

GRUPUL DE SUPRAVEGHERE COMUNĂ SIS II

**SISTEMUL DE INFORMAȚII SCHENGEN**  
**GHID PENTRU EXERCITAREA DREPTULUI DE ACCES**

---

Secretariat postal address: rue Wiertz 60 - B-1047 Brussels  
Offices: rue Montoyer 30

E-mail : [EDPS-sis@edps.europa.eu](mailto:EDPS-sis@edps.europa.eu)  
Tel.: 02-283 19 13 - Fax : 02-283 19 50

**Acest ghid a fost elaborate de  
Grupul de Supraveghere Comună SIS II  
Address: rue Wiertz 60 - B-1047 Brussels  
Offices: rue Montoyer 30  
E-mail : EDPS-sis@edps.europa.eu  
Tel.: 02-283 19 13 -  
Fax : 02-283 19 50**

## CUPRINS

<b>I.</b>	Introducere Sistemul de Informații Schengen generația a IIa (SIS II) .....	5
<b>II.</b>	Drepturile persoanelor ale căror date sunt prelucrate în SIS II .....	7
<b>II.1</b>	Dreptul de acces .....	8
<b>II.1.1</b>	Acces direct .....	9
<b>II.1.2</b>	Acces indirect .....	9
<b>II.2</b>	Dreptul de intervenție și de ștergere a datelor .....	9
<b>II.3</b>	Căi de atac: dreptul de a înainta o plângere autorității pentru protecția datelor sau de a se adresa justiției .....	10
<b>III.</b>	Descrierea procedurii pentru exercitarea dreptului de acces în statul în cauză .....	10
<b>IV.</b>	AUSTRIA .....	11
<b>V.</b>	BELGIA .....	17
<b>VI.</b>	BULGARIA.....	19
<b>VII.</b>	REPUBLICA CEHĂ.....	23
<b>VIII.</b>	DANEMARCA .....	25
<b>IX.</b>	ESTONIA .....	28
<b>X.</b>	FINLANDA .....	30
<b>XI.</b>	FRANȚA .....	32
<b>XII.</b>	GERMANIA .....	35
<b>XIII.</b>	GRECIA .....	38
<b>XIV.</b>	UNGARIA .....	41
<b>XV.</b>	ISLANDA .....	43
<b>XVI.</b>	ITALIA .....	47
<b>XVII.</b>	LETONIA .....	49
<b>XVIII.</b>	LUXEMBURG .....	52
<b>XIX.</b>	LIECHTENSTEIN.....	54
<b>XX.</b>	LITUANIA .....	56
<b>XXI.</b>	MALTA .....	60
<b>XXII.</b>	OLANDA .....	62

<b>XXIII.</b>	NORVEGIA .....	65
<b>XXIV.</b>	POLONIA .....	67
<b>XXV.</b>	PORTUGALIA .....	71
<b>XXVI.</b>	ROMÂNIA .....	73
<b>XXVII.</b>	SLOVACIA.....	76
<b>XXVIII.</b>	SLOVENIA .....	79
<b>XXIX.</b>	SPANIA .....	83
<b>XXX.</b>	SUEDIA .....	87
<b>XXXI.</b>	ELVEȚIA .....	89
<b>XXXII.</b>	REGATUL UNIT.....	91
	ANEXE (Modele cereri) .....	93

Persoanele ale căror date sunt colectate, păstrare sau prelucrare în Sistemul de Informații Schengen generația a IIa (denumit în continuare SIS II) beneficiază de dreptul de acces, de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal<sup>1</sup>.

Acest Ghid descrie modalitățile de exercitare a acestor drepturi.

Ghidul este împărțit în 3 secțiuni: (I) descrierea SIS II, (II) descrierea drepturilor acordate persoanelor ale căror date sunt prelucrate în SIS II și (III) descrierea proceduri de exercitare a dreptului de acces în fiecare stat în cauză.

## **I. INTRODUCERE SISTEMUL DE INFORMAȚII SCHENGEN GENERAȚIA A IIA (SIS II)**

SIS II este un sistem IT la scară largă înființat ca o măsură compensatorie pentru eliminarea controalelor la frontierele interne și intenționează să asigure un nivel ridicat de securitate în zona de libertate, securitate și justiție a Uniunii Europene, inclusiv menținerea securității publice și ordinii publice și garantarea securității pe teritoriile statelor membre. SIS II este implementat deja în toate statele membre, cu excepția Ciprului, Croației și Irlandei<sup>2</sup>, precum și în patru state asociate: Islanda, Norvegia, Elveția și Liechtenstein.

SIS II este un sistem de informații care permite autorităților naționale de aplicare a legii, judiciare și administrative să îndeplinească atribuții specifice prin schimbul de date relevante. Agențiile Europene EUROPOL și EUROJUST au acces limitat de acest sistem.

### *Categorii de informații prelucrate*

SIS II centralizează două mari categorii de informații ce iau forma alertelor privind, în primul rând *persoane* – care sunt căutate pentru a fi arestate, au fost date dispărute, în vederea participării la o procedură judiciară, fac obiectul unor controale discrete sau specifice, fac obiectul unei semnalări ca

---

<sup>1</sup> Aceste drepturi sunt garantate în temeiul art. 41 din Regulamentul (CE) nr. 1987/2006 din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II) și art. 58 din Decizia 2007/533/JAI din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II).

<sup>2</sup> Informații din iulie 2015. Cu toate că folosesc SIS, Bulgaria și România încă dețin frontiere interne. UK are acces la SIS cu excepția alertelor pentru scopul de neadmitere pe teritoriul Schengen.

inadmisibil sau având interdicție de ședere în spațiul Schengen și, în al doilea rând, *obiecte* – precum vehicule, documente de călătorie, cărți de credit pentru a fi confiscate sau folosite ca probe în cursul procedurilor penale sau fac obiectul unor controale discrete sau specifice.

### *Temeiul legal*

În funcție de tipul de alertă, SIS II este reglementat de Regulamentul (CE) 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II) cu privire la procedurile pentru alerte ce intră sub incidența Titlului IV din Tratatul de înființare a Comunității Europene (fostul pilon I)<sup>3</sup> sau de Decizia Consiliului 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație în ceea ce privește procedurile ce intră sub incidența Titlului VI din Tratatul Uniunii Europene (fostul pilon III)<sup>4</sup>.

### *Categoriile de date personale prelucrate*

Atunci când alerta se referă la o persoană, informațiile trebuie să includă întotdeauna numele, prenumele și orice pseudonim, sexul, o trimitere la decizia privind alerta și acțiunea ce trebuie să fie luată. Dacă sunt disponibile, alerta poate conține informații precum orice caracteristici specifice, obiective, fizice ce nu pot fi schimbate; locul și data nașterii; fotografii; amprentele digitale; cetățenia (cetățeniile); dacă persoana în cauză este înarmată, violentă sau evadată; motivul alertei; autoritatea care emite alerta; legături cu alte alerte emise în SIS II în conformitate cu art. 37 din SIS II Regulamentul SIS II sau art. 52 din Decizia SIS II.

### *Arhitectura sistemului*

SIS II este compus din:

- un sistem central („SIS II Central”)
- un sistem național („N.SIS II”) în fiecare dintre Statele Membre (sistemele naționale de date care vor comunica cu SIS II Central)

---

<sup>3</sup> Denumit în continuare „Regulamentul SIS II”.

<sup>4</sup> Denumită în continuare „Decizia SIS II”.

- o infrastructură de comunicare între sistemul central și sistemele naționale care asigură o rețea virtuală criptată consacrată datelor SIS II și schimbului de date între autoritățile responsabile pentru schimbul de informații suplimentare\* (Birourile SIRENE)<sup>5</sup>.

## II. DREPTURILE PERSOANELOR ALE CĂROR DATE SUNT PRELUCRARE ÎN SIS II

În conformitate cu principiile pe protecția datelor, tuturor persoanele ale căror date sunt prelucrate în SIS II le sunt recunoscute drepturile specifice<sup>6</sup> prin Decizia SIS II și Regulamentul SIS II menționate mai sus.

Acestea sunt în principal:

- dreptul de acces la datele stocate în SIS II,
- dreptul de rectificare a datelor inexacte și ștergerea datelor stocate în mod ilegal,
- dreptul de a introduce o acțiune la instanțele judecătorești sau la autoritatea competentă pentru rectificarea sau ștergerea datelor sau pentru obținerea de compensații<sup>7</sup>.

Oricine persoană ce își exercită oricare dintre aceste drepturi se poate adresa autorităților competente din statul Schengen, la alegerea sa. Această opțiune este posibilă, deoarece toate bazele de date naționale (N.SIS II) sunt identice cu baza de date centrală (CS.SIS)<sup>8</sup>. Prin urmare aceste drepturi pot fi exercitate în orice stat Schengen indiferent de statul care a emis alerta.

Atunci când o persoană își exercită dreptul de acces, de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal, răspunsurile autorităților competente trebuie transmise într-un termen limită. Astfel, persoana este informată cât mai curând posibil și, în orice caz, într-un termen de

---

<sup>5</sup> Datele SIS II sunt introduse, actualizate, șterse și căutate prin intermediul diferitelor sisteme naționale. Sistemul central care îndeplinește funcții de control tehnic și funcții administrative este localizat în Strasbourg (Franța). Acesta oferă servicii pentru introducerea și prelucrarea datelor SIS II. Sistemul de rezervă a sistemului central, capabil să preia toate funcțiile sistemului central principal în cazul căderii acestuia, este localizat lângă Salzburg (Austria). Fiecare Stat Membru este responsabil pentru înființarea, operaționalizarea și menținerea propriei copii naționale și pentru conectarea la sistemul central. Desemnează o autoritate, oficiul național SIS II (oficiul N.SIS II) care își asumă responsabilitatea principală pentru sistemul N.SIS II al respectivului stat. Această autoritate este responsabilă pentru buna funcționare și pentru securitatea N.SIS II.

<sup>6</sup> Vezi în special art. 41 din Regulamentul SIS II și art. 58 din Decizia SIS II.

<sup>7</sup> Vezi art. 43 din Regulamentul SIS II și art. 59 din Decizia SIS II.

<sup>8</sup> Vezi art. 4(1)(b) din Regulamentul SIS II și din Decizia SIS II.

maximum 60 de zile de la data la care depune cererea de acces sau mai devreme, în cazul în care acest lucru este prevăzut de legislația națională<sup>9</sup>.

De asemenea, persoana interesată va fi informată cu privire la rezultatul exercitării drepturilor acesteia de rectificare și de ștergere cât mai curând posibil și, în orice caz, într-un termen care nu depășește trei luni de la data la care a depus cererea de rectificare sau de ștergere sau mai devreme, în cazul în care acest lucru este prevăzut de legislația națională<sup>10</sup>.

## II.1. Dreptul de acces

Dreptul de acces reprezintă posibilitatea oricărei persoane care solicită acest lucru să aibă cunoștințe despre informațiile ce o privesc stocate într-un fișier de date prevăzut de legislația națională. Acesta reprezintă un principiu fundamental de protecție a datelor care permite persoanelor interesate să-și exercite controlul asupra datelor cu caracter personal păstrate de terți.

Acest drept este prevăzut în mod expres în art. 41 din Regulamentul SIS II și în art. 58 din Decizia SIS II<sup>11</sup>.

Dreptul de acces este exercitat în conformitate cu legislația Statului Membru pe teritoriul căruia este înaintată cererea. Procedura și regulile de comunicare a datelor către solicitant diferă de la un stat la altul. Când în Stat Membru primește o cerere de acces la o alertă emisă de alt stat, primul stat trebuie să ofere statului emitent ocazia de a-și face cunoscută poziția cu privire la posibilitatea dezvoltării datelor către solicitant<sup>12</sup>.

Informații nu sunt comunicate către persoana vizată dacă acestea sunt indispensabile pentru efectuarea unei operațiuni în legătură cu alerta sau pentru apărarea drepturilor și libertăților unor terți.

---

<sup>9</sup> Vezi art. 41(6) din Regulamentul SIS II și art. 58(6) din Decizia SIS II.

<sup>10</sup> Vezi art. 41(7) din Regulamentul SIS II și art. 58(7) din Decizia SIS II.

<sup>11</sup> Ambele articole prevăd: “Dreptul oricărei persoane de a avea acces la datele care le privesc introduse în SIS II în conformitate cu prezentul regulament se exercită în conformitate cu legislația Statului Membru față de care persoana respectivă invocă acest drept [...]”.

<sup>12</sup> Vezi art. 41(3) din Regulamentul SIS II și art. 58(3) din Decizia SIS II.



De asemenea, în prezent există două modalități de exercitare a dreptului de acces la datele prelucrate de autoritățile de aplicare a legii și, prin urmare, aplicabile datelor SIS. În anumite State Membre dreptul de acces este direct, în alte este indirect.

#### *II.1.1. Acces direct*

În această situație persoana vizat se adresează direct autorităților ce prelucrează datele (poliție, *jandarmarie*, vămi etc.). Dacă legea națională permite, solicitantul poate primi informațiile referitoare la el.

#### *II.1.2. Acces indirect*

În această situație persoană se adresează autorității naționale pentru protecția datelor din statul unde se depune cererea. Autoritatea pentru protecția datelor efectuează verificările necesare pentru a gestiona cererea și oferă un răspuns solicitantului.

### **II.2. Dreptul de rectificare și de ștergere a datelor**

Pe lângă dreptul de acces, există, de asemenea, dreptul de rectificare a datelor personale inexacte sau incomplete sau dreptul de a solicita ștergerea datelor personale stocate în mod ilegal (art. 41(5) din Regulamentul SIS II) și art. 58(5) din Decizia SIS II).

Potrivit cadrului legal Schengen numai Statul Membru responsabil pentru introducerea unei alerte în SIS o poate modifica sau șterge (vezi art. 34(2) din Regulamentul SIS II și art. 49(2) din Decizia SIS II).

În situația în care solicitarea este transmisă altui Stat Membru decât cel care a emis alerta, autoritățile competente implicate vor coopera, prin schimbul de informații și prin efectuarea de verificări necesare, în vederea soluționării cazului.

Solicitantul va motiva cererea de rectificare sau ștergere a datelor și va transmite orice informații relevante în susținerea acesteia.

### **II.3. Căi de atac: dreptul de a înainta o plângere autorității pentru protecția datelor sau de a se adresa justiției**

Art. 43 din Regulamentul SIS II și art. 59 din Decizia SIS II prezintă căile de atac accesibile persoanelor atunci când nu sunt mulțumite de răspuns. Orice persoană poate introduce o acțiune la instanțele judecătorești sau la autoritatea competentă potrivit legislației naționale pentru accesarea, rectificarea, ștergerea datelor sau pentru obținerea de compensații în legătură cu o alertă care o privește.

În situația în care este vorba de o plângere cu un element transnațional, autoritățile pentru protecția datelor trebuie să coopereze pentru a garanta drepturile persoanelor vizate.

### **III. DESCRIEREA PROCEDURII PENTRU EXERCITAREA DREPTULUI DE ACCES ÎN STATUL ÎN CAUZĂ**

Procedurile specifice fiecărui stat ce aplica acquis-ul Schengen ce trebuie respectate de persoanele ce doresc să-și exercite dreptul de acces, rectificare sau ștergere sunt descrise în fișele naționale de la capitolele IV-XXXII.

## IV. AUSTRIA

### 1. Natura dreptului de acces

În Austria, dreptul la informare potrivit legislației pe protecția datelor este direct adică solicitările de informații trebuie transmise și se va primi răspuns de la partea responsabilă pentru prelucrarea datelor (cunoscută drept „*Auftraggeber*” (operator) în Austria). Această regulă este aplicabilă în general potrivit legislație pe protecția datelor din Austria și este aplicabilă, în același timp, și informațiilor din SIS II privind alertele în conformitate cu art. 24 din Regulamentul SIS II și art. 26, 32, 34, 36 din Decizia SIS II.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Cererile de informații trebuie înaintate organelor de poliție (în calitate de operator) de la care persoanele vizate doresc să afle dacă prelucrează date care le privesc. Cererile de acces la SIS pot fi adresate direct *Bundeskriminalamt (Oficiul Federal de Infrațiuni)* care găzduiește Biroul SIRENE. Autoritatea pentru protecția datelor din Austria pune la dispoziție pe pagina sa web (<http://www.dsb.gv.at/site/6226/default.aspx>) un formular (în germană și engleză) pentru cererile de acces la datele Schengen

### 3. Formalități pentru cereri: informații și documente furnizate – posibile costuri

Potrivit §26 din *Datenschutzgesetz (DSG) 2000* (Legea pe protecția datelor 2000), operatorul trebuie să furnizeze persoanei vizate informații:

- atunci când solicitarea este transmisă de persoana vizată în scris (și verbal cu consimțământul operatorului) și
- dacă persoana vizată dovedește identitatea sa în modalitatea corespunzătoare (spre exemplu copie de pe cartea de identitate).

Informațiile trebuie să include:

- datele prelucrate
- informațiile disponibile referitoare la sursă

- toți destinatarii sau grupurile de destinatari ai datelor transmise
- scopul utilizării datelor
- temeiul legal, în termeni ușor de înțeles
- la solicitarea persoanei vizate, numele și adresele furnizorilor de servicii ce prelucrează datele.

Nu vor fi furnizate informații:

- dacă sunt necesare pentru a proteja persoana vizată din motive speciale,
- dacă prevalarea intereselor legitime ale operatorului sau ale unui terț constituie un impediment,
- dacă prevalarea intereselor publice constituie un impediment pentru dezvăluirea informațiilor având în vedere necesitatea:
  - o protejării instituțiilor constituționale ale Austriei
  - o asigurării că forțele armate federale sunt gata de acțiune
  - o protejarea intereselor de apărare națională,
  - o protejarea intereselor politicii externe, economice sau financiare importante ale Austriei sau Uniunii Europene,
  - o anticiparea, prevenirea sau cercetarea infracțiunilor.

În situația în care divulgarea trebuie să fie refuzată pentru a proteja interesele publice în domeniul de aplicare a legii, observația că „niciuna dintre datele referitoare la persoana vizată, care apare ca urmare a obligației de a furniza informații, nu a fost folosită” (paragraful 5) trebuie să fie indicată în toate cazurile în care nu se oferă informații (inclusiv în cazul în care, de fapt, nu au fost folosite date).

Refuzul de a furniza informații face obiectul verificării de către *Datenschutzybehörde* (Autoritatea pentru protecția datelor), precum și unei proceduri speciale de apel.

Informații nu pot fi furnizate în cazul în care persoana vizată nu a reușit să colaboreze în cadrul procedurii de informare sau nu a reușit să plătească taxa solicitată în mod legal.

Persoana vizată trebuie să coopereze cu întrebări rezonabile în cadrul procedurii de informare.

În termen de 8 săptămâni operatorul trebuie să furnizeze informațiile sau să motiveze în scris refuzul parțial sau total.

Informații este furnizate gratuit atunci când se referă la o bază de date actualizată și atunci când persoana vizată nu a înaintat aceeași cerere în același an.

În toate celelalte cazuri poate fi percepută o taxă de 18.89 EUR care poate varia în situația în care sunt suportate cheltuieli mai mari. Dacă dezvăluirea de informații are drept rezultat rectificarea datelor, taxa trebuie restituită.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Datenschutzbehörde

Hohenstaufengasse 3

A - 1010 Viena

Tel.: +43 1 531 15/2525

Fax: +43 1 531 15/2690

E-mail:

[dsb@dsb.gv.at](mailto:dsb@dsb.gv.at)

Dacă organele de poliție nu respectă termenul de 8 săptămâni, adică nu este primit niciun răspuns sau

Dacă autoritatea de poliția nu respectă limita de opt săptămâni, adică în cazul în care a fost primit nici un răspuns sau în cazul în care răspunsul oferit menționează faptul că nicio dată referitoare la persoana vizată nu a fost prelucrată, acest aspect poate fi prezentat autorității pentru protecția datelor în conformitate cu § 31(1) și §31a din legea pe protecția datelor 2000.

În cazul în care în cadrul unui apel în conformitate cu § 31a din legea pe protecția datelor 2000, operatorul invocă necesitatea prevalării secretului în interesul public, autoritatea pentru protecția datelor trebuie să verifice dacă secretul a fost necesar; în caz contrar, ordonă divulgarea datelor dacă secretul față de persoana în cauză nu a fost justificat.

Cu toate acestea, autoritatea poate face recurs la *Bundesverwaltungsgericht* (Curtea Federală Administrativă). Altfel, trebuie respectată decizia autorității pentru protecția datelor în termen de 8 săptămâni, iar în caz contrar, autoritatea pentru protecția datelor poate divulga ea însăși datele către persoana vizată.

## 5. Referințe principalele dispoziții naționale aplicabile

§26 din legea pe protecția datelor 2000 (DSG 2000), *BGBI.* (Monitorul Oficial) I, nr. 165/1999.

§26 (1) Operatorul trebuie să ofere persoanei vizate informații privind datele prelucrate ce o privesc atunci când persoana vizată solicită acest lucru în scris și își dovedește identitatea în mod corespunzător. Cu acordul operatorului, solicitările de informații pot fi și verbale. Informațiile transmise trebuie să includă datele prelucrate, informațiile disponibile referitoare la sursă, toți destinatarii sau grupurile de destinatari ai datelor transmise, scopul utilizării datelor și temeiul legal, în termeni ușor de înțeles. La solicitarea persoanei vizate, aceasta poate fi informată și cu privire la numele și adresele furnizorilor de servicii ce prelucrează datele care o privesc. Cu consimțământul persoanei vizate, informațiile pot fi oferite și verbal în loc de în scris.

(2) Nu vor fi furnizate informații dacă acestea sunt necesare pentru a proteja persoana vizată din motive speciale, dacă prevalarea intereselor legitime ale operatorului sau ale unui terț constituie un impediment, dacă prevalarea intereselor publice constituie un impediment pentru dezvăluirea informațiilor. O asemenea prevalarea poate apărea din necesitatea:

1. protejării instituțiilor constituționale ale Austriei
2. asigurării că forțele armate federale sunt gata de acțiune
3. protejarea intereselor de apărare națională,
4. protejarea intereselor politicii externe, economice sau financiare importante ale Austriei sau Uniunii Europene,
5. anticiparea, prevenirea sau cercetarea infracțiunilor.

Admisibilitatea refuzului de a furniza informații în temeiul punctelor 1-5 face obiectul verificării efectuate de autoritatea pentru protecția datelor potrivit §30(3), precum și proceduri speciale de recurs înaintea autorității pentru protecția datelor potrivit §31(4). (nota bene: trebuie interpretat „potrivit § 31a”).

(3) Persoana vizată trebuie să coopereze cu întrebări rezonabile în cadrul procedurii de informare pentru a evita activitatea disproporționată a operatorului.

(4) În termen de 8 săptămâni operatorul trebuie să furnizeze informațiile sau să motiveze în scris refuzul parțial sau total. De asemenea, există posibilitatea de a nu furniza informații atunci când persoana vizată nu a cooperat potrivit procedurii prevăzută la alin. (3) sau nu a achitat taxa.

(5) În domeniul aplicării legii responsabil pentru îndeplinirea atribuțiilor menționate la alin. (2), punctele 1-5, următoarea procedură trebuie respectată în vederea respectării intereselor publice care necesită refuzul de a furniza informații: în toate situațiile în care nu sunt oferite informații – de asemenea chiar și atunci când de fapt nu sunt folosite date – în loc de temeiul legal trebuie indicat faptul că nu sunt folosite date referitoare la persoana vizată. Admisibilitatea acestei proceduri face obiectul unei verificări din partea autorității pentru protecția datelor potrivit §30(3) și procedurilor speciale de recurs înaintea autorității pe protecția datelor potrivit §31(4).

(6) Informațiile trebuie furnizate în mod gratuit când se referă la o bază de date actualizată și atunci când persoana vizată nu a înaintat aceeași cerere în același an având același subiect. În toate celelalte cazuri poate fi percepută o taxă de 18.89 EUR care poate varia în situația în care sunt suportate cheltuieli mai mari. Taxele achitate trebuie să fie restituite fără a aduce atingere cererilor de despăgubire în situația în care datele au folosite în mod ilegal sau dacă este vorba de o rectificare.

(7) Odată de operatorul este conștient de faptul că o cerere pentru informații a fost depusă, acesta nu poate șterge datele referitoare la persoana în cauză pe o perioadă de 4 luni și, dacă a fost formulat un recurs la autoritatea pentru protecția datelor potrivit §31, datele nu pot fi șterse până la încheierea definitivă a procedurii.

(8) În cazul în care fișierele de date sunt folosite, prin lege, în scop de verificare de către public, persoana vizată are dreptul la informații în măsura în care există o dreptul de a verifica. Dispozițiile detaliate ce stabilesc registrul public reglementează procedura de inspecție.

(9) În ceea ce privește informațiile din dosarele penale, devin aplicabile prevederile speciale din Legea privind dosarul penal 1968 ce reglementează certificatele dosarului penal.

(10) În situația în care un contractor decide în mod automat, în baza dispozițiilor legale, eticii profesionale sau codurilor de conduită potrivit §6(4) să utilizeze o aplicație de date potrivit teze a treia

din §4 punctul 4, persoana vizată poate adresa inițial cererea de informații părții care a dispus implementarea aplicației. Acesta din urmă trebuie să informeze imediat și în mod gratuit persoana vizată cu privire la numele și adresa contractorului autonom, dacă nu se cunoaște deja acest lucru, pentru a permite persoanei vizate să-și apere dreptul la informare potrivit alin. (1).

## **6. Regimul limbajului**

Potrivit legislației din Austria, persoana vizată poate iniția procedura pentru dreptul de acces în Germania.



## V. BELGIA

### 1. Natura dreptului de acces

Orice persoană are dreptul la acces indirect la datele personale care o privesc ce au fost prelucrate de organele de poliție. În vederea exercitării acestui drept, trebuie înaintată o cerere Comisiei de Protecție a Vieții Private.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Commissie voor de bescherming van de persoonlijke levenssfeer  
Drukpersstraat 35, 1000 Brussel

Commission de la protection de la vie privée  
Rue de la Presse, 35, 1000 Bruxelles

+32 (0)2 274 48 00

+32 (0)2 274 48 35

[commission@privacycommission.be](mailto:commission@privacycommission.be)

Website: <http://www.privacycommission.be>

### 3. Formalități pentru cereri: informații și documente furnizate – posibile costuri

Cererile adresate Comisiei trebuie să fie datate și semnate. Adresa trebuie să conțină numele și prenumele, data nașterii și naționalitatea persoanei în cauză, precum și o fotocopie de pe cartea de identitate.

Trebuie indicate, *dacă sunt cunoscute*, denumirea autorității sau serviciului în cauză, precum și toate informațiile relevante referitoare la datele respective – natura, circumstanțele și sursa datelor, precum și rectificările dorite.

Procedura este gratuită.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Atunci când se primește o solicitare de acces indirect la datele personale prelucrate de poliție, Comisia efectuează toate verificările necesare la autoritatea respectivă.

Odată ce verificările au fost finalizate, Comisia informează persoana vizată că acestea au fost efectuate. Dacă este cazul, atunci când datele sunt prelucrate de poliție în vederea verificării identității și ca urmare a consultării respectivei autorități, Comisia transmite persoanei vizate orice alte informații pe care le consideră adecvate.

#### **5. Referințe principalele dispoziții naționale aplicabile**

- Legea din 8 decembrie 1992 privind protecția vieții private cu privire la prelucrarea datelor personale, modificată prin Legea din 11 decembrie 1998 ce transpune Directiva 95/46/CE din 24 octombrie 1995, în special art. 13;
- Decretul Regal din 13 februarie 2001 ce implementează Legea din 8 decembrie 1992 privind protecția vieții private cu privire la prelucrarea datelor personale, în special art. 36-46.

## VI. BULGARIA

### 1. Natura dreptului de acces

Orice persoană are dreptul de acces la datele sale personale colectate fără știința sa și prelucrate de Ministerul de Interne (MoI) în SIS și trebuie să transmită o cerere de acces la Biroul național SIRENE, stabilit ca unitate în cadrul Direcției de Cooperare Operativă Internațională a MoI.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Ministry of Interior of the Republic of Bulgaria

Sofia, 1000 29

“6-th September” str.

Tel.: + 359 2/9825000 – sediul MoI

Web site: <http://www.mvr.bg/contactus.htm>

### 3. Formalități pentru cereri: informații și documente furnizate – posibile costuri

Persoanele își pot exercita dreptul prin transmiterea unei solicitări scrise (personal sau prin persoane autorizate prin împuternicire avocațială certificată la notar) operatorului (în acest caz Ministerul de Interne).

Cererea poate de asemenea fi trimisă prin poșta electronică potrivit procedurii din Legea privind documentele electronice și semnătură electronică.

Ministerul de Interne este obligată să ia o decizie în termen de 14 zile de la primirea cererii de acces. La cerere, poate fi oferită o copie după datele personale prelucrate ale individului.

Transmiterea cererii de acces la datele SIS este gratuită.

#### 4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil

Commission for Personal Data Protection  
Sofia 1592, 2 “Prof. Tsvetan Lazarov” blvd.

Call centre - Tel.: + 3592/91-53-518

Registry:

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

Fax: +3592/91-53-525

E-mail: [kzld@cpdp.bg](mailto:kzld@cpdp.bg)

Web site: [www.cdpd.bg](http://www.cdpd.bg)

Orice persoană are dreptul de a solicita CPDP să verifice datele care o privesc introduce în Sistemul de Informații Schengen, precum și să primească informații cu privire la utilizarea acestora. Dacă datele sunt introduse de un alt Stat Membru, CPDP va efectua o investigație în strânsă colaborare cu autoritatea de supraveghere a respectivului Stat Membru.

- În situația în care operatorul (Ministerul de Interne) nu ia în considerare cererea de acces a persoanei și consideră că este vorba de o încălcare a LPPD prin prelucrarea datelor sale personale (adică împiedică exercitarea drepturilor persoanei), persoana în cauză se poate adresa cu o plângere la CPDP (pentru inițierea procedurilor potrivit procedurii administrative). Dacă persoana nu a transmis o plângere la CPDP, aceasta poate contesta decizia (refuzul de acces sau de transmitere de informații sau împiedicarea exercitarea dreptului de ștergere, rectificare sau blocare) la instanță. Comisia pentru Protecția Datelor Personale soluționează plângerea și adoptă decizia care, după intrarea în vigoare, este obligatorie pentru operator. Dacă subiectul plângeri este refuzul de acces, prin decizia sa, CPDP poate oblica operatorul să exercite accesul solicitate și să ofere instrucțiuni în acest sens.
- Atunci când se constată o încălcare în ceea ce privește prelucrarea datelor personale, CPDP poate aplica operatorului sancțiuni administrative – amenzi sau sancțiuni asupra bunurilor.

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

În legea Ministerului de Interne (MIA) este prevăzut că fiecare persoană are dreptul de a solicita accesul la datele sale personale, colectate fără știrea sa și prelucrate în sistemele MoI. Operatorul de date emite o decizie în termen de 14 zile de la data primirii cererii de acces. În situația în care dorește, persoana poate primi o copie pe hârtie a datelor sale prelucrate. Organismele MoI refuză parțial sau în totalitate transmiterea datelor:

- când acest lucru ar afecta securitatea națională sau ordinea publică;
- în vederea protejării informațiilor clasificate sau a secretelor de stat;
- când pot fi dezvăluite sursele de informare sau mijloacele și metodele de colectare;
- când transmiterea datelor persoanei constituie derogarea de la exercitarea atribuțiilor MoI potrivit legii;
- sau când datele introduse în SIS de către un alt stat care nu a permis acest lucru.

Persoanele sunt informate în scris cu privire la temeiul legal al refuzului. Dacă notificarea nu este transmisă în termenul legal prevăzut, se consideră a fi un refuz. Potrivit art. 161 MIA, refuzul constituie subiect al recursului potrivit procedurii stabilite prin Codul Administrativ Penal.

## **6. Referințe principalele dispoziții naționale aplicabile**

- Legea Ministerului de Interne – promulgat prin SG 17/24.02.2006, modificată și completată prin SG 70/09.08.2013, intrată în vigoare începând cu 09.08.2013.
- Regulamente privind implementarea Legii Ministerului de Interne – adoptate prin Decretul Consiliului de Miniștri 126/02.06.2006, promulgate prin SG 47/09.06.2006, modificate și completate prin SG 10/10.04.2014.
- Ordonanța 2727 din 16 noiembrie 2010 privind organizarea și funcționarea Sistemului Național de Informații Schengen al Republicii Bulgare – emisă de MoI – în vigoare începând cu 30.11.2010, modificată și completată prin SG 28/19.03.2013.

- Ordonanța pentru modificarea și completarea Ordonanței 2727 din 16 noiembrie 2010 privind organizarea și funcționarea Sistemului Național de Informații Schengen al Republicii Bulgare – emisă de MoI – în vigoare începând cu 19.03.2013, promulgată prin SG 28/19.03.2013.

- Legea pentru protecția datelor personale – promulgată prin SG 1/04.01.2002, modificată și completată prin SG 15/15.02.2013.

## **7. Regimul limbajului**

Cererile de acces la datele prelucrate în Sistemul de Informații Schengen se transmit în bulgară.

## VII. REPUBLICA CEHĂ

### 1. Natura dreptului de acces

Persoana vizată are drept de acces direct. Persoana vizată trebuie să-și exercite în primul rând dreptul de acces în ceea ce privește SIS la operatorul de date, adică Poliția Republicii Cehe.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Police Presidium of the Czech Republic

P. O. Box 62/K-SOU

Strojnická 27

170 89 Prague 7

### 3. Formalități pentru cereri: informații și documente furnizate – posibile costuri

Informații privind modalitatea de solicitare de informații sau de corectare/ștergere a datelor sunt disponibile pe site-ul autorității de supraveghere ([www.uoou.cz](http://www.uoou.cz)), inclusiv formulare pe care persoana vizată de poate folosi. Pagina web a poliției ([www.policie.cz](http://www.policie.cz)) și a Ministerului de Interne (<http://www.mvcr.cz/eu-schengen.aspx>) oferă de asemenea informații, precum și site-ul general „European” al Republicii Cehe ([www.euroskop.cz](http://www.euroskop.cz)).

Orice persoană vizată are dreptul de a transmite o cerere în scris Poliției Republicii Cehe (la adresa menționată mai sus) pentru a-și exercita dreptul la informare și ștergere sau rectificare a datelor sale personale prelucrate în SIS. Informațiile privind prelucrarea datelor personale din SIS vor fi dezvăluite doar persoanei vizate (sau avocatului său). Solicitarea trebuie să conțină datele de identificare ale solicitantului – toate numele, prenumele, data și locul nașterii, adresa, sexul și cetățenia. Pentru a asigura identificarea solicitantului și, prin urmare, prelucrarea de încredere a solicitării, este recomandată includerea unei copii de pe un documente de identificare care servește drept dovadă a identității solicitantului și ajută la evitarea riscului de a dezvălui date personale unei persoane neautorizate. Poliția este obligată să răspundă în termen de 60 de zile. Exercițarea dreptului de acces este gratuită.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

The Office for Personal Data Protection

Pplk. Sochora 27

170 00 Praha 7

Czech Republic

Oficiul pentru Protecția Datelor Personale este competent pentru verificarea prelucrării datelor personale în ceea ce privește partea națională SIS la cererea persoanelor vizate în situațiile în care există o suspiciune de prelucrare ilegală sau în situația în care operatorul (Poliția Republicii Cehe) nu a furnizat un răspuns satisfăcător.

#### **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Poliția ar trebui să răspundă dacă date personale cu privire la persoana vizată sunt conținute în SIS, care sunt acestea, care a fost motivul introducerii lor (scopul) și ce autoritatea le-a introdus.

Potrivit art. 83 (4) din Legea poliției, poliția nu trebuie să răspundă la cerere dacă acest lucru pune în pericol îndeplinirea atribuțiilor polițienești în ceea ce privește procedurile penale sau securitatea națională sau periclitează interesele legitime ale unui terț.

#### **6. Referințe principalele dispoziții naționale aplicabile**

Legea nr. 101/2000 privind Protecția datelor Personale și privind modificări aduse anumitor legi (art. 12 și 21)

Legea nr. 273/2008 privind Poliția Republicii Cehe (art. 83 și 84)

#### **7. Regimul limbajului**

Limba cehă este singura limbă oficială pentru comunicarea cu autorități cehe. Totuși, autoritatea pentru protecția datelor din Cehia comunică, de asemenea, și în engleză. Informațiile de bază privind modalitatea de exercitare a dreptului de acces de pe site-ul autorității pentru protecția datelor din Cehia sunt disponibile și în engleză.



## **VIII. DANEMARCA**

### **1. Natura dreptului de acces**

Persoana vizată are drept de acces direct.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Cererile de acces trebuie adresate operatorului de date, respectiv Poliției:

Rigspolitiet  
Polititorvet 14  
DK-1780 København V  
Tel.: +45 33 14 88 88

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Nu există anumite cerințe formale pentru transmiterea cererilor.

Cererile de acces trebuie soluționate cât mai curând posibil, iar atunci când în situații excepționale nu se poate oferi un răspuns în termen de 4 săptămâni, operatorul trebuie să informeze solicitantul în acest sens. O asemenea comunicare trebuie să menționeze motivele pentru care nu se poate lua o decizie în termen de 4 săptămâni, dar și când va fi luată o asemenea hotărâre.

De principiu, accesul trebuie oferit în scris dacă aceasta este dorința solicitantului. În situația în care persoana vizată se adresează operatorului, trebuie stabilit dacă aceasta dorește un răspuns în scris sau o explicație verbală cu privire la conținutul datelor.

Cererile de acces sunt gratuite.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Datatilsynet  
Borgergade 28, 5. sal  
DK-1300 København K  
Tel.: +45 3319 3200  
Fax: +45 3319 3218  
E-mail: dt@datatilsynet.dk  
www.datatilsynet.dk

Plângerile privind decizia Poliției în legătură cu accesul pot fi înaintate Agenției pentru Protecția Datelor în calitate de instanță administrativă pentru plângeri. Pentru soluționarea plângerilor, Agenția pentru Protecția Datelor examinează cazul pentru a se asigura că nu au fost introduse date într-o manieră ce contravine regulilor din Regulamentul SIS II și din Decizia SIS II.

#### **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Potrivit secțiunii 31(1) din Legea privind prelucrarea datelor personale, operatorul (în acest caz Poliția) trebuie să informeze persoana care a înaintat o solicitare dacă datele care o privesc sunt sau nu sunt prelucrate. În situația în care aceste date sunt prelucrate, comunicarea către respectiva persoană cu privire datele prelucrate, scopurile prelucrării, categoriile de destinatari ai datelor, precum și alte informații disponibile cum ar fi sursa datelor trebuie realizată într-o formă inteligibilă.

Potrivit secțiunii 32(1) coroborat cu secțiunea 30(2) din lege, nu este aplicabil în situația în care interesul persoanei vizate de a obține aceste informații prevalează interesele publice vitale, inclusiv:

- (1) securitatea națională
- (2) .....
- (3) securitatea publică
- (4) prevenirea, investigarea, detectarea și punerea sub urmărire a infracțiunilor sau a încălcării eticii în cazul profesiunilor reglementate
- (5) .....
- (6) .....

## **6. Referințe principalele dispoziții naționale aplicabile**

Legea nr. 429 din 31 mai 2000 privind prelucrarea datelor personale.

## **7. Regimul limbajului**

Daneza este limba oficială pentru comunicarea cu autoritățile daneze. Totuși este posibilă comunicarea cu autoritățile daneze și în engleză.

## IX. ESTONIA

### 1. Natura dreptului de acces

Direct, dar în situația în care persoana solicită acces prin intermediul autorității de supraveghere nu o direcționăm către împuternicit, ci solicităm informații pe care le transmitem respectivei persoane.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Police and Border Guard Board

Pärnu mnt 139

15060 TALLINN

telephone 612 3300

fax +372 612 3009

[ppa@politsei.ee](mailto:ppa@politsei.ee)

[www.politsei.ee](http://www.politsei.ee)

### 3. Formalități pentru cereri: informații și documente furnizate – posibile costuri

Solicitarea/cererea semnată electronic sau pe hârtie, copie de pe cartea de identitate sau pașaport. Exercițarea este gratuită.

### 4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil

Data Protection Inspectorate

Väike-Ameerika 19, 10129

Tallinn, Estonia

[info@aki.ee](mailto:info@aki.ee)

[www.aki.ee](http://www.aki.ee)

Autoritatea pentru protecția datelor are toate drepturile să verifice alertele și documentele ce stau la baza acestora, solicitările de acces, de ștergere sau rectificare a datelor personale prelucrate ilegal.

Angajații autorității pentru protecția datelor au dreptul de a intra fără nicio reținere în sediul unui împuternicit în vederea efectuării de investigații, dreptul de acces la documentele și echipamentele unui împuternicit, precum și la datele înregistrate și la software-ul utilizat pentru prelucrarea datelor.

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Rezultatul așteptat este de a oferi acces în măsura în care este prevăzut de lege. În situația protejării procedurilor penale etc., accesul la asemenea date este limitat. DPA poate supraveghea validitatea unei asemenea limitări. Termenul limită național este de 30 de zile.

## **6. Referințe principalele dispoziții naționale aplicabile**

Legea privind protecția datelor personale

Legea privind poliția și poliția de frontieră

Statutul privind menținerea registrului național al Sistemului de Informații Schengen

## **7. Regimul limbajului**

Sunt acceptate cereri în estoniană, engleză și rusă, care sunt cel mai des folosite. Răspunsul va fi în estoniană și engleză.

## **X. FINLANDA**

### **1. Natura dreptului de acces**

Persoana vizată are drept de acces direct.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Cererea trebuie înaintată în persoană la poliția locală județeană.

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Solicitările trebuie transmise în persoană poliției, iar solicitanții trebuie, în același timp, să facă dovada identității lor.

Exercitarea dreptului de inspecție este subiect al unei taxe doar în situația în care nu a trecut 1 an de la ultima exercitare a respectivului drept.

Deținătorul registrului trebuie, fără întârziere, să ofere respectivei persoane posibilitatea de a consulta informațiile din registru și să ofere informații în scris la solicitarea acesteia.

### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Ratapihantie 9

PL 800,

FIN - 00521 Helsinki

Tel.: ++358 (0)29 56 66700

Fax: ++358 (0)29 56 66735

E-mail: [tietosuoja@om.fi](mailto:tietosuoja@om.fi)

Internet: [www.tietosuoja.fi](http://www.tietosuoja.fi)

În situația în care poliția refuză dreptul de a interoga datele SISI II în temeiul Secțiunii 27 din Legea pentru protecția datelor, trebuie emis un certificat în acest sens, iar persoana vizată trebuie direcționată să contacteze autoritatea pentru protecția datelor. Respectiva persoană poate semnala acest aspect autorității în cauză.

Autoritatea pentru protecția datelor emite decizii obligatorii privind dreptul de investigare. Deciziile autorității pot fi contestate prin recurs la instanța administrativă și ulterior Curții Administrative Supreme (Secțiunile 28 și 29 din Legea pentru protecția datelor).

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Legea privind protecția datelor (523/1999)

Legea poliției privind protecția datelor (761/2003)

## **XI. FRANȚA**

### **1. Natura dreptului de acces**

În Franța, dreptul de acces la Sistemul de Informații Schengen (SIS) este mixt. Dreptul de acces este direct pentru persoanele dispărute (art. 32 din Decizia Consiliului 2007/533) sau pentru persoanele menționate sau identificate într-o alertă referitoare la obiecte (art. 38 din aceeași Decizie).

În toate celelalte situații, SIS este considerat a fi un fișier ce implică securitatea națională, apărare sau siguranța publică și, prin urmare, dreptul de acces poate fi exercitat numai indirect prin intermediul Comisiei Naționale pentru Informații și Libertăți (CNIL).

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Dacă cererea se referă la unul din cazurile în care dreptul de acces este direct, aceasta trebuie înaintată:

Direction Centrale de la Police Judiciaire  
Ministère de l'intérieur  
Place Beauvau  
F-75008 Paris  
Tél.: +33(0)1.49.27.49.27  
Internet: [www.interieur.gouv.fr](http://www.interieur.gouv.fr)

În toate celelalte situații, cererea trebuie înaintată:

Commission nationale de l'informatique et des libertés  
8, rue Vivienne - CS 30223  
F-75083 Paris Cedex 02  
Tél.: ++33 1 53 73 22 22  
Fax: ++33 1 53 73 22 00  
E-mail: [mabiven@cnil.fr](mailto:mabiven@cnil.fr)  
Internet: [www.cnil.fr](http://www.cnil.fr)



### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Dreptul de acces este strict personal. Cererea de acces trebuie transmisă și semnată de solicitant (în caz contrar, în alte circumstanțe, poate fi înaintată de un membru al familiei sau o rudă). Totuși, solicitatul poate împuternici un avocat să transmită cererea în numele său, cu condiția ca împuternicirea să fie menționată în clar în cerere.

Nu există o cerință expresă pentru cerere, dar solicitantul trebuie să atașeze la adresa sa o copie lizibilă de pe un document oficial prin care certifică identitatea sa (nume, prenume, data și locul nașterii) precum cartea de identitate, pașaport, permis de ședere, certificat de naștere...

De asemenea, orice documente transmise de solicitat utile pentru efectuarea verificărilor sunt binevenite (notificarea de refuz de viză în baza unei alerte SIS, orice decizie favorabile precum anularea unui ordin de expulzare).

Procedura de exercitare a dreptului de acces este gratuită.

### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Commission nationale de l'informatique et des libertés

8, rue Vivienne - CS 30223

F-75083 Paris Cedex 02

Tél.: ++33 1 53 73 22 22

Fax: ++33 1 53 73 22 00

E-mail: [mabiven@cnil.fr](mailto:mabiven@cnil.fr)

Internet: [www.cnil.fr](http://www.cnil.fr)

Odată ce solicitarea a fost primită, CNIL desemnează unul dintre membrii săi, care este sau a fost un magistrat al „Consiliului de Stat”, „Curții de Casație” sau „Curții de Conturi” să efectueze toate investigațiile, precum și toate modificările necesare. În acest sens, magistratul desemnat se deplasează direct la sediul Biroului SIRENE din Franța și verifică în persoană motivul pentru care solicitantul este înregistrat în sistem.

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

După efectuarea verificărilor, rezultatele pot fi comunicate numai solicitantului ce face obiectul unei alerte naționale în situația în care membrul Comisiei stabilește, cu acordul operatorului, că dezvăluirea datelor nu prejudiciază scopul, securitatea națională, apărare sau siguranța publică.

Atunci când operatorul face obiecții cu privire la dezvăluirea informațiilor (adică persoana face obiectul verificărilor discrete sau specifice, este emis un mandat de arestare pe numele respectivei persoane, persoanei îi este interzisă intrare pe teritoriul statului pe baza politicii publice), Comisia informează solicitantul în sensul că au fost efectuate verificările necesare, dar că nu pot fi furnizate informații solicitantului (art. 88 din Decretul nr. 2005-1309 din 20 octombrie 2005 adoptat în aplicarea Legii nr. 78-17 din 6 ianuarie 1978 privind Tehnologia Informației, Fișierelor de Date și Libertăților Civile). De asemenea, Comisa informează solicitantul cu privire la mijloacele și perioada de timp pe care le are la dispoziție în vederea contestării obiecții.

Dacă solicitantul face obiectul unei alerte introduse de un alt Stat Membru, CNIL va coopera cu autoritatea pentru protecția datelor din respectivul stat.

Dacă verificările efectuate permit ștergerea alertei, acest lucru va fi comunicat persoanei vizate cu condiția ca operatorul să nu aibă obiecții.

Perioada medie de timp variază între 1 lună și 4 luni în funcție dacă solicitantul face obiectul unei alerte sau dacă este nevoie de a continua procedura, cum ar fi cooperarea dintre autoritățile pentru protecția datelor, în vederea verificării validității alertei.

## **6. Referințe principalele dispoziții naționale aplicabile**

Art. 41 din Legea nr. 78-17 din 6 ianuarie 1978 privind Tehnologia Informației, Fișierelor de Date și Libertăților Civile

Art. 86 și Decretul nr. 2005/1309 din 20 octombrie 2005 adoptat în aplicarea Legii nr. 78-17 menționată anterior

## **7. Regimul limbajului**

Solicitantul poate transmite cererea atât în limba franceză, cât și în limba engleză.

## **XII. GERMANIA**

### **1. Natura dreptului de acces**

Dreptul de acces în Germania este direct. Este exercitat direct la autoritatea responsabilă pentru înregistrarea datelor. Dacă dorește, persoana vizată își poate exercita dreptul de acces prin intermediul autorității pentru protecția datelor.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Bundeskriminalamt

– SIRENE Büro –

D – 65173 Wiesbaden

Tel.: ++611 551 65 11

Fax: ++611 551 65 31

E-mail: [sirenedeukschland@bka.bund.de](mailto:sirenedeukschland@bka.bund.de)

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Persoana vizată trebuie să menționeze numele (numele dinaintea căsătoriei, după caz), prenumele și data nașterii pentru a evita orice confuzie. În afară de acestea, nu există o altă cerință expresă, iar procedura este gratuită.

Determinarea detaliilor pentru procedura ulterioară este de competența autorității responsabile – Bundeskriminalamt.

Dacă dreptul de acces este exercitat prin intermediul autorității pentru protecția datelor, respectivul cetățean trebuie să furnizeze o copie semnată a pașaportului pentru a fi verificată identitatea acestuia.

### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Autoritatea națională pentru protecția datelor poate sprijini persoana vizată în procedura de exercitare a drepturilor sale prin transmiterea cererii de informații organismului responsabil pentru înregistrarea

datelor, adică *Bundeskriminalamt* (Biroul Federal pentru Investigarea Infracțiunilor) sau prin inițierea unei investigații pe protecția datelor la respectiva entitate. Adresa autorității este:

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Husarenstraße 30

D - 53117 Bonn

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

Fax: ++49-228-997799-550

E-mail: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

Internet: [www.bfdi.bund.de](http://www.bfdi.bund.de)

În situația în care solicitarea se referă la o alertă potrivit art. 24 din Regulamentul SIS II, informațiile sunt de obicei dezvăluite.

În situația în care solicitarea se referă la o alertă potrivit art. 36 din Decizia SIS II, se poate refuza dacă cel puțin unul din motivele valide pentru refuzul dezvăluirii de informații, prevăzute în § 19(4) din Legea Federală pentru Protecția Datelor este aplicabil cererii, adică dacă dezvăluirea informații poate prejudicia îndeplinirea corespunzătoare a atribuțiilor obligatorii pentru organismul de a înregistra datele sau poate prezenta o amenințare la securitatea publică sau lege și ordine sau dacă datele sau faptul că au fost înregistrate trebuie păstrate secrete prin lege sau prin definiție, în special dacă prevalează interesele unui terț și trebuie să se renunțe la interesele persoanei vizate în obținerea informațiilor.

În situația în care alerta a fost introdusă de o autoritatea străină potrivit art. 26 din Decizia SIS II, trebuie avută în vedere poziția autorității străine emițătoare potrivit celei de-a treia teze din art. 41(3) din Regulamentul SIS II sau art. 58(3) din Decizia SIS II. De obicei, informațiile sunt oferite de *Bundeskriminalamt* – Biroul SIRENE. Dacă persoana vizată a aplicat la autoritatea națională pentru protecția datelor, informațiile sunt furnizate de Comisarul Federal pentru Protecția Datelor. De regulă, informațiile includ temeiul legal al alertei, data emiterii și perioada probabilă de păstrare, precum și autoritatea emițătoare.

## **5. Referințe principalele dispoziții naționale aplicabile**

Textele naționale principale aplicabile sunt art. 41(3) din Regulamentul SIS II și art. 58(3) din Decizia SIS II coroborate cu art. 19 din Legea Federală pentru Protecția Datelor sau reglementările relevante privind dreptul la informare din alte legi pe protecția datelor la nivel *Länder*.

## **6. Regimul limbajului**

Potrivit legislației naționale „(§23 din Legea Federală privind procedurile administrative – *Verwaltungsverfahrensgesetz*)” limba oficială e germana, dar cu privire la cetățenii Uniunii Europene, așa cum este menționat în art. 17 din Tratatul CEE, pot fi acceptate și cereri în alte limbi ale UE.

## **XIII. GRECIA**

### **1. Natura dreptului de acces**

Potrivit art. 12 din Legea nr. 2472/1997, dreptul de acces este direct (solicitanții transmit cererea directă Biroului SIRENE). În situația în care înaintează cererea Autorității pentru Protecția Datelor Personale, aceștia sunt sfătuiți să o transmită direct Biroului SIRENE.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Legea prevede ca cererile să fie transmise Biroului SIRENE a cărui adresă este următoarea:

Ministry of Public Order and Citizen Protection  
Hellenic Police Headquarter  
International Police Cooperation Division  
3d Department - SIRENE  
P. Kanellopoulou 4  
PC: 101 77 Athens  
Tel.: ++301 69 81 957  
Fax: ++301 69 98 264/5  
E-mail: [sirene@police.gr](mailto:sirene@police.gr)  
Internet: ---

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Cererile trebuie să conțină numele și prenumele solicitantului, prenumele tatălui, data nașterii și naționalitatea. Sunt opționale celelalte detalii precum codul numeric personal, numărul pașaportului, adresa și numărul de telefon și prenumele mamei. Solicitantul trebuie să furnizeze o copie de pe pașaport.

Pentru a exercita dreptul de acces potrivit art. 12 din Legea nr. 2472/1997, solicitanții trebuie să achite operatorului o taxă de 5EUR (Biroul SIRENE) și o taxă de 60EUR pentru exercitarea dreptului de opoziție potrivit art. 13 din legea menționată mai sus și Decizia 122 adoptată de Autoritatea pentru

Protecția Datelor din 9 octombrie 2001. Trebuie adăugat faptul că, în vederea exercitării dreptului de acces la SIS, taxa ne semnificativă de 5EUR nu este niciodată percepută.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Datele de contract ale autorității naționale pentru protecția datelor din Grecia sunt următoarele:

Hellenic Data Protection Authority

Kifisias 1-3, 1st floor

GR – 115 23 Athens

Tel.: ++30 210 6475600

Fax: ++ 301 210 6475628

E-mail: [contact@dpa.gr](mailto:contact@dpa.gr)

Internet: [www.dpa.gr](http://www.dpa.gr)

Autoritatea națională pentru Protecția Datelor Personale verifică legalitatea alertelor SIS în legătură cu persoana respectivă.

#### **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Dacă alerta a fost emisă potrivit art. 2 din Regulamentul SIS II, solicitantul va fi informat cu privire la datele ce îl privesc.

Dacă alerta a fost emisă potrivit art. 26 sau art. 36 din Decizia SIS II, cel mai probabil solicitantului îi va fi refuzată dezvăluirea datelor. Mai mult, în conformitate cu art. 12(5) din Legea nr. 2472/1997, datele nu vor fi dezvăluite dacă prelucrarea a fost efectuată în temeiul securității naționale sau pentru investigarea unor infracțiuni grave. Atunci când alerta potrivit art. 26 din Decizia SIS II a fost introdusă de o autoritate străină, opinia acesteia din urmă va fi luată în considerare în luarea deciziei de transmitere a datelor către solicitant.

Informațiile transmise către solicitant conțin temeiul legal al alertei, data introducerii acesteia în SIS II, autoritatea care a introdus alerta, perioada de păstrare a acesteia.

## **6. Referințe principalele dispoziții naționale aplicabile**

Prevederile aplicabile sunt art. 41 din Regulamentul SIS II și art. 58 din Decizia SIS II și art. 12 (exercitarea dreptului de acces) și art. 13 (exercitarea de opoziție) din Legea nr. 2472/1997.

### **Comentariu**

În situația în care celelalte detalii ale solicitantului au fost înregistrate în SIS de poliția din Grecia, solicitările de exercitare a dreptului de acces și de opoziție potrivit art. 12 și 13 din Legea nr. 2472/1997 se adresează direct operatorului.

În ceea ce privește regimul limbajului, limba oficială este greaca, totuși, sunt luate în considerare și cererile în engleză.



## XIV. UNGARIA

### 1. Natura dreptului de acces

Dreptul de acces poate fi exercitat atât direct, cât și indirect.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Biroul SIRENE al sediului Poliției Naționale

H-1139 Budapest, Teve utca 4-6.

Tel: +36 1 443 5861

e-mail: [sirene@nebek.police.hu](mailto:sirene@nebek.police.hu)

Nemzeti Adatvédelmi és Információszabadság Hatóság

Postal address: 1530 Budapest, Pf.: 5.

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

Tel: +36 1 391-1400

Fax: +36 1 391-1410

Email: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

Web: <http://naih.hu>

În Ungaria, orice persoană interesată în a afla dacă datele ce o privesc sunt înregistrate în SIS sau dorește rectificarea sau ștergerea datelor incorecte trebuie să contacteze orice serviciu guvernamental (<http://www.kormanyhivatal.hu/hu>), secție de poliție (<http://www.police.hu/magyarendorseg/szervezetif>) sau orice Consulat sau Ambasadă a Ungariei (<http://www.kormany.hu/hu/kovetsegek-konzulatusok>) și completează o cerere de informații care este transmisă Biroului SIRENE din cadrul Poliției Naționale Ungare.

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Persoana vizată trebuie să furnizeze dovezi în legătură cu identitatea sa și/sau autorizația sa. Cererile pot fi transmise în maghiară, engleză, germană sau franceză. Informațiile trebuie transmise în scris în cel mai scurt timp posibil, dar nu mai târziu de 30 de zile de la data primirii cererii. Solicitarea este gratuită. Dacă persoana vizată transmite în mod regulat pe perioada unui an o astfel de cerere, va suporta cheltuielile pentru furnizarea informațiilor.

### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Autoritatea Națională pentru Protecția Datelor și Libertatea de Informare din Ungaria are autoritatea de a efectua o investigație sau o procedură administrativă pentru protejarea datelor ca urmare a unei cereri înaintate potrivit prevederilor relevante (52-61.§) din Legea CXII din 2011 privind auto-determinarea informațională și libertatea de informare (legea privind viața privată). În plus, dacă persoana vizată are îndoieli cu privire la răspunsul primit de la Biroul SIRENE sau nu primește un răspuns, poate informa Autoritatea Națională pentru Protecția Datelor și Libertatea de Informare din Ungaria.

### **5. Referințe principalele dispoziții naționale aplicabile**

Legea CXII din 2011 privind auto-determinarea informațională și libertatea de informare (legea privind viața privată)

Legea CLXXXI din 2012 privind schimbul de informații în contextul Sistemului de Informații Schengen generația a II-a

Decretul guvernului no. 15/2013 (28/I) în legătură cu procedurile detaliate privind schimbul de informații în contextul Sistemului de Informații Schengen generația a II-a

## **XV. ISLANDA**

### **1. Natura dreptului de acces**

Dreptul de acces este direct ceea ce înseamnă că persoanele vizate trebuie să se adreseze cu cerere de informații, rectificare sau ștergere la Biroul SIRENE, care decide asupra acestora.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Cererile trebuie înaintate Biroului SIRENE din Islanda, care se află în subordinea Comisarului Poliției Naționale din Islanda (CINP).

Adresa CINP este următoarea:

Ríkislögreglustjórnin

SIRENE-skrifstofa

Skúlagata 21

101 Reykjavík

ICELAND

Tel.: ++354 444 2500

Fax: ++354 444 2501

E-mail: [rls@rls.is](mailto:rls@rls.is)

Internet: [www.rls.is](http://www.rls.is)

Formularele speciale pot fi completate la secțiile locale de poliție sau la sediul CINP. Biroul SIRENE ia decizia cu privire la dezvoltarea informațiilor.

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Solicitantul trebuie să facă dovada identității sale, iar formularul de solicitare trebuie completat în prezența unui polițist. Persoana respectivă poate solicita informații doar despre ea. Totuși, un reprezentant legal poate înainta cererea în numele său. Exercițarea dreptului la investigație este gratuită, dar fiecare persoană va beneficia de acces la informații o singură dată pe an, cu excepția situațiilor de excepție când se poate solicita acces de mai multe ori. În aceste situații, Biroul SIRENE va consulta autoritatea pentru protecția datelor (DPA).

Cererile trebuie făcute de persoana vizată. Este necesară dovedirea identității. Informațiile trebuie oferite în mod gratuit.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

În situațiile în care un solicitant a primit răspunsul standard: „nu sunt informații înregistrate/nu este permisă dezvăluirea informațiilor înregistrate” (vezi punctul 5), Biroul SIRENE informează solicitantul cu privire la posibilitatea de contestare a deciziei în fața Ministerului de Justiție și a Drepturilor Omului. Ministerul poate solicita opinia autorității pentru protecția datelor în ceea ce privește decizia Biroului SIRENE.

The Ministry of Justice and Human Rights:

Dómsmála- og mannréttindaráduneytid

Skuggasund

IS - 150 Reykjavík

Tel.: ++354 545 9000.

Fax: ++354.552.7340

E-mail: [postur@dmr.stjr.is](mailto:postur@dmr.stjr.is)

Internet: [www.domsmalaraduneyti.is](http://www.domsmalaraduneyti.is)

Adresa autorității pentru protecția datelor este:

Persónuvernd

Rauðarástígur 10

IS - 105 Reykjavík

Tel.: ++354 510 9600.

Fax: ++354 510.9606

E-mail: [postur@personuvernd.is](mailto:postur@personuvernd.is)

Internet: [www.personuvernd.is](http://www.personuvernd.is)

Dacă nu este oferit accesul, autoritatea pentru protecția datelor poate emite o opinie în legătură cu drepturile persoanei vizate. Cu toate acestea, autoritatea pentru protecția datelor nu are atribuții cu privire la SIS II.

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Biroul SIRENE trebuie să răspundă tuturor solicitărilor fără întârziere și nu mai târziu de o lună de la data primirii cererii. Dacă un solicitant este înregistrat, acesta va fi informat cu privire la scopul și motivele înregistrării. În situații în care este necesară păstrarea secretului informațiilor pentru atingerea scopului propus al introducerii datelor în sistem sau în vederea protejării intereselor altor persoane sau atunci este în curs de desfășurare o supraveghere discretă, persoana vizată nu are dreptul de a fi informată cu privire la datele înregistrate. Solicitantul va primi același răspuns standard precum cel ce nu este înregistrat, respectiv „nu sunt informații înregistrate/nu este permisă dezvăluirea informațiilor înregistrate”.

Art. 13 și 15 din Legea privind Sistemul de Informații Schengen în Islanda (<http://www.personuvernd.is/information-in-english/greinar/nr/440>):

### **Art. 13**

Orice persoană ale cărei date sunt introduse în sistemul de informații (persoana vizată) are dreptul de a fi informată cu privire la datele ce o privesc introduse în sistem.

Dreptul la informare al persoanei vizate potrivit alin. (1) nu este aplicabil atunci când este necesară păstrarea informațiilor secrete în vederea îndeplinirii scopului pentru care au fost introduse sau în vederea protejării intereselor altor persoane. Când se află în desfășurare supravegherea discretă potrivit art. 7, persoana vizată nu are dreptul la informare la datele înregistrate.

În situația în care o persoană solicită să fie informată dacă datele ce o privesc au fost introduse în sistem de un al stat, acel stat va avea ocazia de a-și exprima poziția înainte ca cererea să fie soluționată.

### **Art. 15**

Atunci când Comisarul Poliției Naționale din Islanda primește o cerere potrivit art. 13 sau 14, acesta va emite o poziție fără întârziere. Motivele deciziei comisarului vor fi oferite în măsura în care nu se dezvăluie orice informații ce ar trebui păstrate secrete.

## **6. Referințe principalele dispoziții naționale aplicabile**

Principalele acte normative aplicabile sunt: Legea nr. 16/2000 privind Sistemul de Informații Schengen în Islanda și Regulamentul nr. 110/2000 privind Sistemul de Informații Schengen în Islanda.

## **7. Regimul limbajului**

Deși nu e prevăzut în lege, islandeze este limba folosită în administrație în Islanda. Cu toate acestea, dacă o autoritate islandeză primește o solicitare în altă limbă, aceasta va primi un răspuns. Dacă solicitarea este transmisă de o persoană care nu poate înțelege răspunsul în islandeză (adică un cetățean străin), acesta va primi răspunsul într-o limbă pe care o înțelege.

Au fost tipărite și distribuite în Aeroportul Internațional Keflavik broșuri informative atât în engleză, cât și islandeză. Persoana vizată are dreptul de a primi informații într-o limbă pe care o înțelege.

## **XVI. ITALIA**

### **1. Natura dreptului de acces**

Accesul poate fi exercitat doar direct, prin transmiterea unei solicitări operatorului, Departamentul de Securitatea Publică din cadrul Ministerului de Interne.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

În temeiul ghidului oferit de Departamentul de Securitatea Publică, toate cererile de acces și verificare trebuie trimise la următoarea adresă:

Ministero dell'interno  
Dipartimento della pubblica sicurezza  
Ufficio coordinamento e pianificazione delle forze di polizia  
Divisione N.SIS  
Via di Torre di Mezza Via 9/121 - 00173 Roma

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Nu trebuie îndeplinite cerințe speciale pentru depunerea cererii (acestea pot fi transmise prin poștă sau fax) și nici nu se percepe vreo taxă. Exercițarea dreptului de acces este gratuită.

Cu toate că nu există cerințe exprese în legislația în vigoare cu privire la stabilirea identității solicitantului de acces la N-SIS, în vederea urgentării soluționarea unei astfel de plângeri, aceasta ar trebui întocmită pe cât posibil în italiană, engleză, franceză sau germană și **semnată de persoana vizată**, să conțină o scurtă descriere a temeiului cererii și însoțită de o **copie de pe cartea de identitate valabilă a persoanei vizate**.

### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

În situația în care persoana vizată nu este mulțumită de răspuns, poate înainta o plângere la Garante per la protezione dei dati personali la următoarea adresă:

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

Plângerile ar trebuie transmise preferabil prin poștă și nu prin fax, pentru a se asigura că toate documentele sunt lizibile. Acestea trebuie să conțină datele de contact ale petentului; dacă este posibil, și adresa acestuia pentru a facilita corespondența.

#### **5. Rezultatele cererilor de acces. Conținutul informațiilor**

În general, răspunsul trebuie transmis în termen de 30 de zile (nu neapărat cel final).

#### **6. Referințe principalele dispoziții naționale aplicabile**

Principalele legi aplicabile sunt următoarele:

- (a) Legea nr. 388 din 30 septembrie 1993 privind ratificarea și implementarea Acordului Schengen și Convenția de aplicare (vezi în special art. 9, 10, 11 și 12);
- (b) Decretul nr. 196/2003.

#### **7. Regimul limbajului**

Solicitarea ar trebui întocmită pe cât posibil în italiană, engleză, franceză sau germană.



## **XVII. LETONIA**

### **1. Natura dreptului de acces**

Orice persoană (cetățeni sau nu ai Statelor Membre în spațiul Schengen) are dreptul la acces direct la datele personale păstrate în SIS. (Acest lucru este stabilit prin Regulamentul Cabinetului de Miniștri nr. 622: „*Ordin privind modalitatea de solicitare de informații de către persoana vizată și modalitatea de primire a informațiilor privind datele stocate în Sistemul de Informații Schengen și în sistemul de informații SIRENE*”). Persoana vizată trebuie să primească un răspuns la solicitare în termen de 1 lună. Organismul competent să se pronunțe cu privire la orice recurs înainte de o persoană a cărei cerere de vizualizare a datelor personale care o privesc a fost fie refuzată fie nu a primit un răspuns este Inspectoratul de State privind Datele care este, de asemenea, competent să efectueze inspecții asupra punerii în aplicare a dreptului de rectificare a datelor incorecte sau de ștergere a datelor personale ilegale.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Solicitarea (în scris) pentru acces direct trebuie înaintată Poliției de State sau reprezentanților diplomatice și consulare ale Republicii Letonia.

#### **State Police**

Čiekurkalna 1.linija 1, k-4

Riga, LV-1026

Ph: +371 67075212; fax +371 67371227

e-mail: [kanc@vp.gov.lv](mailto:kanc@vp.gov.lv)

Datele de contact ale reprezentanțelor diplomatice și consulare ale Republicii Letonia sunt disponibile pe pagina web a Ministerului Afacerilor Externe (<http://www.mfa.gov.lv/en/mission/>).

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Cererile trebuie înaintate Poliției de Stat sau reprezentanțelor diplomatice și consulare ale Republicii Letonia personal sau electronic și trebuie să fie semnate și datate. La depunerea cererii personal, persoana vizată trebuie să facă dovada identității sale prin prezentarea unui document de identitate. Dacă solicitarea este transmisă electronic, trebuie să poarte o semnătură electronică sigură.

Cererea trebuie să conțină numele și prenumele persoanei vizate, data nașterii, codul numeric personal (dacă deține unul), locul nașterii, țara de origine, tipul (dacă este cazul) și numărului actului de identitate, denumirea autorității emițătoare, data emiterii și data expirării actului de identitate, informațiile solicitate (informații cu privire la persoana vizată, informații privind destinatarul datelor), modalitatea de primire a răspunsului (personal la oficiul Poliției de Stat sau a reprezentanțelor diplomatice și consulare sau indicarea unei adrese de corespondență).

Procedura este gratuită.

### **4. Rezultatele cererilor de acces. Conținutul informațiilor**

La primirea unei cereri de informații de la o persoană vizată, reprezentanții Poliției de Stat sau a reprezentanțelor diplomatice și consulare din Letonia verifică identitatea respectivei persoane prin transmiterea unei solicitări și a cererii inițiale la sub-unitatea Poliției de Stat – Biroul SIRENE din Letonia.

Biroul SIRENE efectuează verificările necesare în legătură cu cererea transmisă și, în termen de 1 lună, oferă un răspuns persoanei vizate sau refuză furnizarea informațiilor prin transmiterea unui răspuns la adresa sau la instituția indicată de persoana vizată – adresa la care trebuie transmis răspunsul sau la Poliția de Stat sau reprezentanțele diplomatice și consulare din Letonia

### **5. Referințe principalele dispoziții naționale aplicabile**

- Legea privind protecția datelor personale
- Legea privind operaționalizarea Sistemului de Informații Schengen
- Regulamentul Cabinetului de Miniștri nr. 622 (11.09.2007) „Ordin privind modalitatea de solicitare de informații de către persoana vizată și modalitatea de primire a informațiilor privind datele stocate în Sistemul de Informații Schengen și în sistemul de informații SIRENE”.

## **6. Regimul limbajului**

În ceea ce privește limba, potrivit Legii privind limba oficială în Republica Letonia, toate procedurile în fața autorităților din Letonia trebuie să fie în letonă, fiind aplicabilă și dreptului de acces la SIS. Totuși, Legea privind petițiile (art. 7 secțiunea 1 alin. (4)) menționează că petiția sau plângerea poate să nu primească răspuns dacă textul acesteia nu poate fi înțeles. Biroul SIRENE din Letonia a precizat că sunt luat în considerare și cererile transmise în engleză și rusă.

## **XVIII. LUXEMBURG**

### **1. Natura dreptului de acces**

Accesul este indirect, adică dreptul de acces poate fi exercitat prin autoritatea de supraveghere.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Autoritatea de supraveghere stabilită potrivit art. 17 din Legea din 2 august 2002 privind protecția persoanelor cu privire la prelucrarea datelor personale modificată prin Legea din 31 iulie 2006, Legea din 22 decembrie 2006 și Legea din 27 iulie 2007.

Parquet Général du Grand-Duché de Luxembourg

(Principal State Prosecutor's Office)

BP 15

L-2010 Luxembourg

Tel.: ++352 47 59 81-331

Fax: ++352 47 05 50

E-mail: [parquet.general@mj.etat.lu](mailto:parquet.general@mj.etat.lu)

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Legea din 2002 nu stabilește cerințe speciale pentru cereri.

Procedura este gratuită.

Potrivit art. 17 din Legea din 2002, autoritatea de supraveghere va efectua verificări și investigații corespunzătoare și stabilește rectificările necesare.

#### **4. Rezultatele cererilor de acces. Conținutul informațiilor**

Autoritatea de supraveghere va informa persoana vizată că prelucrarea în cauză nu conține date contrare tratatelor, legilor sau regulamentelor de implementare.

Nimic nu este dezvăluit cu privire la conținutul datelor solicitantului.

#### **5. Referințe principalele dispoziții naționale aplicabile**

Legea din 2 august 2002, modificată, privind protecția persoanelor cu privire la prelucrarea datelor personale.

Regulamentul Marelui Ducat de Luxemburg din 9 august 1993 ce autorizează stabilirea și utilizarea unei baze de date drept secțiunea națională a Sistemului de Informații Schengen (N.SIS) (regulamentul cu acoperă dreptul de acces).

#### **6. Regimul limbajului**

Persoana vizată poate iniția procedura privind dreptul de acces în următoarele limbi:

- luxemburgheză
- franceză
- germană
- engleză.

## **XIX. LIECHTENSTEIN**

### **1. Natura dreptului de acces**

Persoana vizată are dreptul de acces direct.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Landespolizei des Fürstentums Liechtenstein (National police)

Kommando

Gewerbeweg 4

Postfach 684

9490 Vaduz

FÜRSTENTUM LIECHTENSTEIN

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Cererea de acces trebuie înaintată în scris Poliției Naționale. Solicitantul trebuie să facă dovada identității sale. Dacă solicitarea nu este completată personal la Poliția Națională, solicitantul trebuie să ofere o copie certificată de pe pașaportul său.

### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

#### **Data Protection Office**

Kirchstrasse 8

Postfach 684

9490 Vaduz

Liechtenstein

Tel. +423 / 236 60 90

[info.dss@llv.li](mailto:info.dss@llv.li)

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

În general, un răspuns este oferit în termen de 30 de zile. În situația în care nu este furnizat un răspuns în termenul respectiv, solicitantul trebuie informat. Totuși, răspunsul trebuie oferit într-un termen ce nu trebuie să depășească 60 de zile de la data depunerii cererii.

## **6. Referințe principalele dispoziții naționale aplicabile**

Art. 11 și 12 din Legea pentru protecția datelor

Art. 34g din Legea privind Poliția Națională (LGBI. 1989 nr. 48)

Art. 47-19 din Ordonanța privind Sistemul de Informații Schengen și Biroul SIRENE (LGBI. 2011 nr. 140)

## **7. Regimul limbajului**

Solicitarea trebuie să fie în germană.

## **XX. LITUANIA**

### **1. Natura dreptului de acces**

Persoana vizată are drept de acces direct.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Cererile de acces, rectificare sau ștergere trebuie adresate Ministerului de Interne a Republicii Lituania, în calitatea sa de operator de date:

Ministry of the Interior of the Republic of Lithuania  
Šventaragio str. 2, LT-01510 Vilnius  
Lithuania  
Phone +370 5 271 7130, fax +370 5 271 8551  
Email [bendrasisd@vrm.lt](mailto:bendrasisd@vrm.lt)

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Cererile trebuie transmise în scris și trebuie semnate. Acestea trebuie să includă identitatea persoanei ce dorește să aibă acces la datele ce o privesc sau dorește rectificarea/ștergerea datelor (numele și prenumele, codul numeric personal (data nașterii dacă nu posedă un cod numeric personal), reședința, datele de contact (număr de telefon sau adresa de email)). Solicitantul trebuie să furnizeze operatorului un document prin care certifică identitatea sa. Exercițarea drepturilor este gratuită.

### **4. Rezultatele cererilor de acces. Conținutul informațiilor**

Persoana vizată are dreptul de a obține informații cu privire la sursele și tipul de date personale ce au fost colectate, scopul prelucrării acestora și destinatarii datelor către care sunt sau au fost dezvăluite datelor în ultimul an.



La primirea unei cereri de la persoana vizată privind prelucrarea datelor sale personale, operatorul trebuie să informeze individul dacă datele personale ce îl privesc au fost prelucrate și va dezvălui datele solicitate în termene de 30 de zile de la data primirii cererii (art. 25 din Legea privind protecția datelor personale).

În situația în care persoana vizată, după verificarea datelor sale personale, constată că acestea sunt incorecte, incomplete și inexacte și se adresează operatorului, acesta din urmă trebuie să verifice datele personale respectiv fără întârziere și la solicitarea scrisă a persoanei vizate depusă personal, prin poștă sau prin mijloace de comunicații electronice, acesta rectifică fără întârziere datele personale incorecte, incomplete și inexacte și (sau) suspendă prelucrarea acelor date personale, cu excepția stocării lor. În situația în care constată că datele personale sunt prelucrate ilegal și nedrept și se adresează operatorului, acesta din urmă verifică fără întârziere și gratuit legalitatea și corectitudinea prelucrării datelor personale și, la solicitarea scrisă a persoanei vizate, șterge datele personale colectate ilegal și pe nedrept sau suspendă prelucrarea acelor date personale, cu excepția stocării lor.

Operatorul trebuie să informeze, fără întârziere, persoana vizată și destinatarii datelor cu privire la rectificarea, ștergerea datelor personale sau suspendarea prelucrării datelor personale la solicitarea persoanei vizată (art. 26 din Legea privind protecția datelor personale).

Potrivit art. 23 alin. (2) din Legea privind protecția datelor personale, operatorul trebuie să prevadă condițiile de exercitarea a drepturilor de către persoana vizată, cu excepția situațiilor prevăzute de lege când este necesar să se asigure:

- 1) securitatea sau apărarea națională;
- 2) ordinea publică, prevenirea, cercetarea și reprimarea infracțiunilor;
- 3) interesele economice și financiare importante ale statului;
- 4) prevenirea, cercetarea și reprimarea încălcărilor eticii profesionale;
- 5) protecția drepturilor și libertăților persoanei vizate sau a altor persoane.

Persoanei vizate îi va fi refuzată cererea de informare cu privire la datele sale personale atunci când este necesar pentru îndeplinirea acțiunilor privind o alertă sau pentru protejarea drepturilor și libertăților unor persoane terțe. Informațiile privind datele personale nu trebuie dezvăluite persoanei vizate pe durata validității unei alerte privind supravegherea discretă.

Operatorul trebuie să motiveze refuzul de a soluționa cererea persoanei vizate. operatorul trebuie să informeze persoana vizată în termene de 30 de zile calendaristice de la data primirii cererii cu privire la refuzul de a furniza datele solicitate.

Regulamentul privind Sistemul Național de Informații Schengen din Lituania adoptate prin Ordinul din 17 septembrie 2007 al Ministrului de Interne al Republicii Lituania nr. 1V-324 prevede că, în situațiile în care alertele privind o persoană vizată au fost introduse de o altă parte contractantă, operatorul de date N.SIS nu trebuie să dezvăluie informațiile către persoana vizată cu privire la datele personale din SIS național fără autorizarea primită de la cealaltă parte contractantă ce a emis alerta de a furniza aceste date.

Ca răspuns la solicitarea scrisă a persoanei vizate de a rectifica datele personale incorecte, incomplete și inexacte, de a șterge datele personale prelucrate ilegal sau de a suspenda operațiunile de prelucrare a datelor personale, operatorul N.SIS trebuie să înainteze imediat cererea către instituția competentă a părții contractante, cu notificarea persoanei vizate. Atunci când autoritatea competentă a părții contractante a corectat datele incorecte sau inexacte, a actualizat datele incomplete, a distrus datele stocate ilegal sau a suspendat operațiunile de prelucrare a acestor date, operatorul N.SIS trebuie să informeze imediat persoana vizată și destinatarii datelor N.SIS către care au fost dezvăluite datele incorecte, inexacte sau incomplete.

## **5. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

State Data Protection Inspectorate  
A.Juozapavičiaus str. 6 , LT-09310 Vilnius  
Lithuania  
Phone +370 5 279 1445, fax +370 5 261 9494  
E-mail: [ada@ada.lt](mailto:ada@ada.lt)  
Internet: [www.ada.lt](http://www.ada.lt)

Atunci când persoana vizată nu este mulțumită de răspunsul primit de la operator sau operatorul refuză să răspundă la cererea de exercitare a dreptului de acces la datele personale care o privesc, de a solicita rectificarea sau ștergerea datelor personale sau suspendarea prelucrărilor ulterioare sau operatorul nu

răspunde în termen de 30 de zile calendaristice de la data primirii cererii, persoana vizată de poate adresa Inspectoratului de Stat pentru Protecția Datelor în termen de 3 luni de la primirea răspunsului de la operator sau în termen de 3 luni de la expirarea termenului de răspuns. Persoana vizată poate anexa documente (răspunsul operatorului la cererea sa etc.) când este cazul subliniind aspectele menționate în plângere, pentru a se asigura că aceasta din urmă este investigată în mod eficient.

După primirea plângerii, Inspectoratul de Stat pentru Protecția Datelor verifică legalitatea prelucrării datelor personale și decide asupra aspectelor semnalate prin plângere.

## **6. Referințe principalele dispoziții naționale aplicabile**

Legea privind protecția datelor personale

Regulamentul privind Sistemul Național de Informații Schengen din Lituania adoptate prin Ordinul din 17 septembrie 2007 al Ministrului de Interne al Republicii Lituania nr. 1V-324

## **7. Regimul limbajului**

Cererile de acces, rectificare sau ștergere trebuie transmise în limba oficială a statului (lituaniană). Cererile primite într-o altă limbă vor fi analizate potrivit procedurii generale. Dacă solicitarea este într-o altă limbă decât cea oficială a statului, aceasta trebuie tradusă în lituaniană. Răspunsul va fi transmis în limba oficială a statului (lituaniană).

Limba prevăzută de procedura de investigare a plângerii este lituaniană. Atunci când plângerea unei persoane vizate este transmisă Inspectoratului de Stat pentru Protecția Datelor în altă limbă, aceasta trebuie tradusă în lituaniană. Decizia cu privire la plângere va fi adoptată, iar răspunsul la plângere va fi în limba oficială a statului (lituaniană).

## **XXI. MALTA**

### **1. Natura dreptului de acces**

Persoana vizată are drept de acces direct.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Cererile de acces, rectificare sau ștergere trebuie înaintate autorității naționale competente la următoarea adresă:

Data Protection Officer  
Legal Unit  
Police Headquarters  
Floriana  
Tel: 21224001  
Email: [dpu.police@gov.mt](mailto:dpu.police@gov.mt)

### **3. Formalități pentru cereri**

În conformitatea cu legislația din Malta, cererea semnată trebuie transmisă în scris de persoana vizată. Cererea trebuie să fie în malteză sau engleză care sunt cele două limbi oficiale recunoscute de Constituția din Malta. Răspunsul trebuie furnizat în aceeași limbă ca cea folosită de persoana vizată la transmiterea cererii. Informațiile trebuie furnizate fără cheltuieli și fără întârziere.

### **4. Procedura**

Regulamentul și Decizia SIS II stabilesc că dreptul persoanelor de a solicita acces la datele personale introduse în Sistemul de Informații Schengen generația a IIa (SIS II) se exercită în conformitate cu legislația națională a autorității naționale competente către care a fost transmisă solicitarea.

După ce a depus o cerere, o persoană este îndreptățită să primească informațiile în scris în conformitate cu prevederile generale în domeniul protecției datelor conținute în Legea privind Protecția Datelor din Malta (cap. 440). Informațiile trebuie furnizate într-o formă clară cu privire la datele personale ce au fost prelucrate, sursa de colectare a informațiilor, scopul prelucrării și posibili destinatari ai datelor. Refuzul sau restricționarea dreptului de acces poate apărea atunci când este justificat pentru reprimarea infracțiunilor sau dacă este necesar pentru protecția persoanelor vizate sau a libertăților altor persoane. În eventualitatea unei restricții sau a unui refuz, persoana trebuie să fie informată în scris în legătură cu o asemenea decizie, inclusiv motivele ce stau la baza deciziei, cu excepția cazului în care o asemenea comunicare ar putea afecta o atribuție legală a poliției sau drepturile și libertățile altor persoane.

## **5. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Office of the Information and Data Protection Commissioner

2, Airways House,

High Street

Sliema.

Malta

Tel: +35623287100, fax: +35623287198

Email: [idpc.info@gov.mt](mailto:idpc.info@gov.mt)

Website: [www.idpc.gov.mt](http://www.idpc.gov.mt)

În situația unei restricții sau a unui refuz, persoana are dreptul de a depune o contestație la Comisarul pentru Informații și Protecția Datelor în termen de 30 de zile de la comunicarea deciziei către aceasta sau în situația în care persoana consideră în mod rezonabil că trebuie să aibă cunoștință de o asemenea decizie.

În vederea analizării contestației, Comisarul pentru Informații și Protecția Datelor trebuie să revizuiască decizia și trebuie să fie convins că restricția sau refuzul este întemeiat.

## **6. Referințe principalele dispoziții naționale aplicabile**

Instrumentele legale aplicabile sunt Legea privind protecția datelor (cap. 440) și Regulamentul S.L. 440.05 aplicabil prelucrărilor de date personale în sectorul polițienesc.

## **XXII. OLANDA**

### **1. Natura dreptului de acces**

Natura dreptului de acces în Olanda este direct. Legea privind datele poliției (Wet politiegegevens) este aplicabilă secțiunii naționale a Sistemului de Informații Schengen II (N.SIS). Dreptul de acces este prevăzut de art. 25 din Legea privind datele poliției. Orice persoană poate transmite în scris o cerere de acces la datele sale personale din SIS II prin trimiterea unei cereri la Ofițerul pe protecția datelor a Poliției Naționale din Olanda. În termen de 6 săptămâni de la primirea cererii de acces, trebuie comunicat un răspuns solicitantului. Răspunsul va conține comunicarea conținutului datelor, cu excepția situației de refuz a comunicării ar conduce la aplicarea art. 27 din Legea privind datele poliției. Comunicarea poate fi refuzată dacă este necesară pentru:

- a) exercitarea corespunzătoare a atribuțiilor polițienești;
- b) protejarea drepturilor persoanei vizate sau a drepturilor și libertăților terților;
- c) securitatea națională.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Cererile de acces trebuie transmise la:

Dutch National Police  
Central Unit, Intelligence division  
Attention of the Data Protection Officer  
PO Box 3016  
NL – 2700 KX Zoetermeer  
Tel.: ++31-79-345 9911  
Fax: ++31-79-345 90 10  
E-mail: [mailboxipoljz@klpd.politie.nl](mailto:mailboxipoljz@klpd.politie.nl)

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

La primirea unei cereri de informații, ofițerul pe protecția datelor contactează persoana vizată în legătură cu aranjamentele pentru soluționarea cererii. Trebuie furnizată o copie de pe actul de identitate

și, atunci când este cazul, o copie de pe împuternicirea de a reprezenta solicitantul. Se poate solicita achitarea unei taxe de 4.50 EUR pentru soluționarea cererilor, dar în practică nu se percepe o astfel de taxă.

Cererile privind alertele în baza Regulamentului SIS II vor fi redirecționate autorității responsabil pentru această categorie de alertă, Serviciul de Imigrare și Naturalizare (Immigratie en Naturalisatiedienst, IND) din cadrul Ministerului Securității și Justiției.

Cererile privind celelalte alerte vor fi soluționate de autoritățile competente (poliție).

Odată ce informațiile au fost obținute, se poate înainta o cerere de completare, rectificare sau ștergere a datelor.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

În cazul unei contestații cu privire la prelucrarea cererii, se poate înainta o solicitare de mediere la:

College Bescherming Persoonsgegevens

PO Box 93374

NL – 2509 AJ Den Haag

Tel.: ++31-70-8888500

Fax: ++31-70-8888501

E-mail: [info@cbpweb.nl](mailto:info@cbpweb.nl)

Internet: [www.cbpweb.nl](http://www.cbpweb.nl)

Cererea trebuie transmisă în termen de 6 săptămâni de la primirea informațiilor.

Cazurile în cererea a fost refuzată vor fi analizate în mod gratuit de Autoritatea pentru protecția datelor din Olanda (College Bescherming Persoonsgegevens, CBP). Ca și alternativă sau dacă prin mediere nu s-a ajuns la niciun rezultat, solicitarea poate fi înaintată instanței districtuale (secțiunea administrativă) în vederea analizării cazului și să decidă asupra lui.

## **5. Regimul limbajului**

Cererile de acces pot fi în scris, de preferat, în olandeză sau engleză, dar sunt acceptate și cele în franceză, germană sau spaniolă. Solicitanții ce folosesc o altă limbă ar trebuie să aibă în vedere timp suplimentar pentru traducere.



## **XXIII. NORVEGIA**

### **1. Natura dreptului de acces**

Dreptul de acces este direct.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Kriminalpolitisen  
(National Criminal Investigation Service NCIS)  
PO Box 8163 Dep.  
NO-0034 OSLO  
Tel.: ++47 23 20 80 00  
E-mail:  
Fax: + +47 23 20 88 80  
Internet: [www.kripos.no](http://www.kripos.no)

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Cererile de acces trebuie să fie semnate și transmise în scris. Răspunsul va fi transmis, fără întârziere, în scris și nu mai târziu de 30 de zile de la data primirii cererii.

### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Datatilsynet  
PO Box 8177 Dep.  
NO-0034 OSLO  
Tel.: +47 22 39 69 00  
Fax: + 47 22 42 23 50  
E-mail: [postkasse@datatilsynet.no](mailto:postkasse@datatilsynet.no)  
Internet: [www.datatilsynet.no](http://www.datatilsynet.no)

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Cererile de acces sunt soluționate în prima fază de administratorul de înregistrare (NSIS). Dacă acest pas a fost întreprins, se va înainta autorității care a solicitat introducerea cererea pentru o opinie. Ulterior aceasta va înainta solicitarea administratorului de înregistrare, însoțită de opinia sa.

Dacă nu se oferă acces deoarece solicitantul nu este înregistrat sau din cauza aplicabilității unor excepții prevăzute de Legea SIS (secțiunea 15), trebuie oferite, de fiecare dată, alte motive astfel încât să nu se indice faptul că datele ce nu pot fi dezvăluite sunt înregistrate.

## **6. Referințe principalele dispoziții naționale aplicabile**

Legea privind Sistemul de Informații Schengen (LOV 1999-07-16-66)

Reglementările privind Legea nr. 66 din 16 iulie 1999 privind Sistemul de Informații Schengen (reglementări SIS)

## **XXIV. POLONIA**

### **1. Natura dreptului de acces**

Dreptul de acces la informații este direct.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Potrivit Legii din 24 august 2007 privind participarea Republicii Polonia la Sistemul de Informații Schengen și Sistemul de Informații privind Vizele, operatorul de date din Polonia pentru Sistemul de Informații Schengen este Comandantul Poliției. Cererile de acces sau rectificarea datelor trebuie transmise acestuia.

Adresa de corespondență:  
General Headquarters of the Polish Police (KGP)  
Central Technical Authority KSI  
02-514 Warsaw  
148/150 Puławska Street  
Poland

Dacă este nevoie de consultare privind conținutul cererilor de acces la datele personale, este posibilă contactarea autorității telefonic sau prin adresa de poștă electronică:

tel.: +48 (22) 601-53-29  
tel.: +48 (22) 601-53-15  
e-mail: [cot.admin.ksi@policja.gov.pl](mailto:cot.admin.ksi@policja.gov.pl)

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Orice persoană are dreptul de a primi informații complete cu privire la datele personale ce o privesc și care sunt prelucrate în cadrul sistemelor de date.

În conformitate cu art. 32 (5) din Legea din 29 august 1997 privind protecția datelor personale (Monitorul Oficial din 2014, punctul 1182 cu modificări), persoana vizată își poate exercita dreptul de a obține informații o dată la 6 luni.

Solicitarea de acces este gratuită.

Potrivit art. 32 (1-5a) din Legea privind protecția datelor personale, persoana vizată poate solicita următoarele informații privind prelucrarea datelor personale:

- dacă datele există în sistem
- perioada de prelucrare a datelor
- sursa datelor
- perioada în care datele au fost disponibile
- scopul prelucrării datelor
- în ce măsură și cui au fost dezvăluite datele.

Operatorul va răspunde la cererea de informații în 30 de zile. Pentru a obține asemenea informații, trebuie transmisă o cerere în scris, în poloneză.

*Cererea de informații trebuie să includă:*

1. numele și prenumele solicitantului
2. numărul de identificare personală din Polonia – PESEL (atunci când este cazul)
3. naționalitatea
4. data și locul nașterii
5. copie de pe un document de identitate ce conține o fotografie clară
6. reședința (țara, orașul, strada și numărul casei/apartamentul)
7. subiectul cererii
8. semnătura solicitantului.

În conformitate cu art. 32 din Legea din 14 iunie 1960 privind Codul de procedură administrativă (Monitorul Oficial din 200, nr. 98, punctul 1071, cu modificările ulterioare), o parte poate fi reprezentată în procedurile administrative printr-o împuternicire, cu excepția cazului în care natura

activităților necesită o acțiune în persoană. Art. 33 din Cod stabilește regulile de procedură pentru împuternicirea avocațială, adică:

- împuternicitul poate fi o persoană fizică ce are capacitatea legală;
- împuternicirea avocațială trebuie notificată în scris;
- împuternicitul depune împuternicirea în original sau o copie certificată oficial a acesteia.

Avocatul, consilierul juridic sau intermediarul poate autentifica el însuși copia de pe împuternicirea oferită.

#### *Refuzul de a oferi informații cu privire la datele personale prelucrate*

Potrivit art. 30 din Legea privind protecția datelor personale, operatorul poate refuza accesul atunci când:

1. rezultatul dezvăluirii informațiilor constituie secret de stat,
2. presupune o amenințare la adresa securității sau apărării naționale, viața sau starea de sănătate umană sau siguranța și ordinii publice,
3. reprezintă o amenințare la adresa interesului economic sau financiar al statului,
4. duce la o încălcare substanțială a intereselor personale ale persoanelor vizate sau terților.

#### *Dreptul de intervenție asupra datelor, solicitare de suspendare a prelucrării sau de ștergere a datelor*

Persoana vizată poate solicita operatorului să completeze, actualizeze, corecteze, elimine sau să suspende temporar sau permanent prelucrarea datelor care o privesc. Cu toate acestea, persoana vizată trebuie să demonstreze că datele sunt incomplete, depășite, inexacte, că au fost colectate prin încălcarea legii sau că prelucrarea datelor nu mai este necesară pentru atingerea scopului pentru care au fost colectate. Procedurile de aplicare sunt efectuate în conformitate cu prevederile Codului de procedură administrativă.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Pentru a oferi un nivel adecvat de protecție legală a persoanelor ale căror date sunt stocate în Sistemul de Informații Schengen, Inspectorul General pentru Protecția Datelor Personale monitorizează dacă utilizarea datelor încalcă drepturile persoanelor vizate. Această supraveghere se exercită în conformitate cu legislația privind protecția datelor personale.

Adresa de corespondență:

Bureau of the Inspector General for Personal Data Protection (GIODO)

2 Stawki Street

00-193 Warsaw

Poland

tel. +48 (22) 860-73-93

fax +48 (22) 860-70-86

<http://www.giodo.gov.pl>

[kancelaria@giodo.gov.pl](mailto:kancelaria@giodo.gov.pl)

Orice persoană ale cărei date sunt prelucrate în Sistemul de Informații Schengen este îndreptățită să înainteze o plângere la Inspectorul General pentru Protecția Datelor Personale în legătură cu implementarea prevederilor privind protecția datelor cu caracter personal.

#### **5. Referințe principalele dispoziții naționale aplicabile**

- Legea din 24 august 2007 privind participarea Poloniei la Sistemul de Informații Schengen și Sistemul de Informații privind Vizele,
- Legea din 29 august 1997 privind protecția datelor cu caracter personal
- Legea din 14 iunie 1960 privind Codul de procedură administrativă
- Legea din 7 octombrie 1999 privind limba poloneză

## XXV. PORTUGAL

### 1. Natura dreptului de acces

Dreptul de acces, corectare și ștergere a datelor personale prelucrate în SIS II se exercită indirect, prin intermediul autorității naționale pentru protecția datelor – CNPD.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Comissão Nacional de Protecção de Dados – CNPD

Rua de S. Bento, 148, 3º

1200-821 Lisboa

[www.cnpd.pt](http://www.cnpd.pt)

**Front Office - Privacy Line:** (00.351) 393 00 39 (Mondays to Fridays, from 10-13h GMT)

**Personal attendance:** Mondays to Fridays, from 14.30 – 16.30h (GMT)

### 3. Formalități pentru cereri: informații și documente furnizate – posibile costuri

Solicitările trebuie transmise în scris prin utilizarea unui dintre cele 3 formulare specifice, fie pentru dreptul de acces, pentru dreptul de intervenție fie pentru dreptul de ștergere. Aceste formulare sunt disponibile pe site-ul autorității pentru protecția datelor în portugheză, engleză și franceză. Cererile pot fi depuse în persoană la registratura autorității pentru protecția datelor sau prin poșta electronică. Solicitanții trebuie să prezinte un document de identificare (pașaport sau carte de identitate pentru cetățenii portughezi). Dacă solicitările sunt transmise prin poșta electronică, trebuie să se atașeze formularul în clar, precum și o copie de pe pașaport sau cartea de identitate. Cererile sunt gratuite.

### 4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil

Datele de contact ale CNPD sunt prezentate la punctul 2.

Toate informațiile privind drepturile persoanelor în legătură cu Sistemul de Informații Schengen sunt disponibile în PT, EN și FR pe pagina web a autorității pentru protecția datelor.

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Autoritatea pentru protecția datelor efectuează toate diligențele în relația cu autoritățile competente Schengen și oferă un răspuns solicitantului cât mai curând posibili și, în orice caz, nu mai târziu de 30 de zile de la primirea cererilor de acces. Pentru cererile de corectare și ștergere, autoritatea pentru protecția datelor, în situația în care nu poate oferi un răspuns final, va informa solicitantul în termen de 90 de zile de la primirea cererii.

## **6. Referințe principalele dispoziții naționale aplicabile**

Legea nr. 67/98 din 26 octombrie (art. 11) – Legea privind protecția datelor

## **7. Regimul limbajului**

Cererile trebuie transmise în portugheză, iar documentele anexate trebuie traduse în portugheză. Biroul registratură va oferi sprijin în soluționarea cererii, după caz.



## **XXVI. ROMANIA**

### **1. Natura dreptului de acces**

În România dreptul de acces este direct.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Potrivit art. 62(3) din Legea nr. 141/2010 privind înființarea, organizarea și funcționarea Sistemului Informatic Național de Semnalări și participarea României la Sistemul de Informații Schengen, cererile se pot depune la Biroul SIRENE național sau la orice operator din cadrul Ministerului Afacerilor Interne ori al unei structuri teritoriale a acestuia, care transmite cererea Biroului SIRENE național, în termen de 5 zile de la data primirii acesteia.

Adresa de corespondență:

Centrul de Cooperare Polițienească Internațională

Biroul SIRENE

1-5 Calea 13 Septembrie, București, sectorul 5

România

Tel.: +40 21 315 96 26

Tel.: +40 21 314 05 40

Fax: +40 21 314 12 66

Fax: +40 21 312 36 00

E-mail: [ccpi@mai.gov.ro](mailto:ccpi@mai.gov.ro)

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Drepturile persoanei vizate în contextul prelucrării datelor cu caracter personal în SINS sau în SIS se exercită potrivit prevederilor Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare, cu derogările prevăzute de prezenta lege.

Potrivit art. 13 (1) din Legea nr. 677/2001, *solicitarea de acces la date este gratuită.*

Persoanei vizate nu îi sunt comunicate informațiile privind prelucrarea datelor cu caracter personal în SINS sau în SIS atât timp cât acest lucru este indispensabil pentru realizarea acțiunilor în baza semnalării ori a obiectivului semnalării sau pentru apărarea drepturilor și libertăților altor persoane.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Legalitatea prelucrării datelor cu caracter personal în N.SIS pe teritoriul României și transmiterea acestor date în străinătate, precum și schimbul și procesarea ulterioară a informațiilor suplimentare sunt monitorizate și se supun controlului A.N.S.P.D.C.P.

Auditarea operațiunilor de prelucrare a datelor cu caracter personal în N.SIS se efectuează de către A.N.S.P.D.C.P., în conformitate cu standardele internaționale de audit, cel puțin o dată la 4 ani.

Adresa de corespondență:

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

Bd. G-ral Gheorghe Magheru nr. 28-30

Sector 1, București

România

Tel.: +40 31 805 92 11

Fax: +40 31 805 96 02

E-mail: [anspdcp@dataprotection.ro](mailto:anspdcp@dataprotection.ro)

#### **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Cererile persoanelor vizate în contextul prelucrării datelor cu caracter personal în SINS sau în SIS se adresează numai Biroului SIRENE național, care răspunde solicitantului cât mai curând posibil, dar nu mai târziu de 60 de zile de la data primirii cererii, în cazul exercitării dreptului de acces la datele personale, și cât mai curând posibil, dar nu mai târziu de 90 de zile de la data primirii cererii, în cazul exercitării dreptului de rectificare și ștergere a datelor personale, prin derogare de la prevederile Legii nr. 677/2001, cu modificările și completările ulterioare.

## **6. Referințe principalele dispoziții naționale aplicabile**

- Legea nr. 141 din 12 iulie 2010 privind înființarea, organizarea și funcționarea Sistemului Informatic Național de Semnalări și participarea României la Sistemul de Informații Schengen
- Legea nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

## **7. Regimul limbajului**

Persoana vizată, cetățean român, poate transmite solicitarea în limba română, iar cetățenii străini pot transmite solicitarea în engleză.

## XXVII. SLOVACIA

### 1. Natura dreptului de acces

Potrivit art. 41 din Regulamentul SIS II și art. 58 din Decizia SIS II, orice persoană are dreptul de acces la datele care o privesc introduse în Sistemul de Informații Schengen generația a IIa (SIS). Acest drept se exercită în conformitate cu legislația națională a părții contractante. În situația Slovaciei, persoana vizată a dreptului de acces direct.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Cererile de acces trebuie înaintate Ministerului de Interne, în calitate de operator:

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

Pribinova 2, 812 72 Bratislava

Slovenská republika

Phone: 02/5094 1111

Fax: 02/5094 4397

Internet: <http://www.minv.sk>

### 3. Formalități pentru cereri: informații și documente furnizate – posibile costuri

Potrivit art. 69c din Legea nr. 171/1993 privind forțele de poliție, orice persoană are dreptul de a solicita, în scris, Ministerului de Interne de a furniza ce date personale ce o privesc sunt prelucrate. În același timp, operatorul Sistemului de Informații Schengen este obligată să furnizeze informațiile în mod gratuit, în termen de 30 de zile de la data primirii **solicitării în scris**.

Formularul standard de solicitare pentru cererea de mai sus este disponibil pe site-ul Ministerului de Interne.

Persoana în cauză este obligată să furnizeze datele sale personale (numele, prenumele, domiciliul, locul și data completa de naștere și naționalitatea), precum și o copie de pe cartea de identitate sau pașaport pentru a dovedi identitatea sa.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Furnizarea de date cu caracter personal solicitantului din informații din sistemele operate de poliție este efectuată în conformitate cu art. 69c din Legea nr. 171/1993 privind forțele de poliție.

În ceea ce privește Sistemul de Informații Schengen II, dacă alerta a fost emisă potrivit art. 26-34 și art. 38 din Decizia SIS II, solicitantul va fi informat cu privire la datele ce-l privesc (cel puțin următoarele informații: nume, prenume, data și locul nașterii, sexul, naționalitatea și motivul alertei, adică scopul prelucrării datelor sale personale).

Atunci când dreptul de acces la informații se referă la o alertă ce nu a fost introdusă de Slovacia, statul emitent trebuie să aibă posibilitatea de a-și exprima poziția cu privire la posibilitatea de dezvoltare a datelor către solicitant.

Dacă alerta a fost emisă în baza art. 36 din Decizia SIS II, cel mai probabil solicitantului îi va fi refuzată dezvoltarea datelor (prelucrarea a fost efectuată pe motiv de securitatea națională sau pentru investigarea anumitor infracțiuni grave).

Cu alte cuvinte, comunicarea de informații către persoana vizată va fi refuzată dacă este necesar pentru îndeplinirea unei atribuții legale în legătură cu alerta sau pentru protejarea drepturilor și libertăților terților. În orice caz, trebuie refuzată pe perioada validității unei alerte în scop de supraveghere discretă.

Potrivit art. 69c din Legea nr. 171/1993 privind forțele de poliție, persoana vizată are dreptul de a **solicita în scris** Ministerului de Interne corectarea sau ștergerea datelor sale personale prelucrate în Sistemul de Informații Schengen (formularul standard privind cererea de ștergere/corectare a datelor este disponibil pe pagina web a Ministerului de Interne).

În situația în care persoana vizată suspectează că datele sale personale sunt prelucrate fără autorizare, potrivit art. 20 alin. (6) din Legea privind protecția datelor, poate înainta o **plângere** direct la Oficiul pentru Protecția Datelor din Slovacia care va verifica dacă există vreo încălcare a drepturilor persoanei vizate în cadrul prelucrării și utilizării datelor personale ale persoanei vizate păstrate în Sistemul de Informații Schengen II.

Înaintarea plângerilor este reglementată de prevederile Secțiunii 63 din Legea nr. 122/2013 privind protecția datelor personale...(Formularul standard pentru depunerea unei plângeri este disponibil, de asemenea, pe pagina web a Ministerului de Interne).

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Úrad na ochranu osobných údajov Slovenskej republiky  
(Office for Personal Data Protection of the Slovak Republic)

Hraničná 12

827 07 Bratislava 27

Slovenská republika

Tel: +421 2 32 31 32 14

Fax: 421 2 32 31 32 34

e-mail: [statny.dozor@pdp.gov.sk](mailto:statny.dozor@pdp.gov.sk)

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

## **6. Referințe principalele dispoziții naționale aplicabile**

Legea nr. 122/2013 privind protecția datelor și pentru modificarea și completarea altor acte normative precum completarea Legii nr. 84/2014.

## XXVIII. SLOVENIA

### 1. Natura dreptului de acces

Există un drept de acces direct.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Solicitările pot fi depuse în scris sau verbal la poliție (Ministerul de Interne). Adresa este următoarea:

Policija, Ministrstvo za notranje zadeve

Štefanova 2

1501 Ljubljana

Slovenia

Fax: + 386 1 428 47 33

E-mail: [gp.mnz@gov.si](mailto:gp.mnz@gov.si)

Solicitările pot fi depuse și la punctele de trecere a frontierei, unitățile administrative și misiunile diplomatice sau oficiile consulare ale Sloveniei. Acestea sunt înaintate imediat poliției.

Link-ul către formularul de Solicitare de Informații privind Datele din Sistemul Național de Informații Schengen în Slovenia (N.SIS), care poate fi descărcat în engleză:

<http://www.ip-rs.si/index.php?id=346>

### 3. Formalități pentru cereri: informații și documente furnizate – posibile costuri

În Slovenia, procedura de exercitare a dreptului de consultare a propriilor date personale este reglementată în conformitate cu legea privind protecția datelor personale (art. 30 și 31) și legea privind Comisarul pentru Informații.

Art. 30 din legea privind protecția datelor personale solicită poliție, care se subordonează Ministerului de Interne și care e operator de date, să:

1. permită consultarea sistemului SIS;
2. certifice dacă datele referitoare la persoana vizată sunt prelucrate sau nu și să permită consultarea datelor personale conținute în sistemul național SIS referitoare la aceasta, precum și să transcrie sau să copieze datele personale;
3. furnizeze un rezumat al datelor personale ce o privesc conținute în sistemul național SIS;
4. ofere o listă a destinatarilor datelor, menționând temeiul și scopul transmiterii;
5. ofere informații cu privire la sursele pe care se bazează evidențele privind o persoană fizică ce apare în SIS, precum și metoda de prelucrare;
6. ofere informații privind scopul prelucrării și tipul datelor personale prelucrate în SIS, precum și toate explicațiile necesare în acest sens;
7. explice procedurile tehnice și logic-tehnice de luare a deciziilor.

Prelucrarea solicitărilor este în prezent gratuită. Solicitantului i se pot percepe costuri numai pentru materialele folosite pentru fotocopiere conform Regulilor de tarifare a costurilor legate de exercitarea dreptului de acces la propriile date.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Informacijski pooblaščenec  
(Information Commissioner)

Zaloska 59

1000 Ljubljana

Slovenia

Tel.: ++ 386 1 230 97 30

Fax: ++ 386 1 230 97 78

E-mail: [gp.ip@ip-rs.si](mailto:gp.ip@ip-rs.si)

Internet: [www.ip-rs.si](http://www.ip-rs.si)



Comisarul pentru Informații este competent pentru decizia asupra contestației unei persoane atunci când o solicitare de consultare a datelor sale personale a fost refuzată sau autoritatea competentă a refuzat să răspundă la solicitare.

Solicitanții care consideră că oricare dintre drepturile lor a fost încălcat în ceea ce privește o cerere de acces, aceștia pot depune o plângere la Comisarul pentru Informații. Comisarul pentru Informații, după ce a primit plângerea, o redirecționează operatorului astfel încât să poată menționa ceea ce acesta consideră a fi relevant. În cele din urmă, Comisarul pentru Informații ia o decizie cu privire la plângere, după ce a primit observațiile și rapoartele, dovezile și alte documente de anchetă, precum și după consultarea dosarelor, acolo unde este necesar și după realizarea interviurilor cu persoana vizată și operator, și o înaintează persoanelor vizate.

Procedura de contestare este în prezent gratuită.

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Dacă datele referitoare la o persoană se regăsesc în sistemul SIS și dacă solicitarea este primită, operatorul va furniza persoanei vizate datele care o privesc în formatul solicitat. Poliția trebuie să permită persoanei să consulte, transcrie, copieze și să obțină un certificat nu mai târziu de 15 zile de la data primirii cererii sau, în același interval, să informeze în scris persoana vizată cu privire la motivele ce au stat la baza refuzului. Poliția este obligată să ofere persoanei vizate în termen de 30 de zile de la primirea cererii informațiile menționate mai sus la punctul 3, lista de la punctul 4, informațiile de la punctele 5 și 6 și explicațiile de la punctul 7 sau, în același interval, să informeze în scris cu privire la motivele refuzului.

De asemenea, dreptul persoanei de a consulta datele personale care o privesc poate fi, de asemenea, în mod excepțional, limitat în conformitate cu art. 36 din Legea privind protecția datelor personale, din motive de protecție a suveranității naționale și apărării naționale, protecția securității naționale și ordinii constituționale a statului, securitate, interesele politice și economice ale statului, îndeplinirea atribuțiilor de poliție, prevenire, constare, detectare, cercetarea și urmărirea penală a infracțiunilor și contravențiilor, constatarea și pedepsirea încălcării normelor etice pentru anumite profesii, din motive monetare, bugetare sau fiscale, supravegherea de către poliție și protecția persoanei la care se referă

datele personale sau a drepturilor și libertăților altor persoane. Aceste restricții pot fi impuse numai în măsura în care sunt necesare pentru atingerea scopului pentru care a fost instaurată restricția.

## **6. Referințe principalele dispoziții naționale aplicabile**

- Legea privind protecția datelor personale (Monitorul Oficial al Sloveniei nr. 94/2007, textul oficial consolidat), traducerea neoficială în engleză a legii este disponibilă la: <http://www.ip-rs.si/index.php?id=339>;
- Legea Comisarului pentru Informații (Monitorul Oficial al Slovenie nr. 113/2005), traducerea neoficială în engleză a legii este disponibilă la: <http://www.ip-rs.si/index.php?id=325>;
- Regulilor de tarifare a costurilor legate de exercitarea dreptului de acces la propriile date (Monitorul Oficial al Sloveniei nr. 85/2007), este disponibil doar textul în limba slovenă al regulilor: <http://www.ip-rs.si/zakonodaja/zakon-o-varstvu-osebni-podatkov/pravilnik-o-zaracunavanju-stroskov-pri-izvrsevanju-pravice-posameznika-doseznanitve-z-lastnimi-osebni-podatki/>.

## **XXIX. SPANIA**

### **1. Natura dreptului de acces**

Persoanele vizate au drept de acces direct, dar, atunci când operatorul nu dă curs solicitării de acces sau când persoana vizată nu este mulțumită de răspuns, acestea au acces indirect prin intermediul Autorității pentru Protecția Datelor din Spania.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Cererile de acces la informații trebuie transmise la:

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

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Orice solicitare de acces trebuie transmisă în scris operatorului. În acest scop, persoanele vizate trebuie să transmită o solicitare operatorului prin orice mijloc ce oferă dovada expedierii și primirii cererii.

Nu există un formular oficial standard sau alte cerințe formale. Totuși, urmare a procedurii administrative generale, solicitarea trebuie să conțină o descriere completă a cererii și trebuie să fie însoțită de o fotocopie de pe un document ce dovedește identitatea persoanei vizate – adică cartea de identitate națională sau pașaport. În plus, persoanele vizate pot atașa la solicitare copii de pe documentele relevante pe care le consideră importante în susținerea cererii descrisă în solicitare.

Procedura este gratuită.

#### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Agencia Española de Protección de Datos (Data Protection Authority)

C/ Jorge Juan, 6

E - 28001 – Madrid

Tel.: + 34 901 100 099

Fax: + 34 91 445 56 99

E-mail: [ciudadano@agpd.es](mailto:ciudadano@agpd.es)

Internet: [www.agpd.es](http://www.agpd.es)

Așa cum a fost menționat, persoanele vizate au drept de acces direct. Cu toate acestea, au și acces indirect prin intermediul Autorității pentru Protecția Datelor din Spania (denumită în continuare DPA Spania) în situația în care un operator nu răspunde solicitării de acces înaintată de o persoană vizată sau când răspunsul transmis este nesatisfăcător. În ambele situații persoanele vizate pot înainta o cerere la DPA Spania. Potrivit secțiunii 117 din Decretul Regal nr. 1720/2007 prin care sunt aprobate normele de implementare a Legii organice nr. 15/1999 privind protecția datelor cu caracter personal, procedura trebuie inițiată la solicitarea persoanei vizate, ce își exprimă în mod clar cererea și prevederile din actul normativ pe protecția datelor menționat anterior ce au fost încălcate.

Odată ce DPA Spania primit solicitarea, procedura de protejare a drepturilor persoanelor trebuie inițiată. Potrivit acestei proceduri, DPA Spania redirecționează solicitarea către operator pentru a-i oferi posibilitatea de a depune orice dovezi pe care le consideră relevante în vederea sprijinirii deciziei de a refuza accesul sau în vederea susținerii răspunsului oferit solicitantului.

Aceste comentarii, dacă este cazul, sunt transmise solicitantului care poate emite declarații sau comentarii. Acestea din urmă sunt transmise operatorului care are posibilitatea de a oferi explicații privind decizia sa și de a răspunde la comentariile și declarații solicitantului.

După primirea declarațiilor și documentelor, Directorul DPA Spania ia o decizia în vederea soluționării cererii primite.

Este important de subliniat faptul că perioada de timp pentru emiterea și notificarea deciziei este de 6 luni de la data primirii solicitării de către DPA Spania.

Dacă decizia este în favoarea solicitantului, DPA Spania comunică acest aspect operatorului care trebuie să acceseze persoanei vizate dreptul de acces în termen de 10 zile de la data înștiințării. Mai mult, operatorul este obligat să ofere în scris autorității de supraveghere dovada respectării deciziei DPA Spania în același termen.

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Dacă alerta a fost emisă de autoritățile spaniole, atunci este de competența operatorului să decidă conținutul informațiilor furnizate solicitanților. De obicei, persoana vizată primește copii de pe documentele administrative ce conțin date personale stocate în sistem.

Totuși, dacă alerta a fost emisă de autoritățile unui alt stat Schengen, operatorul trebuie să informeze omologul său din statul de a primit solicitarea, în conformitate cu principiul cooperării dintre autoritățile naționale pentru protecția datelor. Autoritățile din celelalte state Schengen decid ce informații pot fi furnizate persoanei vizate.

## **6. Regimul limbajului**

Persoana vizată ce dorește să inițieze o procedură pentru dreptul de acces în Spania trebuie să se adreseze organismelor publice din Spania.

## **7. Formulare**

DPA Spania oferă prin intermediul pagii sale web un formular standard neoficial (în spaniolă) pentru exercitarea dreptului de acces ce poate fi folosit de persoana vizată când dorește. Formularul poate fi găsit la:

[http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/derecho\\_schengen\\_den/common/DERECHO\\_DE\\_ACCESO\\_Schengen\\_Es.pdf](http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/derecho_schengen_den/common/DERECHO_DE_ACCESO_Schengen_Es.pdf).

Persoanele vizate ce doresc să depună la DPA Spania o cerere referitoare la dreptul de la acces pot folosi următorul link (doar în spaniolă): <https://sedeagpd.gob.es/sede-electronica-web/vistas/formReclamacionDerechos/tipoSolicitud/solicitudPresencial.jsf>

## **XXX. SUECIA**

### **1. Natura dreptului de acces**

Există un drept de acces direct.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Cererile de acces trebuie transmise Autorității polițienești din Suedia (Polismyndigheten) care este autoritatea responsabilă pentru unitatea suedeză a Sistemului de Informații Schengen.

Polismyndigheten

Box 12256

Polhemsgatan 30

S - 102 26 Stockholm

Tel: ++46 77-114 14 00

E-mail: [registrator.kansli@polisen.se](mailto:registrator.kansli@polisen.se)

Internet: [www.polisen.se](http://www.polisen.se)

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Cererile trebuie transmise în scris Autorității polițienești din Suedia și semnate în persoană de solicitant. La cerere trebuie atașată o copie de pe cartea de identitate națională sau pașaport. În general, o cerere de acces trebuie să primească răspuns în termen de 1 lună. O dată pe anul calendaristic, solicitanții beneficiază de acces gratuit.

### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Datainspektionen

Box 8114

Drottninggatan 29, 5th floor

S - 104 20 Stockholm

Tel.: ++46 (0)8-657 61 00

Fax: ++46 (0)8-652 86 52

E-mail.: [datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se)

Internet: [www.datainspektionen.se](http://www.datainspektionen.se)

Consiliul privind Protecția Datelor se asigură că prelucrarea datelor personale în Suedia se realizează în conformitate cu Legea privind Protecția Datelor și alte acte normative privind protecția datelor. Consiliul poate iniția verificări pe baza unei plângeri sau din oficiu. O persoană ce nu este mulțumită de modalitatea de soluționare a solicitării de acces la informațiile din SIS se poate adresa cu o plângere la Consiliul privind Protecția Datelor. Plângerea poate conduce la o investigație privind respectarea normelor referitoare la dreptul de acces. Decizia Autorității polițienești din Suedia referitoare la dreptul de acces poate totuși să fie contestată la instanța administrativă.

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Dezvăluirea sau nu a datelor depinde de prevederile din Legea privind documentele și secretele oficiale (2009:400) care poate interzice dezvăluirea anumitor date. Atunci când este permisă dezvăluirea, Autoritatea polițienească din Suedia este responsabilă cu transmiterea acestora.

## **6. Referințe principalele dispoziții naționale aplicabile**

Legea aplicabilă: Secțiunile 26 și 27 din Legea privind Protecția Datelor (1998:204), Secțiunea 8 din Legea privind Sistemul de Informații Schengen (2000:344) și Secțiunea 21 din reglementarea privind Sistemul de Informații Schengen (2000:836).

## **7. Regimul limbajului**

Nu există reguli specifice privind acest aspect în Suedia. Se acceptă și cererea în engleză.



## **XXXI. ELVEȚIA**

### **1. Natura dreptului de acces**

Există un drept de acces direct. Autoritatea competentă ce prelucrează solicitările persoanelor cu privire la dreptul de acces la datele personale din SIS este Ofițerul pe Protecția Datelor din cadrul Oficiului Federal de Poliție din Elveția.

### **2. Datele de contact ale organismului către care trebuie înaintate cererile de acces**

Federal Office of Police (fedpol)  
Legal department/ Data protection  
Data Protection adviser  
Nussbaumstrasse 29  
CH-3003 Berne  
[www.fedpol.ch](http://www.fedpol.ch)

### **3. Formalități pentru cereri: informații și documente furnizate – posibile costuri**

Cererile persoanelor privind datele personale care le privesc prelucrate în SIS trebuie înaintate direct Oficiului Federal de Poliție, operatorul sistemului SIS din Elveția. De obicei, cererile trebuie transmise în scris, atașând o copie de pe cartea de identitate sau pașaportul valid și împuternicirea avocațială în situația în care persoana este reprezentată. Dacă solicitarea este transmisă prin poșta electronică, persoana trebuie să menționeze adresa poștală și să anexeze o copie de pe cartea de identitate sau pașaportul valid.

### **4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil**

Federal Data Protection and Information Commissioner (FDPIC)  
Feldeggweg 1,  
CH-3003 Berne  
Phone: +41(0)31 322 43 95, Fax +41-(0)31 325 99 96  
<http://www.edoeb.admin.ch/index.html?lang=en>

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Potrivit art. 50 (4) din Ordonanța privind Secțiunea Națională a Sistemului de Informații Schengen (N-SIS) și Biroul SIRENE (Ordonanța N-SIS), persoana vizată va fi informată în termen de 30 de zile de la primirea cererii de acces. Dacă nu se poate realiza informare în acest termen, persoana trebuie informată în legătură cu această întârziere. Termenul limită de informare a persoanei este de 60 de zile de la primirea cererii. Dacă nu există niciun motiv de refuz, persoana va fi pe deplin informată.

Potrivit art. 50 (5) din Ordonanța N-SIS, persoana vizată va fi informată în termen de 3 luni de la data primirii cererii de corectare sau ștergere.

Dreptul de a fi informat în cazul unei decizii de non-admisibilitate este reglementat de art. 51 din Ordonanța N-SIS.

## **6. Referințe principalele dispoziții naționale aplicabile**

- Legea Federală din 19 iunie 1992 privind protecția datelor (FADP; RS. 235.1)
- Ordonanța din 14 iunie 1993 privind Legea Federală privind protecția datelor (OFADP; RS. 235.1)
- Ordonanța privind Secțiunea Națională din Sistemul de Informații Schengen (N-SIS) și Biroul SIRENE (Ordonanța N-SIS; RS. 362.0)

## **7. Regimul limbajului**

Cererile pot fi transmise în franceză, germană, italiană sau engleză.

## XXXII. REGATUL UNIT

### 1. Natura dreptului de acces

În UK dreptul de acces este direct – atunci când persoana se poate adresa direct autorităților ce folosesc datele adică forțele de poliție locale. Ulterior, cererile vor fi redirecționate către *ACRO Criminal Records Office (ACRO)* pentru soluționare. În mod alternativ, persoana se poate adresa direct ACRO.

### 2. Datele de contact ale organismului către care trebuie înaintate cererile de acces

Cererile de acces vor fi înaintate direct *ACRO Criminal Records Office*:

[https://www.acro.police.uk/subject\\_access.aspx](https://www.acro.police.uk/subject_access.aspx) sau în scris la:

ACRO (SAR)

PO Box 662

FAREHAM

PO14 9LQ

### 3. Formalități pentru cereri: informații și documente furnizate – posibile costuri

Pentru cererile de acces se percepe o taxă națională de £10 GBP în conformitate cu procedura Cererea de Acces a Solicitantului. Persoanele vizate trebuie să completeze un formular în care să se evidențieze clar numele persoanei, data nașterii, adresa poștală actuală și semnătura și să atașeze două dovezi oficiale a identității lor.

### 4. Datele de contact ale autorității naționale pentru protecția datelor și rolul său posibil

Information Commissioner's Office

Wycliffe House Water Lane

Wilmslow

Cheshire

SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 sau dacă preferați să utilizați numărul național

Fax: 01625 524 510

Email: [casework@ico.org.uk](mailto:casework@ico.org.uk) (vă rugăm să indicați numărul dvs. de telefon)

Dacă depuneți o plângere la ICO cu privire la soluționarea cererii de acces, ICO va utiliza toate informațiile pe care le-ați furnizat, inclusiv răspunsul entității, pentru a decide dacă îngrijorarea dvs. oferă o oportunitate de a îmbunătăți practica referitoare la informarea cu privire la drepturi. În situația în care considerăm că este o oportunitate, vor lua măsurile corespunzătoare. Acest lucru ar putea avea o varietate de forme. ICO nu va investiga, de obicei, aspecte care au fost aduse cu întârziere în atenția noastră. Trebuie să ne contactați în termen de 3 luni de la ultimul contact semnificativ cu organizația implicată.

## **5. Rezultatele cererilor de acces. Conținutul informațiilor**

Răspunsul la cererea de acces trebuie oferit persoanei vizate în termen de 40 de zile calendaristice de la data primirii solicitării. Secțiunile 28 și 29 din Legea privind Protecția Datelor acoperă regulile specifice de excepție de ne-dezvăluire a informațiilor în cadrul unui răspuns.

## **6. Referințe principalele dispoziții naționale aplicabile**

UK introduce alerte potrivit prelucrărilor interne și *Legii privind Protecția Datelor din 1998*. Alertele străine sunt reglementate de obligațiile prelucrării transfrontaliere (protocolul 36 din Regulamentul 28) – *Partea 4 din Regulamentul 2014 privind justiția penală și protecția datelor (Protocolul nr. 36)*

## **7. Regimul limbajului**

Toate răspunsurile la cererile de acces vor fi în engleză.

## ANEXE (MODELE DE CERERI)

*Următoarele modele de cereri pot fi utilizate pentru a înainta o cerere cu excepția cazului în care autoritatea națională competentă la care ați depus cerere solicită utilizarea unui formular standard specific.*

Anexa 1

### Model cerere solicitare acces

Către: **Denumirea și adresa autorității competente**

DD-LL-XXXX,  
Orașul

Stimate domn / Stimate doamnă,

Potrivit art. 41 din Regulamentul (CE) 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II) și art. 58 din Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), Subsemnatul \_\_\_\_\_ (prenume, nume), \_\_\_\_\_ (naționalitate), \_\_\_\_\_ (data și locul nașterii), \_\_\_\_\_ (adresa), solicit accesul la datele mele personale introduse în Sistemul de Informații Schengen.

Vă transmit atașat:

1. copie de pe cartea de identitate validă potrivit legislației naționale a Statului Schengen (pașaport/carte de identitate/permis de conducere, alt document de identitate valid);
2. copie de pe împuternicirea avocațială de reprezentare a solicitantului;
3. altele.

Solicitant / reprezentantul legal

.....

Semnătură

Model cerere solicitare rectificare sau ștergere date personale

Către: **Denumirea și adresa autorității competente**

DD-LL-XXXX,  
Orașul

Stimate domn / Stimate doamnă,

Potrivit art. 41 (5) din Regulamentul (CE) 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II) și art. 58 (5) din Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), Subsemnatul \_\_\_\_\_ (prenume, nume ), \_\_\_\_\_ (naționalitate), \_\_\_\_\_ (data și locul nașterii), \_\_\_\_\_ (adresa), solicit rectificarea datelor mele persoanele inexacte sau ștergerea datelor mele persoanele ce au fost stocate ilegal în Sistemul de Informații Schengen. Datele mele personale ar trebuie rectificate/ștergere deoarece:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_.  
Vă transmit atașat:

1. copie de pe cartea de identitate validă potrivit legislației naționale a Statului Schengen (pașaport/carte de identitate/permis de conducere, alt document de identitate valid);
2. copie de pe împuternicirea avocațială de reprezentare a solicitantului;
3. altele.

Solicitant / reprezentantul legal

.....

Semnătură