o jej przesłankach, o ile podanie takich informacji nie zakłóca pracy policji ani nie godzi w prawa ani wolności osób trzecich.

5. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Office of the Data Protection Commissioner [*urząd inspektora ochrony danych*]

2, Airways House,

High Street

Sliema.

Malta

Tel: +35623287100, fax: +35623287198

Email: idpc.info@gov.mt

Internet: www. idpc.gov.mt

W razie ograniczenia lub odmowy dostępu zainteresowany ma prawo odwołać sie do Inspektora Ochrony Danych w terminie 30 dni od dnia otrzymania decyzji lub od dnia, w którym jak można racjonalnie przypuszczać, dowiedział sie on o decyzji.

Rozpatrując odwołanie, Inspektor Ochrony Danych weryfikuje decyzje i upewnia sie, czy odmowa lub ograniczenie mają rozsądne i solidne podstawy.

6. Najważniejsze przepisy krajowe

Akty prawne, które maja zastosowanie, to ustawa o ochronie danych (rozdział 440) i obwieszczenie prawne 142 z roku 2004 regulujące przetwarzanie danych osobowych w sektorze policji.

XXII. HOLANDIA

1. Charakter gwarantowanego dostępu

W Holandii obowiązuje prawo do dostępu bezpośredniego. Do krajowego modułu systemu informacyjnego Schengen (N.SIS) ma zastosowanie ustawa o danych policyjnych (*Wet politiegegevens*). Prawo do dostępu jest sformułowane w art. 25 tej ustawy. Każdy może wystąpić o dostęp do swoich danych osobowych przechowywanych w SIS, kierując pisemny wniosek do inspektora ochrony danych w Policji Państwowej (*Korps Landelijke Politiediensten*). Odpowiedzi na wniosek o dostęp należy zainteresowanemu udzielić w ciągu 6 tygodni. W odpowiedzi należy poinformować o treści danych, o ile nie zachodzą przesłanki uzasadniające zastosowanie art. 27 ustawy o danych policyjnych. Innymi słowy, można odmówić udzielenia informacji przez wzgląd na:

a. właściwe wykonywanie zadań przez policje

b. istotny interes stron trzecich

c. bezpieczeństwo państwowe.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski o informacje należy kierować na adres:

Korps Landelijke Politiediensten [*korpus państwowych służb policji*]

Attention of the data protection officer

Postbus 3016

NL – 2700 KX Zoetermeer

Tel.: ++31-79-345 90 62

Faks: ++31-79-345 90 10

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Po otrzymaniu wniosku o informacje inspektor ochrony danych kontaktuje sie z zainteresowanym, żeby ustalić kwestie związane z rozpatrywaniem wniosku. Zainteresowany musi dostarczyć kopie dowodu osobistego. Za rozpatrzenie wniosku może zostać pobrana opłata w wysokości 4,50 EUR. Rozpatrując wniosek, ustala sie, czy można sie do niego przychylić, czy też zachodzą przesłanki uzasadniające odmowę.

Wnioski dotyczący wpisów dokonanego na podstawie rozporządzenia SIS II są przekazywane organowi odpowiadającemu za takie wpisy – Wydziałowi Imigracji i Naturalizacji przy Ministerstwie Sprawiedliwości.

Wnioski dotyczące wszelkich innych wpisów są rozpatrywane przez właściwe organy (policji).

Po otrzymaniu odpowiedzi zainteresowany może wystąpić o uzupełnienie, sprostowanie lub usuniecie danych.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

W razie sporu dotyczącego rozpatrzenia wniosku można wystąpić o mediacje do:

College Bescherming Persoonsgegevens [*komisja ochrony danych osobowych*]
Postbus 93374
NL – 2509 AJ Den Haag
Tel.: ++31(0)708888500
Faks: ++31(0)708888501
E-mail: info@cbpweb.nl
Internet: www.cbpweb.nl

Skargę należy złożyć w terminie 6 tygodni od otrzymania odpowiedzi.

Jeżeli wniosek zainteresowanego o dostęp został odrzucony, *College Bescherming Persoonsgegevens* rozpatrzy skargę bezpłatnie.

Zamiast tego – lub jeżeli mediacja nie przyniosła skutku – można odwołać sie do sadu okręgowego (wydział administracyjny), by rozpatrzył sprawę i dokonał stosownego rozstrzygnięcia.

5. Wymagany język

Wnioski powinny być składane pisemnie, najlepiej po holendersku lub angielsku, ale przyjmowane są także wnioski po francusku, niemiecku i hiszpańsku. Wnioskodawcy posługujący się innym językiem, powinny wziąć pod uwagę wydłużony czas postępowania z uwagi na konieczność wykonania tłumaczeń.

XXIII. NORWEGIA

1. Charakter gwarantowanego dostępu

Obowiązuje prawo do dostępu bezpośredniego.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Kriminalpolitisentralen

[*krajowa kryminalna służba śledcza*]

PO Box 8163 Dep.

NO-0034 OSLO

Tel.: ++47 23 20 80 00

E-mail:

Fax: + +47 23 20 88 80

Internet: www.kripos.no

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Wniosek musi mieć formę pisemną i nosić podpis zainteresowanego. Odpowiedzi na piśmie należy udzielić bez zbędnej zwłoki, najpóźniej w terminie 30 dni od otrzymania wniosku.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Datatilsynet [*ochrona danych*]

PO Box 8177 Dep.

NO-0034 OSLO

Tel.: +47 22 39 69 00

Faks: + 47 22 42 23 50

E-mail: postkasse@datatilsynet.no

Internet: www.datatilsynet.no

5. Oczekiwany skutek. Treść podawanych informacji

Wnioski o dostęp rozpatruje w pierwszej instancji administrator danych (*Kriminalpolitisentralen*). Otrzymane wnioski administrator przekazuje do zaopiniowania organom, które zleciły rejestracje

danych. Jeżeli wniosek został od razu skierowany do organu, który zlecił rejestracje danych, organ ten przekazuje go administratorowi danych wraz ze swoja opinia.

Jeżeli następuje odmowa dostępu, ponieważ zainteresowany nie figuruje w systemie lub ma zastosowanie wyłączający przepis ustawy o SIS (sekcja 15), zawsze należy podać inne powody – takie, które nie zasugerują, że zarejestrowano dane nie podlegające ujawnieniu.

6. Najważniejsze przepisy krajowe

Ustawa dotycząca systemu informacyjnego Schengen (LOV 1999-07-16-66)

Rozporządzenia do ustawy nr 66 z dnia 16 lipca 1999 r. dotyczącej systemu informacyjnego Schengen (rozporządzenia SIS).

XXIV. POLSKA

1. Charakter gwarantowanego dostępu

Obowiązuje prawo do bezpośredniego dostępu do informacji.

2. Dane teleadresowe organu, do którego należy kierować wniosek

W myśl ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w systemie informacyjnym Schengen oraz systemie informacji wizowej, w Polsce administratorem danych przetwarzanych w systemie informacyjnym Schengen jest Komendant Główny Policji. Wnioski o dostęp do danych lub ich modyfikacje należy kierować do niego.

Adres do korespondencji:
Komenda Główna Policji
Centralny Organ Techniczny KSI
02-514 Warszawa
ul. Puławska 148/150
Poland

Jeżeli potrzebna jest konsultacja co do treści wniosku o dostęp do danych osobowych, można się z nami kontaktować telefonicznie lub elektronicznie:

Tel.: +48 (22) 601-53-29
Tel.: +48 (22) 601-53-15
E-mail: cot.admin.ksi@policja.gov.pl

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Każdej osobie przysługuje prawo do uzyskania wyczerpującej informacji o dotyczących jej danych osobowych, które przetwarza sie w zbiorach danych.

W myśl art. 32 ust. 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r., poz. 2135) zainteresowany może skorzystać z prawa do informacji nie częściej niż raz na 6 miesięcy.

Za wniosek o dostępu nie pobiera sie żadnych opłat.

W myśl art. 32 ust. 1–5a ustawy o ochronie danych osobowych osoba, której dotyczą dane, ma

prawo wystąpić o uzyskanie następujących informacji na temat przetwarzania jej danych osobowych:

- czy jej dane figurują w systemie
- od kiedy przetwarza sie jej dane
- z jakiego źródła dane te pochodzą
- w jaki sposób sie je udostępnia
- w jakim celu i zakresie są one przetwarzane
- w jakim zakresie i komu sie je udostępnia.

Administrator udziela żądanych informacji w terminie 30 dni. Aby informacje te uzyskać, należy złożyć pisemny wniosek w języku polskim.

We wniosku należy podać:

1. imię i nazwisko zainteresowanego
2. polski krajowy numer identyfikacyjny PESEL (jeżeli dotyczy)
3. obywatelstwo
4. datę i miejsce urodzenia
5. kserokopie dowodu tożsamości zawierającego czytelny wizerunek posiadacza
6. miejsce zamieszkania (kraj, miejscowość, ulice oraz numer domu lub mieszkania)
7. przedmiot wniosku
8. podpis zainteresowanego.

W myśl art. 32 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2013 r., poz. 267 z późn. zm) strona może być reprezentowana w postępowaniu administracyjnym przez pełnomocnika, chyba że charakter czynności wymaga jej osobistego działania. W art. 33 kodeksu określone są zasady ustanawiania pełnomocnictwa procesowego:

- pełnomocnikiem może być osoba fizyczna posiadająca zdolność do czynności prawnych
- pełnomocnictwo powinno być zgłoszone na piśmie
- pełnomocnik dołącza do akt oryginał lub urzędowo poświadczony odpis pełnomocnictwa. Adwokat, radca prawny lub rzecznik patentowy może sam uwierzytelnić odpis udzielonego mu pełnomocnictwa.

Odmowa udzielenia informacji o przetwarzanych danych osobowych

W myśl art. 30 ustawy o ochronie danych osobowych administrator może odmówić ich udostępnienia, jeżeli spowodowałoby to:

1. ujawnienie wiadomości stanowiących tajemnice państwową,
2. zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego,
3. zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
4. istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

Prawo do żądania sprostowania danych, wstrzymania ich przetwarzania lub ich usunięcia

Zainteresowany może wystąpić do administratora o uzupełnienie, uaktualnienie, sprostowanie, usuniecie oraz czasowe lub stałe wstrzymanie przetwarzania swoich danych. Niemniej zainteresowany musi wykazać, że dane są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są już zbędne do realizacji celu, dla którego zostały zebrane.

Wniosek jest rozpatrywany zgodnie z przepisami Kodeksu postępowania administracyjnego.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Aby zapewnić odpowiedni poziom ochrony prawnej osób, których dane są przechowywane w systemie informacyjnym Schengen, Generalny Inspektor Ochrony Danych Osobowych kontroluje, czy wykorzystywanie danych nie narusza praw osób, których one dotyczą. Kontrole te sprawuje zgodnie z przepisami o ochronie danych osobowych.

Adres do korespondencji:
Biuro Generalnego Inspektora Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa
Poland
tel. +48 (22) 53 10 440
fax +48 (22) 53 10 441
http://www.giodo.gov.pl
kancelaria@giodo.gov.pl

Każda osoba, której dane są przetwarzane w systemie informacyjnym Schengen, ma prawo wnieść skargę do Generalnego Inspektora Ochrony Danych Osobowych na wykonywanie przepisów o ochronie danych osobowych.

5. Najważniejsze przepisy krajowe

- Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
- Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego
- Ustawa z dnia 7 października 1999 r. o języku polskim.

XXV. PORTUGALIA

1. Charakter gwarantowanego dostępu

Obywatele mają prawo do dostępu, poprawienia i usunięcia danych SIS pośredniego poprzez Krajowy Urząd Ochrony Danych.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Comissão Nacional de Protecção de Dados [*krajowa komisja ochrony danych*]

Rua de S. Bento, 148, 3º

1200-821 Lisboa

PORTUGAL

Tel.: (+351) 213 928 400

Faks: (+351) 213 976 832

www.cnpd.pt

Infolinia: (00.351) 393 00 39 (od poniedziałku do piątku w godz. 10:00 – 13:00)

Osobiste porady: od poniedziałku do piątku w godz. 14.30 – 16.30h

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Wniosek należy złożyć pisemnie na jednym z dwóch przeznaczonych do tego formularzy, z których jeden dotyczy prawa dostępu, a drugi – żądania sprostowania lub usunięcia. Formularze te są dostępne na internetowej stronie urzędu po portugalsku, angielsku i francusku. Wniosek można złożyć osobiście (w recepcji urzędu) lub wysłać pocztą. Aby uzyskać dostęp do swoich danych, zainteresowany musi okazać dokument potwierdzający jego tożsamość (np. paszport) lub dołączyć jego poświadczoną kopie do wysyłanego wniosku. Korzystanie z prawa dostępu jest bezpłatne.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Dane teleadresowe krajowego organu ochrony danych osobowych wskazano w pkt. 2. Wszelkie informacje o prawach osób w odniesieniu do Systemu Informacyjnego Schengen są dostępne po portugalsku, angielsku i francusku na stronie internetowej organu.

5. Oczekiwany skutek. Treść podawanych informacji

Organ ochrony danych dokonuje wszelkich koniecznych sprawdzeń w organie właściwym I udziela odpowiedzi wnioskującemu najszybciej jak to jest możliwe, nie później niż w ciągu 30 dni od otrzymania wniosku. W wypadku wniosku o poprawienie lub usunięcie danych, jesli organ ochrony

danych osobowych nie może udzielić ostatecznej odpowiedzi, poinformuje wnioskującego w ciągu 90 dni o podjętych działaniach.

6. Najważniejsze przepisy krajowe

Zastosowanie mają ustawa nr 67/98 z dnia 26 października 1998 r. (art. 11 ust. 2) oraz ustawa nr 2/94 z dnia 19 lutego 1994 r.

7. Wymagany język

Wnioski musza być składane po portugalsku, wszelkie dokumenty do nich dołączone też muszą być przetłumaczone na portugalski. W razie potrzeby przedstawiciele organu pomogą w wypełnieniu wniosku.

XXVI. RUMUNIA

1. Charakter prawa dostępu

Prawo dostępu w Rumunii ma charakter bezpośredni.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Zgodnie z art. 63 ust. 3 ustawy 141/2010 o stworzeniu, organizacji i funkcjonowaniu Krajowego Systemu Wpisów (NISA) i udziale Rumunii w Systemie Informacyjnym Schengen, wnioski mogą być składane do krajowego Biura SIRENE lub do innego administratora w Ministerstwie Administracji i Spraw Wewnętrznych lub w jego strukturach, które prześlą wniosek do krajowego Biura SIRENE w ciągu 5 dni od jego wpłynięcia.

Adres korespondencyjny:
Centrum Międzynarodowej Współpracy Policji
Biuro SIRENE
1-5 Calea 13 Septembrie, Bucharest, 5th District
Rumunia
Tel.: +40 21 315 96 26
Tel.: +40 21 314 05 40
Fax: +40 21 314 12 66
Fax: +40 21 312 36 00
E-mail: ccpi@mai.gov.ro

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Prawa osób, względem danych przetwarzanych w NISA lub SIS II określono w ustawie 677/2001 o ochronie danych osobowych i swobodnym przepływie tych danych, z późniejszymi zmianami i wskazanymi w prawie wyjątkami.
Zgodnie z art. 13 ust. 1 ustawy 677/2001, złożenie wniosku jest bezpłatne.
Osoba, której dane dotyczą, nie zostanie poinformowana o swoich danych przetwarzanych w NISA lub SIS II tak długo, jak jest to niezbędne do wykonania działań na podstawie wpisu lub ze względu

na ochronę praw i wolności innych osób.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Legalność przetwarzania danych w N.SIS na terytorium Rumunii i przekazywania tych danych zagranicę, a także dalsza wymiana i przetwarzanie dodatkowych informacji podlegają nadzorowi i kontroli Krajowego organu ochrony danych osobowych.

Audyt przetwarzania danych osobowych prowadzonych jest przez krajowy organ ochrony danych osobowych zgodnie z międzynarodowymi standardami audyty, co najmniej co 4 lata.

Adres do korespondencji:
National Supervisory Authority For Personal Data Processing
28-30 G-ral Gheorghe Magheru Bld.
Bucharest, 1st district 1
Romania
Tel.: +40 31 805 92 11
Fax: +40 31 805 96 02
E-mail: anspdcp@dataprotection.ro

5. Oczekiwany skutek. Treść podawanych informacji

Wnioski osób, których dane są przetwarzane w NISA lub SIS II mogą być składane tylko do krajowego Biura SIRENE, które przekazuje odpowiedź wnioskodawcy tak szybko jak to możliwe, ale nie później niż 60 dni od chwili otrzymania wniosku w wypadku korzystania z prawa dostępu, a nie później niż 90 dni od otrzymania wniosku w wypadku korzystania z prawa do poprawienia lub usunięcia danych, zgodnie z postanowieniami ustawy 677/2001 z późniejszymi modyfikacjami i zmianami.

6. Najważniejsze przepisy krajowe

- Ustawa nr no. 141 z dnia 12 lipca 2010 o stworzeniu, organizacji i funkcjonowaniu Krajowego Systemu Wpisów (NISA) i udziale Rumunii w Systemie Informacyjnym Schengen,
- Ustawa 677 z dnia 21 listopada 2001 o ochronie danych osobowych i swobodnym przepływie tych danych, z późniejszymi zmianami i wskazanymi w prawie wyjątkami.

7. Wymagany język

Jeśli osoba, której dane dotyczą, jest obywatelem Rumunii, powinna złożyć wniosek po rumuńsku.

Jeśli osoba, której dane dotyczą, jest cudzoziemcem, może złożyć wniosek po angielsku.

XXVII. SŁOWACJA

1. Charakter gwarantowanego dostępu

W myśl art. 41 rozporządzenia SIS II i art. 58 decyzji SIS II każdy ma prawo dostępu do swoich danych wprowadzonych do Systemu Informacyjnego Schengen. Z prawa tego korzysta sie zgodnie z prawem krajowym umawiającej się strony. Na Słowacji osoba, której dotyczą dane, ma prawo do bezpośredniego dostępu.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski o dostęp należy kierować do Ministerstwa Spraw Wewnętrznych, które jest administratorem danych:

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY [*ministerstwo spraw wewnętrznych Republiki Słowackiej*]

Pribinova 2, 812 72 Bratislava

Slovenská republika

Tel.: 02/5094 1111

Faks: 02/5094 4397

E-mail: statny.dozor@pdp.gov.sk

Internet: http://www.dataprotection.gov.sk

3. Kwestie formalne: potrzebne informacje i dokumenty

W myśl art. 69c ustawy nr 171/1993 Zb. o siłach policji każdy ma prawo wystąpić na piśmie do Ministerstwa Spraw Wewnętrznych o ewentualne informacje, jakie dane osobowe go dotyczące się przetwarza. Administrator Systemu Informacyjnego Schengen ma obowiązek udzielić informacji bezpłatnie w terminie 30 dni od daty otrzymania takiego **pisemnego wniosku**.

Standardowy formularz wniosku jest dostępny na stronie internetowej Ministerstwa Spraw Wewnętrznych. Zainteresowany musi podać swoje dane identyfikacyjne (imię, nazwisko, adres stałego zamieszkania, miejsce i pełna datę urodzenia oraz obywatelstwo) i jako potwierdzenie tożsamości dołączyć kopię dowodu osobistego lub paszportu.

4. Oczekiwany skutek. Treść podawanych informacji

Informacji o danych osobowych zawartych w systemach informacyjnych używanych przez policję udziela sie zainteresowanemu na podstawie art. 69c ustawy nr 171/1993 Zb. o siłach policji.

W przypadku Systemu Informacyjnego Schengen, jeżeli wpis ma za podstawę art. 26 - 34 oraz art. 38 decyzji SIS II, zainteresowany otrzyma informacje o dotyczących go danych (przynajmniej o: imieniu, nazwisku, dacie i miejscu urodzenia, płci, obywatelstwie i przyczynie wpisu, tzn. o celu, w jakim przetwarza sie jego dane osobowe).

Jeżeli wniosek o dostęp do informacji dotyczy wpisu, którego dokonało inne państwo, należy państwu temu zapewnić możliwość zajęcia stanowiska co do ewentualnego ujawnienia danych zainteresowanemu.

Jeżeli wpis ma za podstawę art. 36 decyzji SIS II, zainteresowany najprawdopodobniej otrzyma odmowę ujawnienia danych (które były przetwarzane ze względu na bezpieczeństwo państwa lub w związku z dochodzeniem w sprawie szczególnie poważnych czynów zabronionych). Innymi słowy, zainteresowanemu odmawia sie udzielenia informacji, jeżeli jest to konieczne, by zapewnić wykonanie uprawnionej czynności żądanej we wpisie lub chronić prawa i swobody osób trzecich. Natomiast jeżeli wpis służy wszczęciu obserwacji niejawnej, odmowa będzie udzielana przez cały okres jego ważności.

W myśl art. 69c ustawy nr 171/1993 Zb. o siłach policji zainteresowany ma prawo **wystąpić na piśmie** do Ministerstwa Spraw Wewnętrznych o sprostowanie lub usuniecie jego danych osobowych przetwarzanych w Systemie Informacyjnym Schengen (standardowe formularze wniosku o usunięcie lub sprostowanie danych są dostępne na stronie internetowej ministerstwa).

Jeżeli zainteresowany podejrzewa, że jego dane osobowe są przetwarzane bezprawnie, może w myśl art. 20 ust. 6 ustawy o ochronie danych wnieść **skargę** bezpośrednio do Urzędu Ochrony Danych Osobowych Republiki Słowackiej, który sprawdza wtedy, czy doszło do naruszenia praw zainteresowanego podczas przetwarzania i używania jego danych osobowych przechowywanych w Systemie Informacyjnym Schengen.
Wnoszenie skarg podlega przepisom art. 45 ustawy nr 428/2002 Zb. o ochronie danych osobowych (standardowy formularz skargi jest dostępny na stronie internetowej Ministerstwa Spraw Wewnętrznych).

5. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Úrad na ochranu osobných údajov Slovenskej republiky [*urząd ochrony danych osobowych Republiki Słowackiej*]

Odborárske nám. 3

817 60 Bratislava 15

Slovenská republika

Tel.: +421 2 502 39 418

Faks: +421 2 502 39 441

E-mail: statny.dozor@pdp.gov.sk

Internet: http://www.dataprotection.gov.sk

6. Najważniejsze odnośne przepisy krajowe

Ustawa nr 428/2002 Zb. o ochronie danych osobowych z późniejszymi zmianami z ustawy nr 84/2014.

XXVIII. SŁOWENIA

1. Charakter gwarantowanego dostępu

Obowiązuje prawo do dostępu bezpośredniego.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wniosek można złożyć na piśmie albo w formie ustnej (zostaje wtedy zaprotokołowany) na policji (Ministerstwo Spraw Wewnętrznych) pod następującym adresem:

Policija, Ministrstvo za notranje zadeve [*policja, ministerstwo spraw wewnętrznych*]
Štefanova 2
1501 Ljubljana
Slovenia
Faks: + 386 1 428 47 33
E-mail: gp.mnz@gov.si

Wniosek można też złożyć na każdym przejściu granicznym, w dziale administracyjnym oraz w słoweńskich placówkach dyplomatycznych i konsularnych za granicą. Zostaje on wtedy natychmiast przekazany policji.

Formularz wniosku o informacje na temat danych figurujących w krajowym Systemie Informacyjnym Schengen w Słowenii (N.SIS) można pobrać pod adresem: http://www.ip-rs.si/index.php?id=346 (w języku angielskim).

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Korzystanie z prawa wglądu do własnych danych osobowych w Słowenii podlega przepisom ustawy o ochronie danych osobowych (art. 30 i 31) oraz ustawy o inspektorze informacji.

Artykuł 30 ustawy o danych osobowych nakłada na policje (czyli administratora danych) – która jako organ podlega Ministerstwu Spraw Wewnętrznych – obowiązek, by:
1. umożliwić wgląd do katalogu zbiorów danych SIS
2. zaświadczyć, czy dane zainteresowanego są przetwarzane, umożliwić mu wgląd do jego danych osobowych zawartych w zbiorach danych SIS i ich przepisanie lub skopiowanie
3. wydać mu odpis jego danych osobowych zawartych w krajowych zbiorach danych SIS

4. wydać mu listę informująca, komu, kiedy, na jakiej podstawie i w jakim celu przekazano jego dane osobowe
5. poinformować o źródłach, z których pochodzą wpisy o nim przechowywane w SIS, oraz o metodach przetwarzania
6. poinformować o celu przetwarzania i rodzaju danych osobowych przetwarzanych w SIS oraz udzielić wszelkich koniecznych wyjaśnień w tym względzie
7. wyjaśnić techniczne i logiczno-techniczne procedury decyzyjne.

Rozpatrzenie wniosku nie podlega obecnie żadnym opłatom. Zainteresowany może zostać jedynie obciążony kosztami wykonania kserokopii, zgodnie z instrukcja obciążania kosztami za korzystanie z prawa dostępu do swoich danych osobowych.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Informacijski pooblaščenec
[*inspektor informacji*]
Vošnjakova 1
p.p. 78
1001 Ljubljana
Slovenia
Tel.: ++ 386 1 230 97 30
Faks: ++ 386 1 230 97 78
E-mail: gp.ip@ip-rs.si
Internet: www.ip-rs.si

Inspektor Informacji jest organem, do którego powinien odwołać sie zainteresowany, jeżeli jego wniosek o wgląd do danych osobowych został rozpatrzony odmownie lub jeżeli na wniosek ten nie otrzymał odpowiedzi właściwego organu.
Jeżeli zdaniem zainteresowanego doszło do naruszenia jego praw pod względem dostępu, może on wnieść skargę do Inspektora Informacji. Otrzymawszy skargę, Inspektor Informacji przekazuje ją administratorowi zbioru danych, tak by mógł on zająć stanowisko. Po zapoznaniu sie z tym stanowiskiem oraz raportami, dowodami i innymi dokumentami dochodzeniowymi (w tym po zapoznaniu sie w razie konieczności ze zbiorami danych oraz po rozmowie z zainteresowanym

i z administratorem zbioru danych) Inspektor Informacji ostatecznie podejmuje w sprawie skargi decyzje, która przekazuje zainteresowanym stronom.

Rozpatrzenie skargi nie podlega obecnie żadnym opłatom.

5. Oczekiwany skutek. Treść podawanych informacji

Jeżeli dane zainteresowanego figurują w zbiorze danych SIS i jeżeli wniosek został rozpatrzony pozytywnie, administrator zbioru danych udostępnia zainteresowanemu jego dane w żądanej formie, najpóźniej w terminie 15 dni od dnia otrzymania wniosku policja musi zainteresowanemu umożliwić wgląd do danych, ich przepisanie, skopiowanie i uzyskanie zaświadczenia albo – w tym samym terminie – poinformować go na piśmie o przesłankach odmowy. W terminie 30 dni od dnia otrzymania wniosku policja ma obowiązek wydać zainteresowanemu odpis (określony w ppkt 3), listę (określona w ppkt 4), informacje (określone w ppkt 5 i 6) oraz wyjaśnienie (określone w ppkt 7) lub – w tym samym terminie – poinformować go na piśmie o przesłankach odmowy.

Oprócz tego prawo zainteresowanego do wglądu do jego danych może ulec wyjątkowemu prawnemu ograniczeniu, w myśl art. 36 ustawy o ochronie danych osobowych, przez wzgląd na ochronę suwerenności państwa i obronności, ochronę bezpieczeństwa narodowego i konstytucyjnego porządku państwa, interes państwa w dziedzinie bezpieczeństwa, polityki i gospodarki, sprawowanie obowiązków przez policje, uniemożliwianie, ujawnianie, wykrywanie, dowodzenie i ściganie przestępstw i wykroczeń, ujawnianie i karanie naruszeń norm etycznych niektórych zawodów, kwestie monetarne, budżetowe i podatkowe, nadzór nad policja oraz ochronę osoby, której dotyczą dane osobowe, lub ochronę praw i swobód osób trzecich. Ograniczenia te są dozwolone tylko w zakresie koniecznym do osiągnięcia celu, w którym sie je wprowadza.

6. Najważniejsze przepisy krajowe

• Ustawa o ochronie danych osobowych (Dziennik Urzędowy Republiki Słowenii nr 94/2007, tekst ujednolicony), tłumaczenie ustawy na angielski niemające mocy prawnej jest dostępne pod adresem: http://www.ip-rs.si/index.php?id=339

• Ustawa o Inspektorze Informacji (Dziennik Urzędowy Republiki Słowenii nr 113/2005), tłumaczenie ustawy na angielski niemające mocy prawnej jest dostępne pod adresem: http://www.ip-rs.si/index.php?id=325

• Instrukcja obciążania kosztami za korzystanie z prawa do dostępu do danych osobowych (Dziennik Urzędowy Republiki Słowenii nr 85/2007), tekst tylko w wersji słoweńskiej jest

dostępny pod adresem: http://www.ip-rs.si/zakonodaja/zakon-o-varstvu-osebnihpodatkov/pravilnik-o-zaracunavanju-stroskov-pri-izvrsevanju-pravice-posameznika-doseznanitve-z-lastnimi-osebnimi-podatki/

XXIX. HISZPANIA

1. Charakter gwarantowanego dostępu

Osoba, której dotyczą dane, ma prawo do bezpośredniego dostępu. Tym niemniej, jeśli administrator nie odpowie na wniosek lub jeśli jego odpowiedź nie będzie niezadowalającą, osoba, której dane dotycz, ma prawo do pośredniego dostępu za pośrednictwem hiszpańskiego organu ochrony danych osobowych.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski o dostęp do informacji należy kierować na adres:

Secretaría de Estado de Seguridad [*państwowy wydział bezpieczeństwa*]
Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad,
C/ López Santos, 6,
28230 Las Rozas (Madrid)
Spain

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Wniosek o dostęp należy skierować na piśmie do administratora danych (*Secretaria de Estado de Seguridad del Ministerio del Interior*). Zainteresowany może zwrócić sie do administratora danych dowolna droga, która zapewni dowód nadania i potwierdzenie odbioru.

Nie ma standardowego formularza wniosku ani żadnych wymogów formalnych. Niemniej jak wynika z ogólnej procedury administracyjnej, we wniosku należy sprecyzować jego cel i należy dołączyć do niego kserokopie dokumentu potwierdzającego tożsamość zainteresowanego (np. kopie dowodu osobistego lub paszportu). Ponadto zainteresowany może dołączyć kopie wszelkich dokumentów, które uzna za istotne w związku z prośba wyrażoną we wniosku.

Procedura jest bezpłatna.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Agencia Española de Protección de Datos [*hiszpański urząd ochrony danych*]
C/ Jorge Juan, 6

E - 28001 – Madrid

Tel.: + 34 901 100 099

Fax: + 34 91 445 56 99

E-mail: ciudadano@agpd.es

Internet: www.agpd.es

Jak wspomniano, osoba, której dotyczą dane, ma prawo do bezpośredniego dostępu. Oprócz tego ma prawo do dostępu pośredniego (za pośrednictwem hiszpańskiego organu ochrony danych osobowych), jeżeli nie otrzyma odpowiedzi od administratora danych na wniosek o dostęp lub jeżeli otrzymana odpowiedz jest niezadowalającą. W obu przypadkach zainteresowany może wnieść skargę do hiszpańskiego organu ochrony danych. Na mocy art. 117 dekretu królewskiego 1720/2007, którym zostało zatwierdzone rozporządzenie wykonawcze do ustawy organicznej 15/1999 o ochronie danych osobowych, postępowanie wszczyna sie na wniosek zainteresowanego: musi on jasno określić przedmiot swojej skargi i wskazać przepisy wspomnianej ustawy, które jego zdaniem zostały naruszone.

Gdy hiszpański organ ochrony danych otrzyma skargę, wszczyna postępowanie o ochronę praw osobistych. Zgodnie z procedura urząd przekazuje skargę administratorowi danych, by mógł on – jako organ administracyjny – udzielić stosownych wyjaśnień co do odmowy dostępu lub odpowiedzi udzielonej zainteresowanemu.

Ewentualne wyjaśnienia administratora przekazuje sie zainteresowanemu, który może ponownie zając stanowisko i zgłosić dodatkowe uwagi. Jego uwagi zostają przekazane administratorowi danych, który może ustosunkować sie do swojej decyzji oraz do stanowiska i uwag zainteresowanego.

Po otrzymaniu wyjaśnień oraz innych informacji i dokumentów dyrektor hiszpańskiego organu ochrony danych wydaje decyzja w sprawie skargi.

Należy podkreślić, że termin na wydanie i ogłoszenie decyzji wynosi 6 miesięcy od daty wpłynięcia skargi do urzędu.

Jeżeli decyzja jest korzystna dla zainteresowanego, urząd informuje o niej administratora danych, który w terminie 10 dni od ogłoszenia decyzji jest zobowiązany umożliwić zainteresowanemu

skorzystanie z prawa do dostępu. Ponadto administrator musi w tym samym terminie na piśmie zdać sprawę urzędowi z wypełnienia decyzji.

5. Oczekiwany skutek. Treść podawanych informacji

Jeżeli wpisu dokonał organ hiszpański, o treści informacji przekazywanej zainteresowanemu decyduje administrator danych. Zazwyczaj zainteresowany otrzymuje kopie akt zawierających dane osobowe przechowywane w zbiorze danych.

Jeżeli jednak wpisu dokonał organ innego państwa strefy Schengen, administrator danych musi o otrzymanym wniosku poinformować administratora w tym innym państwie, zgodnie z zasadą współpracy miedzy organami krajowymi pod względem ochrony danych osobowych. Decyzje o tym, jakie dane można ujawnić zainteresowanemu, podejmują wtedy organy tego innego państwa strefy Schengen.

6. Wymagany język

Zainteresowany, które chce w Hiszpanii skorzystać z prawa dostępu, powinien w kontaktach z organami publicznymi używać języka hiszpańskiego.

7. Formularze

Hiszpański organ ochrony danych osobowych na swojej stronie internetowej umieścił nieoficjalny formularz (po hiszpańsku) ws. prawa dostępu, który morze być wykorzystywane przez osoby, których dane dotyczą. Formularz można znaleźć pod następującym linkiem: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/derecho_schengen_den/common/DERECHO_DE_ACCESO_Schengen_Es.pdf.

Osoby, których dane dotyczą, które chcą złożyć skargę do hiszpańskiego organu ochrony danych mogą skorzystać z informacji dostępnych pod linkiem (dostępne tylko po hiszpańsku): https://sedeagpd.gob.es/sede-electronica-web/vistas/formReclamacionDerechos/tipoSolicitud/solicitudPresencial.jsf

XXX. SZWECJA

1. **Charakter gwarantowanego dostępu**

   Obowiązuje prawo do dostępu bezpośredniego.

2. **Dane teleadresowe organu, do którego należy kierować wniosek**

   Wniosek o dostęp należy kierować do *Rikspolisstyrelsen* (policji państwowej), która jest organem odpowiadającym za szwedzki moduł Systemu Informacyjnego Schengen.

   Rikspolisstyrelsen
   Box 12256
   Polhemsgatan 30
   S - 102 26 Stockholm
   Tel.: ++46 (0)8-401 90 00
   Faks: ++46 (0)8-401 99 90
   E-mail: rikspolisstyrelsen@polisen.se
   Internet: www.polisen.se

3. **Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty**

   Wniosek do zarządu policji państwowej należy sformułować na piśmie i opatrzyć własnoręcznym podpisem. Zasadniczo odpowiedz powinna zostać udzielona w terminie jednego miesiąca.

   Zainteresowany ma prawo raz w roku kalendarzowym do bezpłatnego dostępu do informacji.

4. **Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji**

   Datainspektionen [*organ ochrony danych*]
   Box 8114
   Fleminggatan 14, 9th floor
   S - 104 20 Stockholm
   Tel.: ++46 (0)8-657 61 00
   Faks: ++46 (0)8-652 86 52
   E-mail: datainspektionen@datainspektionen.se
   Internet: www.datainspektionen.se

Organ ochrony danych kontroluje, czy dane w Szwecji przetwarza się zgodnie z przepisami ustawy o danych osobowych i innych aktów o ochronie danych. Może wszcząć kontrole albo na podstawie skargi, albo z własnej inicjatywy. Zainteresowany, którego nie satysfakcjonuje sposób potraktowania jego wniosku o dostęp do informacji zawartych w SIS, może wnieść skargę do komisji. Skutkiem może być dochodzenie sprawdzające, czy nie naruszono przepisów o prawie do dostępu. Poza tym od decyzji Policji Państwowej na temat prawa do dostępu można się też odwołać do sądu administracyjnego.

5. Oczekiwany skutek. Treść podawanych informacji

Ujawnienie informacji zależy od przepisów ustawy o tajności (1980:100), które mogą zakazywać ujawniania niektórych danych. Gdy jednak ujawnienie danych jest dozwolone, Policja Państwowa odpowiada za ich przekazanie.

6. Najważniejsze przepisy krajowe

Mające zastosowanie przepisy: sekcja 26 i 27 ustawy o danych osobowych (1998:204) oraz sekcja 8 ustawy o systemie informacyjnym Schengen (2000:344).

7. Wymagany język

W Szwecji nie ma wyraźnych zasad regulujących to zagadnienie. Akceptowane są także wnioski po angielsku.

XXXI. SZWAJCARIA

1. Charakter gwarantowanego dostępu

Obowiązuje prawo do dostępu bezpośredniego. Organem właściwym do rozpatrywania wniosków o dostęp do danych osobowych zawartych w SIS jest inspektor ochrony danych w Federalnym Urzędzie Policji w Szwajcarii.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Federal Office of Police [*federalny urzad policji*]
Data Protection Officer or SIRENE Office
Nussbaumstrasse 29
CH-3003 Berne
www.fedpol.ch

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Wnioski dotyczące własnych danych osobowych przetwarzanych w SIS zainteresowani powinni kierować bezpośrednio do Federalnego Urzędu Policji, który jest administratorem zbioru danych SIS w Szwajcarii. Wnioski powinny być przesyłane w formie pisemnej wraz z kopią dowodu tożsamości lub paszportu oraz pełnomocnictwem, jeśli osoba działa poprzez pełnomocnika. Jeśli wniosek przesyłany jest drogą mailową, osoba musi wskazać swój adres pocztowy i przesłać kopię dowodu osobistego lub paszportu.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Federal Data Protection and Information Commissioner (FDPIC)
[*federalny inspektor ochrony danych i informacji*]
Feldeggweg 1,
CH-3003 Berne
Phone: +41(0)31 322 43 95, Fax +41-(0)31 325 99 96
http://www.edoeb.admin.ch/index.html?lang=en

5. Oczekiwany skutek. Treść podawanych informacji

Zgodnie z art. 50 § 4 zarządzenia w sprawie krajowej części Systemu Informacyjnego Schengen (N-SIS) i Biura SIRENE (dalej zwane zarządzeniem N-SIS), osoba, której dane dotyczą, powinna być poinformowana w ciągu 30 dni od złożenia wniosku o dostęp do danych. Jeśli nie można jej udzielić odpowiedzi w tym terminie, wnioskujący musi zostać poinformowany o tym opóźnieniu. Wnioskujący musi zostać poinformowany nie później niż w ciągu 60 dni od złożenia wniosku. Jeśli nie podstaw do odmowy, osoba, której dane dotyczą, musi zostać w pełni poinformowana o swoich danych.

Zgodnie z art. 50 § 5 zarządzenia N-SIS, osoba, której dane dotyczą, powinna być poinformowana nie później niż w ciągu 3 miesięcy od daty złożenia wniosku w sprawie poprawienia lub usunięcia danych.

Prawo do informacji w przypadku odmowy wjazdu regulowane jest w art. 51 zarządzenia N-SIS.

6. Najważniejsze przepisy krajowe

- Federalna ustawa o ochronie danych z dnia 19 czerwca 1992 r. (FADP; RS. 235.1)
- Zarzadzenie z dnia 14 czerwca 1993 r. Dot. Federalnej ustawy o ochronie danych (OFADP; RS. 235.1)
- Zarządzenie w sprawie krajowej częsci Systemu Informacyjnego Schengen (N-SIS) i Biurze SIRENE (N-SIS Ordinance; RS. 362.0)

7. Wymagany język

Wnioski mogą być składane po francusku, niemiecku, włosku lub angielsku.

XXXII. WIELKA BRYTANIA

1. Charakter prawa dostępu

W Wielkiej Brytanii prawo dostępu ma charakter bezpośredni. Osoba, której dane dotyczą, składa wniosek do organów przetwarzających dane np. do lokalnej jednostki policji. Potem jest on przekazywany do rozpatrzenia *ACRO – Biura rejestrów karnych.* Alternatywnie osoba może zwrócić się od razu bezpośrednio do ACRO.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski powinny być kierowane do *ACRO Biura Rejestrów karnych*

Strona internetowa: https://www.acro.police.uk/subject_access.aspx

lub adres pocztowy

ACRO (SAR)

PO Box 662

FAREHAM

PO14 9LQ

3. Kwestie formalne: potrzebne informacje i dokumenty – ewentualne koszty

Wnioski o dostęp są odpłatne – 10 funtów zgodnie z Narodowymi zasadami dot. wniosków o dostęp. Osoby, których dane dotyczą, muszą wypełnić wniosek i dostarczyć dwa, odrębne, dowody/dokumenty potwierdzające tożsamość, które muszą zawierać imię i nazwisko wnioskującego, datę urodzenia, aktualny adres pocztowy i podpis.

4. Dane teleadresowe krajowego organu ochrony danych i zakres jego ewentualnej interwencji

Information Commissioner's Office

Wycliffe House Water Lane

Wilmslow

Cheshire

SK9 5AF

Tel: 0303 123 1113 (opłata lokalna) lub 01625 545 745 (opłata krajowa)

Fax: 01625 524 510

Email: casework@ico.org.uk (e-mail musi zawierać numer telefonu skarżącego)

Jeśli składasz skargę do ICO na sposób załatwienia Twojego wniosku o dostęp, ICO wykorzysta informacje od Ciebie otrzymane, w tym odpowiedź administrator na Twoje zastrzeżenia,, do stwierdzenia czy Twoje doświadczenia mogą przyczynić się do poprawienia praktyki dotyczącej prawa do informacji. I w takim przypadku zostaną podjęte działania przez ICO. Co do zasady ICO nie prowadzi postępowań, jeśli skarga nie została skierowana do ICO bez nieuzasadnionej zwłoki. Swoje wątpliwości trzeba skierować do ICO w ciągu 3 miesięcy od ostatniego znaczącego kontaktu z administratorem.

5. Oczekiwany skutek. Treść podawanych informacji

Odpowiedź na wniosek w sprawie dostępu do danych musi zostać udzielona osobie, której dane dotyczą, w ciągu 40 dni od otrzymania wniosku. Dział 28 i 29 ustawy o ochronie danych zawiera szczególne zasady dot. nieujawniania informacji w odpowiedzi.

6. Najważniejsze przepisy krajowe

Wpisy utworzone przez organy Wielkiej Brytanii będą rozpatrywane w ramach krajowego przetwarzania i ustawy o ochronie danych z 1998 r. Wpisy utworzone przez inne państwa będą rozpatrywane w ramach transgranicznego przetwarzania (protokół 36 rozporządzenia 28) – część 4 *Rozporządzenie ws. wymiaru sprawiedliwości i ochrony danych osobowych (Protokół nr 36).*

7. Wymagany język

Wszystkie odpowiedzi na wnioski o dostęp udzielane są po angielsku.

ANEKSY (WZORY WNIOSKÓW)

Następujące wzory wniosków mogą być wykorzystane przy składaniu wniosków, chyba, że krajowy organ, do którego się zwracasz wymaga złożenia wniosków na innym formularzu.

Aneks 1

Wzór wniosku o dostęp do danych

To: **Nazwa i adres właściwego organu**

DD-MM-RRRR,
Miejscowość

Szanowni Państwo,

Zgodnie z art. 41 rozporządzenia (WE) 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz art. 58 Decyzji Rady 2007/533/JHA z dnia 12 czerwca 2007 w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) ,
Ja,_____(imię, nazwisko),_____(obywatelstwo), _____(data i miejsce urodzenia),_____(adres), proszę o dostęp do moich danych osobowych, figurujących w Systemie Informacyjnym Schengen.

Do wniosku dołączam:
1. Kopie dokumentu tożsamości (paszportu/dowodu osobistego/prawa jazdy/innego ważnego dokumentu tożsamości) ważnego w myśl przepisów państwa strefy Schengen;
2. Kopie pełnomocnictwa do reprezentowania wnioskodawcy;
3. Inne.

Wnioskodawca / Pełnomocnik

(Podpis)

Aneks 2

Wzór wniosku w sprawie poprawienia lub usunięcia przetwarzanych danych osobowych

To: **Nazwa i adres właściwego organu**

DD-MM-RRRR,

Miejscowość

Szanowni Państwo,

Zgodnie z art. 41 ust. 5 rozporządzenia (WE) 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz art. 58 ust. 5 Decyzji Rady 2007/533/JHA z dnia 12 czerwca 2007 w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II),

Ja,_____(imię, nazwisko),_____(obywatelstwo),

_____(data i miejsce urodzenia), _____(adres),

proszę o sprostowanie nieścisłości w moich danych osobowych lub usunięcie danych dotyczących mojej osoby, które zostały bezprawnie przechowywanych w Systemie Informacyjnym Schengen. Moje dane osobowe powinny być poprawione / usunięte, ponieważ:

_____

_____

_____

_____

Do wniosku dołączam:

1. Kopie dokumentu tożsamości (paszportu/dowodu osobistego/prawa jazdy/innego ważnego dokumentu tożsamości) ważnego w myśl przepisów państwa strefy Schengen;
2. Kopie pełnomocnictwa do reprezentowania wnioskodawcy;
3. Inne.

Wnioskodawca/Pełnomocnik

(Podpis)