SYSTEM INFORMACYJNY SCHENGEN

PRZEWODNIK „KORZYSTANIE Z PRAWA DOSTĘPU”

Przewodnik został skompilowany przez

Wspólny Organ Nadzorczy

Schengen

Adres: Data Protection Secretariat
Council of the European Union
175, Rue de la Loi (00FL59)
B-1048 BRUSSELS
Tel.:+32(0)22818996

SPIS TREŚCI

67

Przewodnik opisuje, jak korzystać z prawa dostępu do systemu informacyjnego Schengen (SIS).

Pierwotnie miał być przeznaczony dla osób, których dotyczą dane przechowywane w SIS, jako pomoc w korzystaniu z prawa dostępu. Może być jednak źródłem praktycznych informacji także dla wszystkich, którzy ze względów zawodowych zainteresowani są prawem dostępu (organy ochrony danych, służby policji, wydziały ds. cudzoziemców, prawnicy itd.).
Na przewodnik składają się trzy części: przegląd zasad ogólnych i najważniejszych definicji związanych z SIS, opis postępowania względem prawa dostępu w każdym z odnośnych państw oraz opis niektórych sytuacji szczególnych wymagających specjalnego postępowania.

I. PRZEGLĄD ZASAD OGÓLNYCH

I.A System informacyjny Schengen (SIS)

Układ schengeński z dnia 14 czerwca 1985 r. oraz odnośna konwencja wykonawcza z dnia 19 czerwca 1990 r. zlikwidowały odprawy na granicach wewnętrznych między państwami członkowskimi i wprowadziły zasadę dokonywania kontroli na granicy całej strefy Schengen. Dzięki temu powstał obszar, po którym osoby fizyczne mogą się swobodnie przemieszać.
Aby utrzymać zadowalający poziom bezpieczeństwa, postanowiono oprócz stosowania innych środków (zacieśnienie współpracy organów policji i współpracy organów wymiaru sprawiedliwości, harmonizacja polityki wizowej i azylowej) utworzyć system informacyjny Schengen (SIS).

Zawarte w systemie dane są dostępne dla wszystkich państw członkowskich należących do strefy Schengen. Jest on scentralizowaną bazą z informacjami należącymi do dwóch kategorii: po pierwsze – z danymi osób poszukiwanych, zaginionych lub obserwowanych, a po drugie – z danymi skradzionych lub zagubionych pojazdów i przedmiotów, zwłaszcza np. dowodów tożsamości, dowodów rejestracyjnych czy tablic rejestracyjnych pojazdu.

Oto co przykładowo można znaleźć w SIS:

- informacje o osobach poszukiwanych lub obserwowanych przez policję
- informacje o osobach zaginionych lub wymagających ochrony, zwłaszcza o nieletnich
- informacje o osobach, które nie są obywatelami państwa strefy Schengen i podlegają zakazowi wjazdu do niej.

Wykonanie czynności żądanej we wpisie zależy od prawa państwa strefy Schengen, które tę czynność wykonuje. Jeżeli prawo krajowe zakazuje odnośnej czynności, dane państwo strefy Schengen musi natychmiast poinformować o tym państwo, które dokonało wpisu.

Zgodnie z zasadami ochrony danych konwencja schengeńska przyznaje konkretne prawa wszystkim osobom fizycznym.
Zasadniczo chodzi o:

- prawo dostępu do własnych danych przechowywanych w SIS
- prawo do zażądania sprostowania, jeżeli dane są nieścisłe, lub usunięcia, jeżeli dane są przechowywane wbrew prawu
- prawo, by wystąpić do krajowych organów ochrony danych o skontrolowanie indywidualnych danych zawartych w SIS i sposobu, w jaki te dane są wykorzystywane
- prawo, by wszcząć przed sądem lub właściwym organem postępowanie skutkujące sprostowaniem lub usunięciem nieścisłych danych albo wypłatą odszkodowania.

I.B Prawo dostępu

Prawo dostępu oznacza, że każdy zainteresowany może zgodnie z prawem krajowym uzyskać wgląd do informacji o sobie przechowywanych w zbiorze danych. Jest to fundamentalna zasada ochrony danych pozwalająca osobom, których dotyczą dane, sprawować kontrolę nad swoimi danymi osobowymi przechowywanymi przez strony trzecie.

Prawo to jest jednoznacznie przewidziane w konwencji schengeńskiej z dnia 19 czerwca 1990 r. W myśl art. 109 konwencji każdy ma prawo dostępu do swoich danych wprowadzonych do systemu informacyjnego Schengen. Prawu temu towarzyszy prawo do zażądania sprostowania, jeżeli dane są nieścisłe, lub usunięcia, jeżeli dane są przechowywane wbrew prawu (art. 110).
Dostępu odmawia się, jeżeli przyznanie go może utrudnić wykonanie legalnej czynności wskazanej we wpisie lub jeżeli jest to konieczne do ochrony praw i swobód osób trzecich. Dostępu odmawia się zawsze w okresie ważności wpisu, który zawiera żądanie prowadzenia niejawnej obserwacji (art. 109 ust. 2 konwencji).

Kto pragnie skorzystać z prawa dostępu, może się zwrócić do właściwych organów w dowolnym państwie schengeńskim[1]. Dowolność ta jest możliwa, gdyż wszystkie krajowe bazy danych (N.SIS) są takie same jak system centralny (C.SIS) w Strasburgu (zob. art. 92 ust. 2 konwencji). Zatem prawo dostępu dotyczy zawsze tych samych danych, bez względu na to, do którego państwa się występuje.

Jednak od przepisów państwa, do którego się występuje, zależy sposób wykonywania tego prawa. Otóż państwa różnią się pod względem trybu postępowania: istnieją dwa systemy rządzące prawem dostępu do policyjnych zbiorów danych, a zatem i do SIS. W niektórych państwach istnieje prawo do dostępu bezpośredniego, w innych – dostęp jest pośredni.

Informacje o zasadach rządzących prawem do dostępu i do żądania sprostowania zainteresowani mogą otrzymać od krajowego organu ochrony danych w danym państwie schengeńskim.

I.B.1 Prawo do dostępu bezpośredniego

W tym przypadku zainteresowany zwraca się bezpośrednio do organów operujących jego danymi (policji, żandarmerii, służb celnych itp.). Jeżeli zezwala na to prawo krajowe, zainteresowanemu można przesłać informacje go dotyczące.

[1] Belgia, Czechy, Węgry, Malta, Litwa, Łotwa, Holandia, Luksemburg, Francja, Niemcy, Włochy, Portugalia, Hiszpania, Austria, Grecja, Dania, Słowenia, Słowacja, Polska, Szwecja, Szwajcaria, Finlandia, Norwegia i Islandia (stan na październik 2009 r.).

I.B.2 Prawo do dostępu pośredniego

W tym przypadku zainteresowany dostępem zwraca się do krajowego organu ochrony danych w państwie swojego wyboru. Dane zawarte w SIS są weryfikowane przez ten organ tak samo, jakby chodziło o policyjne zbiory danych dotyczące bezpieczeństwa narodowego, obrony narodowej lub bezpieczeństwa publicznego.

Tryb ujawniania danych jest różny w poszczególnych państwach (zob. dalej) i w niektórych przypadkach może być bardzo rygorystyczny.

I.C Zasada prostowania względnie usuwania danych

W myśl konwencji schengeńskiej jedynie państwo dokonujące danego wpisu w SIS może ten wpis zmodyfikować lub usunąć (art. 106).

Jeżeli wniosek o dostęp do wpisu zostaje skierowany do państwa, które tego wpisu nie dokonało, a w którym obowiązuje prawo do dostępu bezpośredniego, musi ono umożliwić państwu, które wpisu dokonało, zajęcie stanowiska co do ewentualnego ujawnienia danych zainteresowanemu.
W przypadku państwa, w którym obowiązuje prawo do dostępu pośredniego, krajowe organy ochrony danych w obu państwach muszą ściśle współpracować w myśl art. 114 ust. 2 konwencji schengeńskiej (zob. dalej).

II. OPIS POSTĘPOWANIA WZGLĘDEM PRAWA DOSTĘPU W KAŻDYM PAŃSTWIE STREFY SCHENGEN

Procedury, które panują w poszczególnych państwach stosujących prawny dorobek Schengen i obowiązują osoby pragnące skorzystać z prawa dostępu, przedstawiono w krajowych zestawieniach informacyjnych w rozdziale IV–XXVII.

Sytuacje szczególne wymagające określonego postępowania:

III.A WSPÓŁPRACA MIĘDZY KRAJOWYMI ORGANAMI OCHRONY DANYCH

Jeżeli zainteresowany dostępem do swoich danych zwraca się o to do krajowego organu ochrony danych w jednym z państw członkowskich strefy Schengen, a po sprawdzeniu okazuje się, że dane zostały wprowadzone do systemu przez inne państwo schengeńskie, wtedy organy nadzorcze obu tych państw (tzn. państwa, do którego zwrócił się zainteresowany, i państwa, które dokonało wpisu) nawiązują ścisłą współpracę.

Z uwagi na dużą liczbę wniosków o dostęp angażujących co najmniej dwa państwa oraz na ewentualny wpływ wpisu SIS na swobody obywatelskie (zwłaszcza na swobodę przemieszczania się) sprawna i szybka współpraca organów nadzorczych ma zasadnicze znaczenie. Należy przestrzegać następujących zasad (z odpowiednim uwzględnieniem prawa krajowego):

– Krajowy organ nadzorczy, który otrzymał wniosek o dostęp, musi (jeżeli odnośne dane osobowe wprowadziło do SIS inne państwo) działać w ścisłej współpracy z krajowym organem nadzorczym państwa, które dokonało wpisu.
  Wniosek o współpracę pod żadnym pozorem nie zwalnia z odpowiedzialności organu nadzorczego, do którego zwrócił się zainteresowany dostępem.

– Organ nadzorczy, do którego zwrócił się zainteresowany dostępem, musi dostarczyć organowi, do którego sam wystąpił o współpracę, wszelkie posiadane informacje mogące się przydać do kontroli. Krajowy organ nadzorczy poproszony o współpracę musi przeprowadzić żądane kontrole z należytą dbałością.

W szczególności organ nadzorczy musi skontrolować, czy wpis w SIS jest uzasadniony, co czasami wymaga zweryfikowania również danych przechowywanych w zbiorach krajowych.

– Wnioski takie należy traktować priorytetowo, tak by zainteresowany otrzymał odpowiedź bez nadmiernej zwłoki.

Jeżeli przepisy krajowe dają zainteresowanemu prawo do dostępu bezpośredniego i pozwalają mu skontaktować się z organami operującymi krajowymi zbiorami danych, należy zainteresowanego niezwłocznie poinformować o takiej możliwości.

– Po przeprowadzeniu wszystkich kontroli organ nadzorczy poproszony o współpracę przesyła organowi nadzorczemu, do którego zwrócił się zainteresowany dostępem, wszelkie informacje zgromadzone podczas czynności kontrolnych i przedstawia swoją opinię. W opinii tej wyjaśnia, jak prawo dostępu jest ujmowane w jego przepisach krajowych. Może zaznaczyć, jaka decyzja w sprawie dostępu zapadłaby na mocy jego przepisów krajowych. Jeżeli w jego państwie obowiązuje dostęp bezpośredni (a organ występujący o współpracę stosuje dostęp pośredni), musi określić, czy zgadza się na ujawnienie informacji zainteresowanemu.

III.B Rejestracja pseudonimów

Często wpis w SIS dotyczy osób, które padły ofiarą kradzieży tożsamości (np. ich dokumenty tożsamości zostały skradzione i są wykorzystywane przez osobę trzecią). Poszukiwany zostaje zarejestrowany pod wszelkimi tożsamościami, którymi może się posługiwać.

Wpisy w SIS dotyczące osób, które padły ofiarą kradzieży tożsamości, przysparzają poważnych problemów prawnych i praktycznych.

Otóż SIS zawiera w takim przypadku wpis o tożsamości, która ani w świetle prawa, ani w świetle stanu faktycznego nie odpowiada osobie spełniającej kryteria podane w art. 95–100 konwencji schengeńskiej. Wpisy takie naruszają zasadę, że wolno przechowywać tylko dane faktycznie konieczne i ścisłe, która to zasada jest istotnym elementem ochrony danych.

Ponadto, jak wynika z doświadczenia krajowych organów nadzorczych, osoby, które padły ofiarą kradzieży tożsamości, mogą się znaleźć w skrajnie niekorzystnej sytuacji i mieć olbrzymie trudności w korzystaniu ze swoich praw.

Abstrahując od ostatecznie planowanych rozwiązań technicznych, zwracamy uwagę, że przetwarzając wnioski zainteresowanych dostępem, którzy padli ofiarą kradzieży tożsamości, należy przestrzegać następujących zasad:

– Państwa wspólnie korzystające z SIS mają obowiązek zagwarantować, że wprowadzane do niego dane są ścisłe i aktualne, dlatego przechowywanie wpisów o osobach, które padły ofiarą kradzieży tożsamości, jest dopuszczalne tylko w bardzo niewielu przypadkach (tzn. tylko wtedy, gdy w świetle warunków określonych w art. 95–100 sprawa jest na tyle poważna, by uzasadniać przetwarzanie takich danych).

  Prawa osoby, która padła ofiarą kradzieży tożsamości (a zwłaszcza jej prawo do wystąpienia o usunięcie niekorzystnego dla niej wpisu), należy wtedy rozpatrywać w świetle ryzyka powodowanego usunięciem wpisu.

– Jeżeli ofiara kradzieży tożsamości zechce skorzystać z prawa dostępu do swoich danych, państwo, które dokonało wpisu, powinno w większości przypadków maksymalnie szybko przychylić się do wniosku o jego usunięcie, zwłaszcza gdy wpis miał za podstawę art. 96, a nie np. art. 95.
– I wreszcie, jak się czasem zdarza, osoba o tożsamości figurującej w SIS jako „ustalona tożsamość" (*established identity*) twierdzi, że jej imię i nazwisko zostały skradzione do niegodziwych celów. Ta niezręczna sytuacja może się zrodzić wtedy, gdy zatrzymany sprawca czynu karalnego jako własne podał dane osoby, której tożsamość skradł. Zdaniem Wspólnego Organu Nadzorczego Schengen osoba, która w takich przypadkach uważa się za ofiarę kradzieży tożsamości, musi mieć możliwość wykazania wszelkimi możliwymi środkami, że nie popełniła zarzucanego jej czynu, oraz możliwość dochodzenia swoich praw.

III.C Wpis dotyczący obcokrajowca, który posiada dokument pobytowy wydany przez państwo członkowskie

W takich przypadkach art. 25 ust. 2 konwencji schengeńskiej przewiduje następującą procedurę:
„Jeśli okaże się, że wpis do celów odmowy wjazdu został dokonany wobec cudzoziemca legitymującego się ważnym dokumentem pobytowym wydanym przez jedną z Umawiających się Stron, Umawiająca się Strona dokonująca wpisu zasięga opinii Strony, która wydała dokument pobytowy, w celu stwierdzenia, czy istnieją wystarczające przesłanki do cofnięcia dokumentu pobytowego.
Jeżeli nie dochodzi do cofnięcia dokumentu pobytowego, Umawiająca się Strona dokonująca wpisu wycofa go, lecz niezależnie od tego może wprowadzić danego cudzoziemca na krajową listę wpisów do celów odmowy wjazdu".

Może się zdarzyć, że na temat danego cudzoziemca państwo członkowskie dokonało w strefie Schengen wpisu do SIS na podstawie art. 96 konwencji schengeńskiej, choć cudzoziemcowi temu przysługuje legalny pobyt w innym państwie członkowskim.
Sytuacja taka wydaje się przeczyć logice, gdyż osoba mająca prawo pobytu na terytorium jednego państwa członkowskiego strefy Schengen nie powinna równocześnie figurować w SIS jako „cudzoziemiec niepożądany" w strefie Schengen.

W takim przypadku, jeżeli organ ochrony danych stwierdzi, że osoba pragnąca skorzystać z prawa dostępu do SIS jest w opisanej właśnie sytuacji, organ ten powinien sprawdzić, czy dopełniono procedury określonej w art. 25 ust. 2 konwencji schengeńskiej, która to procedura zazwyczaj prowadzi do usunięcia wpisu o danej osobie. Jeżeli według państwa, które wydało dokument pobytowy, nie ma przesłanek do jego cofnięcia, wpis powinien zostać automatycznie usunięty z SIS. W tej materii konwencja nie daje państwu, które dokonało wpisu, żadnej swobody.

Zbadawszy tę kwestię, wspólny organ nadzorczy stwierdził, że procedura ta nie jest konsekwentnie stosowana i że dla zainteresowanego może okazać się niezmiernie długa. Ponadto, jak wynika z tej analizy, państwa członkowskie są przekonane, że jednak mają swobodę decydowania, czy konieczne jest usunięcie wpisu w świetle art. 25 ust. 2 konwencji schengeńskiej.

W związku z tym organy ochrony danych powinny postępować według następujących zasad:

- sprawdzić, czy osoba określona we wpisie do SIS posiada ważny dokument pobytowy wydany przez państwo członkowskie strefy Schengen
- jeżeli tak, przypomnieć odnośnym organom, że usunięcie wpisu ma następować automatycznie (pomijając sytuacje wyjątkowe), oraz nalegać na szybkie usunięcie danych z SIS.

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 się też do informacji zawartych w SIS we wpisach dokonanych na podstawie art. 95–100 konwencji schengeńskiej.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wniosek o informacje zainteresowany powinien kierować do organu policji (jako zleceniodawcy), od którego pragnie się 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 zgodą zleceniodawcy – ustnym) żądaniem oraz

– jeżeli zainteresowany w odpowiedniej formie potwierdzi swoją tożsamość (np. kopią 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 się:

- jeżeli ze szczególnych powodów wymaga tego ochrona samego zainteresowanego
- jeżeli przeszkodą jest wyższej wagi uzasadniony interes zleceniodawcy lub osoby trzeciej
- jeżeli przeszkodą 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 się 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 się żadnych danych zainteresowanego objętych obowiązkiem udzielenia informacji (pkt 5).
Odmowy udzielenia informacji podlegają kontroli ze strony komisji ochrony danych (*Datenschutzkommission*) 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 całkowitą 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 ryczałtową opłatę w wysokości 18,89 EUR, która może się zmienić w razie faktycznie większych kosztów. Pobraną opłatę należy zwrócić, jeżeli w wyniku udzielenia informacji doszło do sprostowania danych.

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

Datenschutzkommission [*komisja ochrony danych*]

Hohenstaufengasse 3
A - 1010 Vienna
Tel.: +43 1 531 15/2525
Faks: +43 1 531 15/2690
E-mail: dsk@dsk.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 się żadnych jego danych objętych obowiązkiem udzielenia informacji, może odwołać się do komisji ochrony danych zgodnie z §31 pkt 1 i 4 ustawy o ochronie danych z roku 2000.

Jeżeli w postępowaniu odwoławczym toczącym się w myśl §31 pkt 4 ww. ustawy zleceniodawca powoła się na konieczność zachowania tajemnicy z uwagi na wyższej wagi interes publiczny, komisja 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 się do Naczelnego Sądu Administracyjnego (*Verwaltungsgerichtshof*). Jeżeli tego nie robi, musi w terminie 8 tygodni wypełnić decyzję komisji ochrony danych, inaczej komisja sama udzieli zainteresowanemu żądanych informacji.

5. Najważniejsze odnośne 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 zgodą 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 odnośne podstawy prawne. Na żądanie zainteresowanego należy także podać nazwy i adresy podmiotów wykonujących usługę przetwarzania danych. Za zgodą zainteresowanego można udzielić informacji nie na piśmie, ale ustnie, zapewniając jednak możliwość wglądu, wykonania odpisu lub kserokopii.

(2) Informacji nie udziela się, jeżeli ze szczególnych powodów wymaga tego ochrona samego zainteresowanego lub jeżeli przeszkodą 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 operacyjną 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, uniemożliwiać lub ścigać czyny zabronione.

Słuszność odmowy udzielenia informacji z powyższych powodów podlega kontroli ze strony komisji ochrony danych na mocy §30 pkt 3 i może być kwestionowana przed tą komisją 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 całkowitą 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 ppkt 1–5, należy – o ile jest to konieczne do ochrony wspomnianego interesu publicznego, który nakazuje odmówić udzielenia informacji – postępować następująco: ilekroć odmawia się udzielenia jakichkolwiek informacji – także z tego powodu, że w rzeczywistości żadne dane nie są wykorzystywane – należy zamiast podawać merytoryczne uzasadnienie, stwierdzić, że nie wykorzystuje się żadnych danych zainteresowanego objętych obowiązkiem udzielenia informacji. Słuszność takiego postępowania podlega kontroli ze strony komisji ochrony danych na mocy §30 pkt 3 i może być kwestionowana przed tą komisją 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 ryczałtową opłatę w wysokości 18,89 EUR, która może się 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 się o żądaniu udzielenia informacji, nie wolno mu przez 4 miesiące niszczyć danych dotyczących zainteresowanego, a jeżeli następuje odwołanie do komisji ochrony danych w myśl §31 – nie wolno ich niszczyć, dopóki postępowanie się nie zakończy.

(8) Jeżeli z mocy przepisów zbiory danych są dostępne do publicznego wglądu, zainteresowani mają 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 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

Commission de la protection de la vie privée [*komisja ochrony prywatności – jęz. fr.*]
Rue Haute 139>
1000 Bruxelles

Commissie voor de bescherming van de persoonlijke levensfeer [*komisja ochrony prywatności – jęz. niderl.*]
Hoogstraat 139
1000 Brussel
Tel.: +32 2 213 85 40
Faks: +32 2 213 85 65
Strona: http://www.privacycommission.be
E-mail: info@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 kserokopię jego dowodu osobistego.

Należy podać (jeżeli znane) nazwę odnośnego 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 odnośne przepisy krajowe

– ustawa z dnia 8 grudnia 1992 r. o ochronie prywatności w przetwarzaniu danych osobowych, zmieniona ustawą 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. wdrażający ustawę z dnia 8 grudnia 1992 r. o ochronie prywatności w przetwarzaniu danych osobowych, zwłaszcza jej art. 36–46.

VI. 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 Policją 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 usunięcie danych (w tym odnośne 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 poświęconych 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 swoją 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 [*urząd ochrony danych osobowych*]

Pplk. Sochora 27

170 00 Praha 7

Czech Republic

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 się 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 odnośne 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 się po angielsku. Także po angielsku są podane na jego stronach podstawowe informacje o trybie występowania o dostęp.

VII. 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 państwowa*]
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 się jej spodziewać.

Zasadniczo, jeżeli zażąda tego zainteresowany, odpowiedzi są udzielane na piśmie. Jeżeli zainteresowany stawi się 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 decyzję policji w sprawie dostępu. Rozpatrując je, urząd analizuje sprawę i sprawdza, czy żadnych danych nie wprowadzono do systemu wbrew postanowieniom konwencji schengeńskiej.

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 sekcją 30 (2) ustawy obowiązek ten nie ma zastosowania, jeżeli stwierdzi się, 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) ……..

Zgodnie z art. 95 oraz art. 98–100 konwencji schengeńskiej informacje wprowadza się do SIS, by umożliwić: aresztowanie poszukiwanych osób, stawiennictwo wezwanych osób, dostarczenie wyroku lub wezwania, obserwację niejawną lub określone kontrole osób lub pojazdów, zlokalizowanie przedmiotów podlegających konfiskacie lub mogących posłużyć jako dowód w postępowaniu karnym.

Z uwagi na te cele może się zdarzyć, że zainteresowanemu nie będzie można udzielić odpowiedzi, czy jego dane, o których mowa w art. 95 oraz 98–100 konwencji, figurują w SIS. W przeciwnym przypadku zainteresowany mógłby podjąć działania, które narażą na niepowodzenie czynności żądne we wpisie (zob. także art. 109 ust. 2 konwencji schengeńskiej).

6. Najważniejsze odnośne przepisy krajowe

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

VIII. 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 się 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
Internet: 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 się 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 się odwołać do właściwego sądu administracyjnego, a dalej do Naczelnego Sądu Administracyjnego (sekcja 28 i 29 ustawy o danych osobowych).

5. Najważniejsze odnośne przepisy krajowe

Ustawa o ochronie danych (523/1999)
Ustawa o ochronie danych policyjnych (761/2003).

IX. FRANCJA

1. Charakter gwarantowanego dostępu

Dostęp ma charakter mieszany.

Dostęp jest bezpośredni, jeżeli osoba figurująca w SIS to:

- osoba poszukiwana z powodów rodzinnych (art. 97 konwencji)
- nieletni mający zakaz opuszczania kraju (art. 97)
- zbiegły nieletni (art. 97)
- osoba, o której jest mowa we wpisie dotyczącym skradzionego pojazdu lub którą można na podstawie tego wpisu zidentyfikować (art. 100)

We wszystkich pozostałych przypadkach dostęp do danych w SIS jest pośredni. Zgodnie z art. 39 ustawy z dnia 6 stycznia 1978 r. o przetwarzaniu danych, zbiorach danych i wolnościach Krajowa Komisja Przetwarzania Danych i Wolności zleca jednemu ze swych członków – sędziemu lub byłemu sędziemu Rady Stanu, Sądu Kasacyjnego lub Sądu Obrachunkowego – przeprowadzenie koniecznego dochodzenia i nakazanie odpowiednich zmian.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski w wymienionych czterech 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 muszą 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 czytelną kserokopię dokumentu tożsamości. Dołączyć należy też kopie wszelkich odnośnych dokumentów (zawiadomienie o odmowie wydania wizy na podstawie wpisu do SIS, korzystna dla zainteresowanego decyzja sądowa uchylająca 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 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

5. Wymagany język

Zainteresowany składa wniosek w języku francuskim.

X. NIEMCY

1. Charakter gwarantowanego dostępu

W Niemczech obowiązuje dostęp bezpośredni. Można z niego skorzystać bezpośrednio po zwróceniu się 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 urząd śledczy*]
– 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 informację organowi odpowiadającemu za rejestrację danych (np. *Bundeskriminalamt*) lub na żądanie wszczyna inspekcję tego organu pod kątem ochrony danych. Adres urzędu jest następujący:

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [*federalny inspektor ochrony danych i wolności 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. 96 konwencji schengeńskiej, informacje z reguły się ujawnia.

Jeżeli wniosek dotyczy wpisu dokonanego na podstawie art. 95 lub 99 konwencji schengeńskiej, udzielenia informacji można odmówić, gdy zachodzi przynajmniej jedna z przesłanek generalnie uzasadniających taką 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. 95 konwencji schengeńskiej, należy uwzględnić stanowisko tego organu zgodnie z art. 109 ust. 1 zdanie trzecie. 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 odnośne przepisy krajowe

Najważniejsze obowiązujące przepisy krajowe to art. 109 konwencji schengeńskiej 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.

XI. 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 się, by zwrócił się 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, pełną 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 i grecki urząd ochrony danych zastanawia się nad jej formalnym zniesieniem.

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
Internet: www.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. 96 konwencji schengeńskiej, zainteresowany otrzyma informacje o dotyczących go danych.

Jeżeli wpis ma za podstawę art. 95 konwencji schengeńskiej, 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. 95 konwencji schengeńskiej dokonał zagraniczny organ, jego stanowisko będzie uwzględnione podczas podejmowania decyzji o ewentualnym ujawnieniu danych zainteresowanemu.

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

6. Najważniejsze odnośne przepisy krajowe

Zastosowanie mają: art. 109 konwencji schengeńskiej 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.

XII. 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

The Office of the Parliamentary Commissioner for Data Protection [*urząd parlamentarnego inspektora ochrony danych*]
H-1051 Budapest, Nádor u. 22.
Tel.: +36 1 475 7100
E-mail: privacy@obh.hu

Wnioski o dostęp można składać osobiście w każdej placówce policji na terytorium Węgier oraz w każdej placówce dyplomatycznej Republiki Węgierskiej. 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 się 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

Inspektor ochrony danych jest upoważniony do odpowiadania na otrzymane wnioski. Odpowiedzi udziela po sprawdzeniu odpowiednich wpisów w systemie informacyjnym Schengen. Ponadto zainteresowany może się do niego zwrócić, jeżeli ma wątpliwości co do odpowiedzi otrzymanej z biura SIRENE lub jeżeli nie otrzymał on stamtąd żadnej odpowiedzi.

5. Najważniejsze odnośne przepisy krajowe

Ustawa LXIII z roku 1992 o ochronie danych osobowych i publicznym dostępie do danych wagi społecznej
Ustawa CV z roku 2007 o współpracy i wymianie informacji w ramach konwencji wykonawczej do układu z Schengen.

XIII. ISLANDIA

1. Charakter gwarantowanego dostępu

Obowiązuje bezpośredni dostęp do informacji.

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski należy kierować do islandzkiego biura SIRENE, prowadzonego przez Komendanta Islandzkiej Policji Państwowej:
Jego adres jest następujący:

Ríkislögreglustjóri
Skúlagata 21
IS - 150 Reykjavik
Tel.: ++354 444 2500
Faks: ++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. Decyzję 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 którą 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.

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 się 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*:]
Dómsmála- og mannréttindaráduneytid
Skuggasund
IS - 150 Reykjavík
Tel.: ++354 545 9000.
Faks: ++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
Faks: ++354 510.9606
E-mail: postur@personuvernd.is
Internet: www.personuvernd.is

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 informację o celu i powodach wpisu. Zainteresowany nie ma prawa zapoznać się z przechowywanymi danymi, jeżeli należy je zachować w tajemnicy, po to by mógł się zrealizować zamysł organu dokonującego wpisu do systemu informacyjnego lub by chronić interes osób trzecich, lub by nie udaremniać trwającej obserwacji niejawnej. Zainteresowany otrzymuje wtedy taką samą standardową odpowiedź, jak osoba niefigurująca w systemie: „Brak informacji w systemie/Zakaz ujawniania przechowywanych informacji".

6. Najważniejsze odnośne przepisy krajowe

Najważniejsze odnośne 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 odpowiedź w języku dla niej zrozumiałym.

XIV. WŁOCHY

1. Charakter gwarantowanego dostępu

Można korzystać tylko z dostępu bezpośredniego, zwracając się 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 weryfikację 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

Jeżeli uzyskana odpowiedź 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 pocztą niż faksem. Należy w nich podać odpowiednie dane teleadresowe zainteresowanego – w miarę możliwości jego adres – by ułatwić korespondencję.

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

Składanie wniosku (pocztą lub faksem) nie wiąże się 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 przyspieszyć rozpatrywanie skargi, zainteresowany powinien ją sporządzić po włosku, angielsku, francusku lub niemiecku, **podpisać**, wskazać w skrócie powody jej złożenia oraz dołączyć do niej **kserokopię swojego ważnego dowodu osobistego**.

4. Oczekiwany skutek. Treść podawanych informacji

5. Najważniejsze odnośne przepisy krajowe

Najważniejsze odnośne przepisy krajowe to:

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

b) dekret legislacyjny nr 196 z roku 2003.

XV. 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 się z odmową lub pozostał bez odpowiedzi, może odwołać się do Państwowego Inspektoratu Danych, który jest też właściwym organem nadzorującym realizację 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*]
Čiekurkalna 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 datą i podpisem należy składać osobiście lub elektronicznie w biurze Policji Państwowej lub w łotewskiej placówce dyplomatycznej bądź konsularnej. Składając wniosek osobiście, zainteresowany musi potwierdzić swoją 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 pocztą – 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 odnośne przepisy krajowe

– ustawa o ochronie danych osobowych

– ustawa o eksploatowaniu systemu informacyjnego Schengen

– rozporządzenia 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 ustawą 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.

XVI. 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 ustawą z dnia 31 lipca 2006 r., ustawą z dnia 22 grudnia 2006 r. i ustawą 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 odpowiednią weryfikację 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 się żadnych informacji o treści danych zainteresowanego.

5. Najważniejsze odnośne 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.

XVII. LITWA

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

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

2. Dane teleadresowe organu, do którego należy kierować wniosek

Wnioski o dostęp, sprostowanie lub usunięcie 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
Tel.: +370 5 271 7130, faks: +370 5 271 8551
E-mail: korespondencija@vrm.lt

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

Wniosek musi mieć formę pisemną i nosić 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 się ujawnia lub ujawniono.

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.

Jeżeli zapoznawszy się ze swoimi danymi osobowymi, zainteresowany stwierdzi, że są one nieprawdziwe, niekompletne lub nieścisłe lub że są przetwarzane nielegalnie lub niesprawiedliwie, i zwróci się 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.

W myśl art. 17 ust. 2 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 się 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 się mu również w okresie ważności wpisu dotyczącego obserwacji niejawnej.
Odmowę przychylenia się 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.

Artykuł 109 ust. 1 konwencji schengeńskiej z dnia 19 czerwca 1990 r. przewiduje, że prawo osób do dostępu do swoich danych wprowadzonych do systemu informacyjnego Schengen wykonywane jest zgodnie z przepisami umawiającej się strony, wobec której osoby te powołują się na to prawo. Jeśli przepisy krajowe tak stanowią, krajowy organ nadzorczy określony w art. 114 ust. 1 decyduje, czy informacje mają być przekazane oraz zgodnie z jakimi procedurami. Umawiająca się strona, która nie wprowadziła danego wpisu, może przekazać informację dotyczącą takich danych tylko wtedy, gdy uprzednio dała umawiającej się stronie wprowadzającej wpis możliwość wyrażenia swojego stanowiska.

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 zgodą 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 się strony i poinformować o tym zainteresowanego. Gdy właściwa instytucja umawiającej się 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 [*państwowy inspektorat ochrony danych*]
A.Juozapavičiaus str. 6 / Slucko str. 2, LT-09310 Vilnius
Lithuania
Tel.: +370 5 279 1445, faks: +370 5 261 9494
E-mail: ada@ada.lt
Internet: www.ada.lt

Jeżeli odpowiedź administratora danych nie satysfakcjonuje zainteresowanego (gdy administrator nie przychylił się 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 którą wygasł termin na odpowiedź. Na poparcie faktów przytoczonych w skardze zainteresowany może załączyć ewentualne dokumenty (odpowiedź 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 decyzję w sprawie faktów opisanych w skardze.

6. Najważniejsze odnośne 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. System językowy

Wnioski o dostęp, sprostowanie lub usunięcie należy składać w języku państwowym (litewskim). Wnioski otrzymane w jakimkolwiek innym języku zostaną rozpatrzone zgodnie z procedurą ogólną. Wnioski w języku innym niż język państwowy muszą zostać przetłumaczone na litewski. Odpowiedź zostanie zainteresowanemu udzielona w języku państwowym (litewskim).

Językiem postępowania odwoławczego jest litewski. Skarga złożona w Państwowym Inspektoracie Ochrony Danych w języku innym niż język państwowy musi zostać przetłumaczona na litewski. Decyzja w sprawie skargi zostanie przyjęta, a odpowiedź na skargę udzielona w języku państwowym (litewskim).

XVIII. MALTA

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

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

2. Dane teleadresowe organu, do którego należy kierować wniosek

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

Data Protection Officer Insp. [*inspektor ochrony danych*] Sandro Camilleri
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. Odpowiedź powinna nastąpić w tym samym języku, którym posłużył się zainteresowany we wniosku. Informacji należy udzielić bezpłatnie i bez zbytniej zwłoki.

4. Procedura

Konwencja schengeńska przewiduje, 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). Odpowiedź 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, faks: +35623287198
E-mail: commissioner.dataprotection@gov.mt
Internet: www.dataprotection.gov.mt

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

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

6. Odnośne przepisy krajowe

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

XIX. 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 policję

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 się z zainteresowanym, żeby ustalić kwestie związane z rozpatrywaniem wniosku. Zainteresowany musi dostarczyć kopię dowodu osobistego. Za rozpatrzenie wniosku może zostać pobrana opłata w wysokości 4,50 EUR. Rozpatrując wniosek, ustala się, czy można się do niego przychylić, czy też zachodzą przesłanki uzasadniające odmowę.

Wniosek dotyczący wpisu dokonanego na podstawie art. 96 jest przekazywany 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 usunięcie danych.

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

W razie sporu dotyczącego rozpatrzenia wniosku można wystąpić o mediację 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. Do komisji tej można też wystąpić o sprawdzenie, czy dane zostały zamieszczone w systemie informacyjnym Schengen zgodnie z konwencją schengeńską i przepisami prawa.
Zamiast tego – lub jeżeli mediacja nie przyniosła skutku – można odwołać się do sądu okręgowego (wydział administracyjny), by rozpatrzył sprawę i dokonał stosownego rozstrzygnięcia.

XX. 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:
Faks: + +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 rejestrację danych. Jeżeli wniosek został od razu skierowany do organu, który zlecił rejestrację danych, organ ten przekazuje go administratorowi danych wraz ze swoją opinią.

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 odnośne 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).

XXI. 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 modyfikację 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 się w zbiorach danych.

W myśl art. 32 ust. 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 nr 101 poz. 926 z późniejszymi zmianami) zainteresowany może skorzystać z prawa do informacji nie częściej niż *raz na 6 miesięcy*.

Za wniosek o dostęp nie pobiera się 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 się jej dane
- z jakiego źródła dane te pochodzą
- w jaki sposób się je udostępnia
- w jakim celu i zakresie są one przetwarzane
- w jakim zakresie i komu się 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. kserokopię dowodu tożsamości zawierającego czytelny wizerunek posiadacza
6. miejsce zamieszkania (kraj, miejscowość, ulicę 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. 2000 nr 98 poz. 1071 z późniejszymi zmianami) 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 tajemnicę 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, usunięcie 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. Kontrolę tę sprawuje zgodnie z przepisami o ochronie danych osobowych.

Adres do korespondencji:
Urząd Generalnego Inspektora Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa
Poland
Tel.: +48 (22)860 -73 -93
Faks: +48 (22)860-70-86
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 odnośne 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.

XXII. PORTUGALIA

1. Charakter gwarantowanego dostępu

Obywatele mają prawo pośredniego dostępu do danych SIS. Na straży tego prawa stoi Krajowy Urząd Ochrony Danych.

2. 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 pocztą. Aby uzyskać dostęp do swoich danych, zainteresowany musi okazać dokument potwierdzający jego tożsamość (np. paszport) lub dołączyć jego poświadczoną kopię do wysyłanego wniosku. Korzystanie z prawa dostępu jest bezpłatne.

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

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

Ujawnienie informacji zależy od tego, czy nie narazi ono na szwank prewencji kryminalnej, dochodzeń karnych albo bezpieczeństwa państwa.
Ujawnienia dokonuje Krajowy Urząd Ochrony Danych.

4. Najważniejsze odnośne 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.

XXIII. SŁOWACJA

1. Charakter gwarantowanego dostępu

W myśl art. 109 konwencji każdy ma prawo dostępu do swoich danych wprowadzonych do systemu informacyjnego Schengen. Z prawa tego korzysta się 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
wyślij e-mail
Internet: http://www.minv.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 pełną 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 się zainteresowanemu na podstawie art. 69c ustawy nr 171/1993 Zb. o siłach policji.
W przypadku systemu informacyjnego Schengen, jeżeli wpis ma za podstawę art. 95–98 oraz art. 100 konwencji schengeńskiej, 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 się 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. 99 konwencji schengeńskiej, 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 się udzielenia informacji, jeżeli jest to konieczne, by zapewnić wykonanie uprawnionej czynności żądanej we wpisie lub chronić prawa i swobody stron 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 usunięcie 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.

XXIV. 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(at)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 policję (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 informującą, 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 instrukcją 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 się 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 się z tym stanowiskiem oraz raportami, dowodami i innymi dokumentami dochodzeniowymi (w tym po zapoznaniu się w razie konieczności ze zbiorami danych oraz po rozmowie z zainteresowanym i z administratorem zbioru danych) Inspektor Informacji ostatecznie podejmuje w sprawie skargi decyzję, którą 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 (określoną 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 policję, uniemożliwianie, ujawnianie, wykrywanie, dowodzenie i ściganie przestępstw i wykroczeń, ujawnianie i karanie naruszeń norm etycznych niektórych zawodów, kwestie monetarne, budżetowe i podatkowe, nadzór nad policją 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 się je wprowadza.

6. Najważniejsze odnośne 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-osebnih-podatkov/pravilnik-o-zaracunavanju-stroskov-pri-izvrsevanju-pravice-posameznika-do-seznanitve-z-lastnimi-osebnimi-podatki/

XXV. HISZPANIA

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 do informacji należy kierować na adres:

Secretaría de Estado de Seguridad [*państwowy wydział bezpieczeństwa*]
Ministerio del Interior [*ministerstwo spraw wewnętrznych*]
Amador de los Ríos, 2
E – 28010 Madrid
Tel.: 060
Faks: ---
E-mail: estafeta@mir.es
Internet: www.mir.es

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 się do administratora danych dowolną drogą, 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 kserokopię dokumentu potwierdzającego tożsamość zainteresowanego (np. kopię dowodu osobistego lub paszportu). Ponadto zainteresowany może dołączyć kopię wszelkich dokumentów, które uzna za istotne w związku z prośbą 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
Faks: + 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 Urzędu Ochrony Danych), jeżeli nie otrzyma odpowiedzi od administratora danych na wniosek o dostęp lub jeżeli otrzymana odpowiedź jest niezadowalająca. W obu przypadkach zainteresowany może wnieść skargę do Hiszpańskiego Urzędu 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 się na wniosek zainteresowanego: musi on jasno określić przedmiot swojej skargi i wskazać przepisy wspomnianej ustawy, które jego zdaniem zostały naruszone.

Gdy Hiszpański Urząd Ochrony Danych otrzyma skargę, wszczyna postępowanie o ochronę praw osobistych. Zgodnie z procedurą 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 się zainteresowanemu, który może ponownie zająć stanowisko i zgłosić dodatkowe uwagi. Jego uwagi zostają przekazane administratorowi danych, który może ustosunkować się do swojej decyzji oraz do stanowiska i uwag zainteresowanego.

Po otrzymaniu wyjaśnień oraz innych informacji i dokumentów dyrektor Hiszpańskiego Urzędu Ochrony Danych wydaję decyzją 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 kopię 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 między organami krajowymi pod względem ochrony danych osobowych. Decyzję o tym, jakie dane można ujawnić zainteresowanemu, podejmują wtedy organy tego innego państwa strefy Schengen.

6. System językowy

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

XXVI. 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 odpowiedź 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 [*inspekcja 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

Inspekcja Danych kontroluje, czy dane w Szwecji przetwarza się zgodnie z przepisami ustawy o danych osobowych i innych aktów o ochronie danych. Może wszcząć kontrolę 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 odnośne 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. System językowy

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

XXVII. 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 urząd 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 (tylko wnioski pisemne z dołączoną kopią ważnego dowodu osobistego lub paszportu).

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

Federal Data Protection and Information Commissioner [*federalny inspektor ochrony danych i informacji*]
Feldeggweg 1,
CH-3003 Berne
Tel.: +41(0)31 322 43 95, faks: +41-(0)31 325 99 96
www.edoeb.admin.ch

Do Federalnego Inspektora Ochrony Danych i Informacji w Szwajcarii, który na szczeblu federalnym jest krajowym organem ochrony danych, należy kierować jedynie wnioski o weryfikację.

ZAŁĄCZNIKI (WZORY WNIOSKÓW)

Załącznik 1

Wzór wniosku o dostęp do danych

Do: **nazwa i adres właściwego organu**

DD-MM-RRRR,

Miejscowość

Szanowni Państwo,

Na podstawie art. 109 konwencji schengeńskiej

ja,_____(imię, nazwisko), mający obywatelstwo _____, urodzony dnia _____ w _____, zamieszkały w _____(adres), proszę o dostęp do moich danych osobowych figurujących w systemie informacji Schengen.

Do wniosku dołączam:

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

Wnioskodawca / Pełnomocnik

(Podpis)

Załącznik 2

Wzór wniosku o sprawdzenie danych

Do: **nazwa i adres właściwego organu**

DD-MM-RRRR,

Miejscowość

Szanowni Państwo,

Na podstawie art. 114 ust. 2 konwencji schengeńskiej

ja,_____(imię, nazwisko), mający obywatelstwo _____, urodzony dnia _____ w _____, zamieszkały w _____(adres), proszę o sprawdzenie moich danych osobowych figurujących w systemie informacji Schengen oraz o sprawdzenie sposobu ich wykorzystywania.

Do wniosku dołączam:

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

Wnioskodawca / Pełnomocnik

(Podpis)

Załącznik 3

Wzór wniosku o sprostowanie danych

Do: **nazwa i adres właściwego organu**

DD-MM-RRRR,
Miejscowość

Szanowni Państwo,

Na podstawie art. 110 konwencji schengeńskiej

ja,_____(imię, nazwisko), mający obywatelstwo _____, urodzony dnia _____ w _____, zamieszkały w _____(adres), proszę o sprostowanie nieścisłości w moich danych osobowych lub usunięcie moich danych osobowych nielegalnie figurujących w systemie informacji Schengen. Moje dane osobowe wymagają sprostowania/należy usunąć, ponieważ:

_____

_____

_____

_____

Do wniosku dołączam:

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

Wnioskodawca / Pełnomocnik

(Podpis)