CONSILIUL UNIUNII EUROPENE

Bruxelles, 10 mai 2010 (07.07)
(OR. en)

9768/10

SCH-EVAL 55
COMIX 361

NOTĂ

Sursă:	Grupul de redactare pentru Catalogul Schengen privind protecția datelor
Destinatar:	Grupul de lucru pentru evaluarea Schengen
Nr. doc. ant.:	10841/2/09 REV 2 SCHEVAL 83 COMIX 485
Subiect:	Catalogul recomandărilor în vederea aplicării corecte a acquis-ului Schengen și al celor mai bune practici: protecția datelor

2010

CATALOGUL SCHENGEN

RECOMANDĂRI ȘI CELE MAI BUNE PRACTICI

PROTECȚIA DATELOR

CUPRINS

*

* *

I. INTRODUCERE

1. În cadrul reuniunii sale din 28 mai 2001, Consiliul a stabilit drept obiectiv, în vederea continuării lucrărilor Grupului de lucru pentru evaluarea Schengen, sublinierea „... celor mai bune practici, în special în materie de control la frontiere, pentru a servi drept exemplu statelor care aderă la Schengen, dar și celor care aplică pe deplin acquis-ul Schengen. Aceste evaluări și identificarea celor mai bune practici vor servi drept bază pentru grupurile de lucru pertinente în vederea stabilirii de norme de definire a nivelului minim de aplicare a acquis-ului Schengen (…)" (mandat conferit Grupului de lucru pentru evaluarea Schengen) (doc. 8881/01 - SCH-EVAL 17, COMIX 371).

   Pe baza acestui mandat, Grupul de lucru pentru evaluarea Schengen a stabilit principiile și procedura privind elaborarea catalogului de recomandări în vederea unei aplicări corecte a acquis-ului Schengen și a celor mai bune practici, denumit în continuare Catalogul de recomandări și cele mai bune practici sau catalogul.

   Obiectivul catalogului este de a clarifica și aprofunda acquis-ul Schengen și de a prezenta recomandările și cele mai bune practici, pentru a servi drept exemplu statelor membre și țărilor asociate, indiferent dacă acestea aplică sau nu acquis-ul Schengen pe deplin. Obiectivul nu este de a defini într-un mod exhaustiv întregul acquis Schengen, ci de a prezenta recomandări care nu au forță juridică și cele mai bune practici, în funcție de experiența dobândită de Grupul de lucru pentru evaluarea Schengen în cadrul verificării aplicării corecte a acquis-ului Schengen în mai multe țări.

   Textul catalogului nu își propune să introducă noi cerințe, dar trebuie să permită de asemenea să atragă atenția Consiliului asupra necesității de a aduce modificări, acolo unde este cazul, anumitor dispoziții ale acquis-ului Schengen pentru ca atunci când prezintă propuneri sau inițiative formale, Comisia și, după caz, statele membre să ia în considerare recomandările și cele mai bune practici.

   Mai mult, catalogul va servi drept instrument de referință pentru evaluări. În consecință, acesta ar putea avea și rolul de a oferi statelor candidate o imagine despre sarcinile care le vor fi atribuite.

2. Grupul de lucru pentru evaluarea Schengen a adoptat următoarele definiții în vederea realizării acestui exercițiu:
   recomandări: un ansamblu neexhaustiv de măsuri care să faciliteze stabilirea unei baze în vederea aplicării corecte a acquis-ului Schengen, precum și a monitorizării acesteia.
   Cele mai bune practici: un ansamblu neexhaustiv de metode de lucru sau de măsuri model care trebuie să fie considerate ca reprezentând aplicarea optimă a acquis-ului Schengen, fiind de la sine înțeles că mai multe bune practici sunt posibile pentru fiecare parte specifică a cooperării Schengen.

3. În perioada 2002-2003, au fost realizate patru volume legate de aplicarea acquis-ului Schengen: privind frontierele externe, îndepărtarea și readmisia (volumul 1), privind Sistemul de Informații Schengen/SIRENE (volumul 2), privind eliberarea vizelor (volumul 3) și privind cooperarea polițienească (volumul 4).

4. În cadrul reuniunii sale din 17 iulie 2008, Grupul de lucru pentru evaluarea Schengen a stabilit obiectivul de revizuire și actualizare a cataloagelor existente pentru a reflecta evoluțiile legislative, organizaționale și tehnice din domeniile tratate de cataloage, ulterioare primei publicări a acestora. În același timp, s-a luat decizia de a realiza un nou catalog privind chestiunile de protecție a datelor care decurg din acquis-ul Schengen.

5. Sarcina realizării noului catalog privind protecția datelor a fost atribuită unui grup de experți condus de Belgia care și-a început activitatea în perioada președinției franceze. Președinția cehă a continuat lucrările la noul catalog și a preluat rolul de coordonare în redactarea acestuia.

6. În urma unei discuții aprofundate referitoare la domeniul care va face obiectul catalogului, și în special la VIS și noul SIS, Grupul de lucru pentru evaluarea Schengen a convenit să adopte o abordare etapizată și să realizeze noul catalog în două faze: într-o primă etapă, să adune informații din rapoartele de evaluare Schengen și să ofere o trecere în revistă a recomandărilor și bunelor practici privind normele aflate în vigoare în prezent (faza 1) și în a doua etapă să completeze acest catalog cu recomandări privind SIS II și VIS într-o fază ulterioară, atunci când acestea vor fi disponibile (faza 2).

7. Astfel, prezentul catalog constituie o versiune provizorie a catalogului, care va fi finalizată în timp util. Catalogul reflectă experiența bogată dobândită din evaluările Schengen recente în domeniul protecției datelor, în ceea ce privește recomandările și exemplele de bune practici identificate, precum și în ceea ce privește experiența Autorității comune de control Schengen.

8. Obiectul principal al acestui catalog este constituit de protecția datelor în Sistemul de Informații Schengen și de normele generale conexe aplicabile protecției datelor cu caracter personal în ceea ce privește legislația națională, autoritățile naționale de control etc. Din această perspectivă, catalogul tratează toate normele relevante în materie de protecția datelor cu caracter personal în cadrul SIS, astfel cum sunt stabilite în acquis-ul Schengen, inclusiv măsurile fără caracter legislativ și cele de punere în aplicare care privesc utilizarea SIS de către toate autoritățile autorizate: măsuri de securitate, cerințe tehnice pentru sistemele IT , confidențialitatea, drepturile persoanelor vizate, sensibilizarea populației etc.

9. Catalogul ar trebui citit în coroborare cu alte volume actualizate de catalog care conțin recomandări și cele mai bune practici privind protecția datelor, în special catalogul privind SIS și catalogul privind eliberarea vizelor.

II. RECOMANDĂRI ȘI CELE MAI BUNE PRACTICI

RECOMANDĂRI ***„un ansamblu neexhaustiv de măsuri care să faciliteze stabilirea unei baze în vederea aplicării corecte a acquis-ului Schengen, precum și a monitorizării acesteia.”***	**CELE MAI BUNE PRACTICI** ***„o serie neexhaustivă de metode de lucru sau de măsuri-model care trebuie considerate ca fiind aplicarea optimă a acquis-ului Schengen, ținând seama de faptul că pentru fiecare aspect specific al cooperării Schengen sunt posibile mai multe astfel de practici.”***
1. CONTEXT LEGISLATIV	
1.1. **Legislația** *Articolele 117, 126 și 127 din Convenția din 19 iunie 1990 de punere în aplicare a Acordului Schengen din 14 iunie 1985 (denumită în continuare „CISA” sau „Convenția Schengen”)*	
- Legislația națională care prevede norme de protecție a datelor în ceea ce privește prelucrarea datelor în SIS respectă pe deplin dispozițiile Convenției Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal din 28 ianuarie 1981 și ale protocolului adițional la aceasta din 8 noiembrie 2001 de asemenea, aceasta respectă prevederile Recomandării nr. R (87) 15 din 17 septembrie 1987 a Comitetului Ministerial al Consiliului Europei care reglementează utilizarea datelor cu caracter personal în activitatea poliției; - legislația națională specifică poate completa sau clarifica chestiunea prelucrării datelor în SIS, după caz; - legislația suplimentară și/sau subsidiară nu ar trebui să interfereze cu competențele autorității naționale de control în ceea ce privește SIS sau să le submineze; - trebuie, de asemenea, respectată Decizia-cadru 2008/977/JAI a Consiliului privind	- Dreptul la protecția datelor cu caracter personal este garantat prin lege ca drept fundamental.

protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (începând cu 27 noiembrie 2010 considerată doar document de referință, deoarece nu se aplică datelor prelucrate în SIS); - Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date trebuie, de asemenea, să fie pusă în aplicare (considerată document de referință, deoarece nu se aplică datelor prelucrate în SIS).	
1.2. **Acorduri bilaterale sau multilaterale (între state membre și țări terțe)** *(supuse reglementărilor de drept internațional)*	
- Toate acordurile bilaterale sau multilaterale cu țările terțe privind prelucrarea datelor în domeniul cooperării polițienești și judiciare în materie penală ar trebui să conțină dispoziții privind prelucrarea datelor în conformitate cu obligațiile care decurg din acquis-ul Schengen; - normele aplicabile în materie de protecția datelor (în baza Convenției Consiliului Europei nr. 108 și protocolul adițional la aceasta din 2001, precum și a Deciziei-cadru 2008/977/JAI) trebuie respectate;	- ar trebui utilizate clauze standard de protecție a datelor în acordurile care asigură protecția efectivă a datelor[1] -

[1] Rezoluția Conferinței de Primăvară a Comisarilor Europeni Însărcinați cu Protecția Datelor (Edinburgh, 24 aprilie) privind acordurile bilaterale și multilaterale dintre state europene și țări terțe în domeniul cooperării polițienești și judiciare în materie penală.

2. AUTORITATEA NAȚIONALĂ DE CONTROL *Articolul 114 alineatul (1) din CISA*	
2.1. **Autoritatea națională de control - independența**	
- Autoritatea națională de control este o autoritate de control independentă căreia îi revine sarcina de a garanta principiile de protecție a datelor cu caracter personal prevăzute în legislația națională și în Convenția Schengen; - independența autorității naționale de control trebuie asigurată prin garanții juridice, instituționale și operaționale; - independența instituțională este asigurată în condițiile în care statutul autorității naționale de control nu prevede nicio relație ierarhică cu autoritățile publice responsabile cu prelucrarea datelor în SIS; un statut administrativ clar ar trebui să sublinieze acest aspect al independenței sale; - independența juridică constă în interzicerea, printr-un text juridic, a interferențelor cu competențele juridice ale autorității naționale de control; - independența operațională a autorității naționale de control ar trebui asigurată prin existența unor resurse bugetare și umane suficiente pentru a permite exercitarea independentă a funcțiilor de control și de consiliere; - statutul juridic și structura autorității naționale de control ar trebui să protejeze membrii acesteia de riscul demiterii ca urmare a exercitării competențelor lor de control; - independența autorității naționale de control se reflectă în componența autorității, în metoda de numire a membrilor acesteia, în durata de	- Independența autorității naționale de control este prevăzută în mod explicit în legislația națională; - autoritatea națională de control este un organism separat din administrația publică care își exercită competențele de control în mod independent; - independența autorității naționale de control este garantată prin legea care reglementează procedura de numire a reprezentanților săi (de înalt nivel);

exercitare și condițiile de încetare ale funcțiilor acestora, în alocarea de resurse suficiente pentru autoritate și în capacitatea de a adopta decizii fără a fi supusă unor ordine sau instrucțiuni din exterior; - pentru a stabili în mod clar poziția independentă a autorității naționale de control, statele membre ar trebui să fie sau să devină părți la Protocolul adițional la Convenția pentru protecția persoanelor fizice față de prelucrarea automatizată a datelor cu caracter personal din 8 noiembrie 2001.	
2.2. **Autoritatea națională de control - competențe (Controale)**	
- Autorității naționale de control i se atribuie competențe (în baza legislației naționale pertinente) în vederea exercitării supravegherii independente a prelucrării datelor de către toate organismele naționale implicate în prelucrarea datelor în SIS și care accesează sistemul; - în cadrul autorității naționale de control, ar trebui elaborată și pusă în aplicare o strategie (un plan) de control pentru cercetarea SIS; - autoritatea națională de control ar trebui să aibă acces la N.SIS (atât in situ, cât și la fișierele jurnal) și competența de a solicita și de a primi documentația relevantă referitoare la obiectul controlului (plângere ad hoc sau supraveghere de rutină); - autoritatea națională de control ar trebui să enunțe în mod clar concluzii și recomandări în vederea recunoașterii sau, după caz, a îmbunătățirii procesului de prelucrare a datelor; - autoritatea națională de control ar trebui să aibă competența de a lua măsurile necesare pentru a fi puse în	- toate competențele autorității naționale de control sunt prevăzute prin lege, în mod clar; - autoritatea națională de control efectuează controale periodice legate de SIS; controalele se bazează pe plângeri ad-hoc, precum și pe un plan de acțiune anual; - strategia (planul) de control se bazează pe o evaluare temeinică a activităților de prelucrare a datelor realizate de organismele responsabile cu prelucrarea datelor în SIS; autoritatea națională de control evaluează toate riscurile, ocupându-se de toate aspectele legate de prelucrarea datelor în SIS; - controalele au ca obiect nu numai N.SIS dar și autoritățile care au drept de acces la datele SIS sau de a introduce date; utilizarea SIS este examinată și în practică (de ex. la frontierele externe ale zonei Schengen, la secțiile locale de poliție, la consulate etc.) - autoritatea națională de control efectuează controale în mod periodic pe baza analizei fișierelor jurnal; - în cazul în care aceste aspecte nu sunt prevăzute în legislația națională, există o

aplicare toate schimbările necesare în vederea îndeplinirii cerințelor prevăzute de dispozițiile privind prelucrarea datelor în SIS; - autoritatea națională de control ar trebui să efectueze controale în mod regulat, nu numai ca răspuns la plângeri; - în cazul statelor federale, ar trebui încheiate acorduri formale între autoritatea federală de control și autoritățile regionale privind cooperarea și o abordare coordonată a controalelor SIS;	înțelegere formală (de exemplu un schimb de scrisori, un memorandum între autoritățile în chestiune) între autoritatea națională de control și autoritățile responsabile cu prelucrarea datelor cu caracter personal în SIS, menită să dea un caracter oficial aranjamentelor de comunicare cu autoritatea națională de control și procedurilor legate de controale; - solicitările autorității naționale de control privind schimbările necesare relativ la prelucrarea datelor în SIS ar trebui să fie obligatorii din punct de vedere juridic sau asociate altor competențe efective de intervenție, în conformitate cu Directiva 95/46/CE privind protecția datelor; - autoritatea națională de control organizează vizite de monitorizare a rezultatelor acestor controale și verifică dacă avizele sau recomandările sale anterioare au fost puse în aplicare și dacă erorile identificate au fost corectate; - autoritatea națională de supraveghere are acces in situ la N.SIS prin intermediul personalului calificat al operatorului sau al experților (IT) din cadrul autorității naționale de control; - în statele federale au loc consultări regulate între autoritatea federală de control și autoritățile regionale; sunt stabilite relații strânse între toate autoritățile.
2.3. **Autoritatea națională de control - structură organizațională, buget, personal**	
- Autoritatea națională de control are toate resursele umane, financiare și logistice necesare pentru a își exercita competențele; - în afara funcțiilor de conducere de nivel înalt, printre membrii personalului autorității naționale de control ar trebui să se numere avocați, specialiști IT,	- Structura autorității naționale de control este (în cazurile în care este posibil) stabilită în funcție de sarcini și de competențe și prevede unități separate pentru management, administrare, audit, sarcini de control, sarcini juridice, sarcini informative și formare profesională; - autoritatea națională de control are un

responsabili cu informațiile și personal administrativ; - autorității naționale de control ar trebui să i se dea dreptul de a decide independent modul de cheltuire a bugetului; - în cazul în care resursele nu sunt suficiente pentru ca autoritatea națională de control să-și exercite competențele în mod independent, ar trebui instituită o procedură prin care autoritatea să poată solicita îmbunătățirea acestor aspecte;	statut bugetar independent în cadrul bugetului de stat; - bugetul autorității naționale de control reflectă sarcinile specifice ale acesteia legate de competențele sale privind SIS (de exmplu, costurile controalelor și al activităților de sensibilizare a populației); - autoritatea națională de control elaborează un modul de formare profesională pentru propriul personal privind chestiuni legate de SIS;
3. DREPTURILE PERSOANELOR VIZATE *Articolele 109, 110, 111, 114 alineatul (2) și 116 din CISA*	
3.1. **Dispoziții generale**	
- Drepturile persoanelor vizate ar trebui reglementate de legislația națională, stabilindu-se reguli și proceduri clare accesibile tuturor părților implicate; - aceste drepturi (inclusiv dreptul la formularea unei căi de atac) sunt exercitate în conformitate cu legislația națională a fiecărui stat membru, indiferent de cetățenia persoanei vizate; - cererea persoanei vizate trebuie tratată fără întârzieri necuvenite; - costurile legate de exercitarea acestor drepturi trebuie păstrate la nivelul unei taxe rezonabile; - aranjamentele de tratare a cererilor efectuate de persoane vizate stabilite în străinătate ar trebui elaborate astfel să	- Există un ghid pentru persoanele vizate care explică modul de exercitare a drepturilor acestor persoane. Ghidul este pus la dispoziție pe situl web al autorității naționale de control, precum și pe site-urile internet autorităților responsabile cu N.SIS. Acest ghid este disponibil și în alte limbi ale statelor Schengen participante; pot fi utilizate ghidurile create de autoritatea comună de control; - pe situl web al autorității naționale de control, precum și pe site-urile internet ale autorităților responsabile cu N.SIS, sunt puse la dispoziție formulare sau scrisori tipizate pentru exercitarea drepturile persoanelor vizate; - drepturile sunt exercitate în mod gratuit; - este ținută la zi și pusă la dispoziția

includă o procedură de confirmare a identității persoanei vizate și a autenticității cererii; - în cazul unui stat federal, ar trebui elaborate aranjamente procedurale între nivelul federal și cel regional privind tratarea cererilor și plângerilor persoanelor vizate.	publicului o listă cu datele de contact ale autorităților competente responsabile cu tratarea cererilor legate de drepturile persoanelor vizate; - autoritatea națională de control poate (în cooperare cu alte autorități naționale de control) să ofere informații și consiliere privind nu numai drepturile persoanelor vizate, dar și aspecte procedurale elementare din alte state membre,
3.2. **Dreptul de acces, dreptul la corectare și ștergere, dreptul la verificare**	
- Persoana vizată are drept de acces la propriile date cu caracter personal prelucrate în SIS și dreptul de a cere corectarea sau ștergerea acestor date și de a solicita pe lângă autoritatea națională de control verificarea acestor date în SIS; - în situația în care, în baza solicitării unei persoane, autoritatea națională de control trebuie să verifice date introduse în SIS de alt stat membru, această operațiune trebuie efectuată în strânsă colaborare cu autoritatea națională de control din respectivul stat membru; - refuzul dreptului de acces trebuie întemeiat pe legislația națională și pe Convenția Schengen și numai în măsura necesară pentru motivarea refuzului; - în condițiile în care acest fapt nu aduce prejudicii siguranței statului, cercetărilor penale sau drepturilor unor terți, persoanei vizate trebuie să i se acorde un maxim de informații; - în cazul în care accesul, ștergerea sau corectarea este refuzată, persoana vizată are dreptul de a înainta o plângere pe lângă autoritatea națională sau pe lângă alt organism independent care are competența de a cerceta dacă refuzul/prelucrarea acestor date este întemeiată;	- Persoanele vizate sunt informate după expirarea alertelor prevăzute la articolul 99 din Convenția Schengen că au fost colectate date în legătură cu ele, mai puțin în cazurile în care se aplică exceptarea menționată la articolul 109 alineatul (2); - se instituie un sistem de înregistrare care realizează o sinteză statistică a cazurilor de exercitare a dreptului de acces la SIS, precum și a urmărilor acestora, oferind astfel o mai bună perspectivă asupra calității datelor prelucrate; - fiecare cerere este tratată individual, ținându-se seama de toate circumstanțele acesteia; în principiu, răspunsul nu se limitează la informația conform căreia datele au fost prelucrate conform legii (sunt comunicate datele prelucrate); - legislația națională nu limitează frecvența cererilor persoanelor vizate; - răspunsul la o cerere este trimis, în general, fără întârzieri necuvenite, în maxim 30 de zile. În cazul în care cererea este emisă de un alt stat Schengen și este necesară cooperarea cu statul respectiv, perioada nu poate depăși 4 luni.

- legislația națională nu ar trebui să limiteze frecvența exercitării drepturilor persoanelor vizate, printr-o dispoziție mai restrictivă decât „la intervale regulate”; - când se răspunde la cererea unei persoane vizate, ar trebui respectat principiul justiției fără întârzieri excesive (i.e o perioadă care depășește 4 luni poate fi considerată în general excesivă); - în cazul în care dreptul este exercitat în mod direct (de către operator), autoritatea națională de control ar trebui să solicite (sau să i se furnizeze) rapoarte periodice privind numărul total al cererilor de acest tip, numărul de cereri care nu au putut fi acceptate, numărul de refuzuri de comunicare a datelor, numărul de cazuri în care în SIS nu exista nicio alertă, numărul de comunicări privind conținutul alertei și timpul aproximativ de răspuns; - în cazul în care persoana vizată care și-a exercitat dreptul de acces este rezident legal al altui stat membru și face obiectul unei alerte SIS emise de un stat membru în temeiul articolului 96 din CISA, ar trebui să se verifice dacă se respectă procedura prevăzută la articolul 25 alineatul (2) din CISA;	
3.3. **Căi de atac**	
- Procedura de exercitare a acestor drepturi ar trebui să fie clară și disponibilă pentru toate părțile implicate; - deciziile operatorului sau ale autorității naționale de control pot fi atacate în instanță (sau contestate de altă autoritate competentă în temeiul legislației naționale) hotărându-se dacă persoana vizată poate obține informațiile, corectarea sau ștergerea acestora sau	- Un ghid pentru persoanele vizate privind modalitățile de exercitare a acestui drept este disponibil pe situl web al autorității naționale de control, precum și pe siturile autorităților responsabile cu N.SIS; - toate părțile împlicate sunt audiate în instanță; acestea sunt invitate în mod oficial să-și expună argumentele; - în cazul în care hotărârea se referă la o alertă

compensații în legătură cu o alertă din SIS care o privește; - legislația națională nu ar trebui să impună restricții privind executarea întocmai a unei hotărâri definitive a respectivei instanțe sau autorități; i.e. pentru măsura solicitată, cum ar fi comunicarea datelor, ștergerea sau corectarea, nu mai sunt necesare alte proceduri în statul în care a fost introdusă alerta; - Deciziile definitive în temeiul articolului 111 din CISA trebuie aplicate în mod egal de toate statele Schengen; - ar trebui create proceduri pentru monitorizarea executării hotărârilor definitive și ar trebui să li se dea autorităților naționale de control posibilitatea să verifice dacă aceste hotărâri definitive au fost executate; În acest scop, este necesară comunicarea între autoritățile naționale de control corespunzătoare; - persoanele fizice nu sunt responsabile cu monitorizarea executării hotărârilor privind propriile date cu caracter personal în alt stat membru;	emisă de alt stat Schengen, autoritățile naționale însărcinate cu protecția datelor se informează reciproc în legătură cu hotărârea și cu executarea acesteia; - hotărârile definitive emise de instanțe în temeiul articolului 111 sunt comunicate de autoritatea emitentă autorității naționale de control; în cazul în care această obligație nu este impusă prin lege, procedura de comunicare este convenită de autoritatea națională de control împreună cu operatorul SIS;
4. SECURITATEA DATELOR *Articolele 118, 126 și 127 din CISA*	
- Măsurile de securitate ar trebui stabilite pe baza unui proces de gestionare a riscurilor, prin care domeniul de aplicare și echipamentele din cadrul SIS, riscurile aferente acestuia și contramăsurile necesare sunt identificate pe baza unei declarații privind cerințele de securitate pentru un anumit sistem (SSRS - „system-specific security requirement statement”); - punerea în aplicare a măsurilor de securitate ar trebui să fie conformă cu normele internaționale; - securitatea datelor presupune accesul la incinte, accesul la SIS precum și o	- autoritatea națională de control și operatorul efectuează verificări prin sondaj ale fișierelor jurnal în vederea depistării eventualelor abuzuri în SIS; se efectuează cel puțin o verificare pe an; - autoritatea națională de control organizează controale în mod periodic în incintele N.SIS și SIRENE; - operatorul utilizează un instrument (software) care permite depistarea intrărilor neautorizate în sistem;

verificare periodică a tuturor măsurilor și a punerii în aplicare a acestora în practica cotidiană; - trebuie să fie disponibilă o soluție tehnică care să permită o implementare unică a SIS la nivel central; - toate interogările se păstrează în jurnale; - ar trebui să existe reguli clare și specifice pentru accesul la datele SIS; - lista persoanelor care au acces la SIS și la fișierele jurnal ar trebui analizată în mod periodic pentru a verifica dacă scopul accesului și domeniul accesibil sunt adecvate și definite în mod clar; - este necesar un sistem adecvat (automatizat sau manual) pentru a efectua căutări în fișiere jurnal SIS în vederea identificării abuzurilor; - ar trebui introdusă o procedură prin care să se garanteze faptul că datele cu caracter personal din fișierele jurnal sunt șterse în timpul cuvenit; - ar trebui utilizate parole criptate în procedura de autentificare; - respectarea tuturor normelor de securitate ar trebui verificată în mod periodic de către operator, precum și de autoritatea națională de control.	- se introduce un sistem de autentificare bazat pe doi factori (certificat și chei de criptare stocate pe un card inteligent, împreună cu un număr personal de identificare; cardul și codul sunt prezentate împreună pentru accesul la SIS).
5. PROTECȚIA DATELOR ÎN LEGĂTURĂ CU ELIBERAREA VIZELOR	
5.1. **Transferul datelor, accesul la SIS și securitatea**	
- Toate autoritățile și serviciile competente, responsabile cu eliberarea vizelor, cu examinarea cererilor de viză, cu eliberarea permiselor de ședere și cu aplicarea legislației privind regimul străinilor în contextul aplicării dispozițiilor Convenției Schengen legate	- Accesul la SIS se face cu ajutorul unui ID de utilizator și a unei parole personale. Există reguli privind schimbarea frecventă a parolelor, interzicerea comunicării ID-urilor de utilizator și a parolelor către alte persoane și stocarea în condiții securizate a ID-urilor de utilizator și a parolelor;

de circulația persoanelor ar trebui să aibă acces online la SIS printr-o legătură de comunicare securizată; - în cazul în care accesul la SIS este oferit offline (de ex. pe CD-ROM), trebuie furnizate elemente de securitate, în special în timpul transportului; în plus, CD-ROM-urile vechi trebuie distruse; - ar trebui pregătite proceduri alternative pentru cazurile în care sistemul nu este disponibil la consulate, pentru a nu afecta procedura de eliberare a vizelor; - ar trebui puse în aplicare măsuri corespunzătoare pentru securitatea și protecția clădirilor/incintelor; - organizarea accesului și a utilizării SIS de personalul diplomatic și/sau local ar trebui reglementată corespunzător prin instrucțiuni oficiale; - accesul la SIS trebuie rezervat exclusiv personalului autorizat în mod corespunzător al consulatelor. personalul local ar trebui să aibă acces numai pentru citire; - funcționarii consulari pot interoga sistemul numai în legătură cu o cerere valabilă de viză; - personalul local poate executa numai activități corespunzătoare nivelului de autorizare atribuit personalului local de către consul; - ar trebui introdusă o procedură scrisă pentru acordarea autorizațiilor; - ar trebui instituită o procedură prin care lista persoanelor autorizate din consulate se menține la zi și se verifică pe baza jurnalelor; - personalul din consulate participă la formări periodice privind punerea în aplicare a cerințelor de protecție a datelor;	- personalul local din cadrul misiunilor diplomatice nu are acces decât la informații de tip „hit/no hit” (răspuns pozitiv sau negativ); - sunt introduse formări periodice privind chestiunile de protecția datelor legate de eliberarea vizelor; - încăperile principale beneficiază de protecție fizică după cum urmează: - alarmă de securitate în zona de prelucrare, în zonele de intrare și ieșire precum și la ferestre; - monitorizare 24/7 prin sisteme de televiziune cu circuit închis (CCTV). - sistem de control al accesului (cartele, elemente biometrice); - detectoare automate de incendiu și de inundație; - imposibilitatea accesului după programul de lucru; - alternative disponibile în caz de pană de curent; - securitatea fizică și de sistem a sistemului de rezervă includ următoarele: - o altă clădire securizată; - sistem de control al accesului (cartele, elemente biometrice); - monitorizare prin sisteme de televiziune cu circuit închis (CCTV) - alarmă de securitate; - terminale de calculator pentru accesul la sistem; - fișiere jurnal și istoricul jurnalelor; - alternative disponibile în caz de pană de curent; - verificări periodice efectuate de administratorul de sistem; - securitatea clădirilor/incintelor ar putea include: - agent de pază la intrare; - protecție printr-un sistem de alarmă; - monitorizare 24/7 prin sisteme de televiziune cu circuit închis (CCTV). - detectoare automate de incendiu, de inundație și de fum; - protecția accesului la clădire (cartele de securitate, mecanisme securizate de încuiere sau sistem biometric); - se introduce un sistem de mesaje de notificare (alertare) prin SMS sau email către administratorul de sistem în

- încăperile principale în care se organizează eliberarea vizelor beneficiază de protecție fizică împotriva abuzurilor din interior și din exterior; - eliberarea vizelor fiind o chestiune de interes pentru mai multe autorități publice, cooperarea între aceste autorități ar trebui să fie reglementată de o platformă de coordonare la care participă autoritatea națională de control.	caz de intrare neautorizată în sistem; - vizitatorii și obiectele personale ale acestora fac obiectul unor controale de securitate; - după programul de lucru, încăperile sunt încuiate și inaccesibile; - întregul personal face obiectul sistemului de autorizare, inclusiv personalul de curățenie;
5.2. **Controale în domeniul eliberării vizelor**	
- Ar trebui elaborată și pusă în aplicare o strategie (un plan) de control care să includă controale la consulate, menit(ă) să verifice respectarea normelor de protecție a datelor și a normelor de securitate; - autoritatea națională de control ar trebui să verifice procedurile aplicate în cazul accesului offline la SIS (în special dacă sunt utilizate CD-ROM-uri).	- Controalele în domeniul eliberării vizelor reprezintă una dintre activitățile periodice ale autorității naționale de control; - autoritatea națională de control verifică în ce măsură au fost instituite la consulate reguli de păstrare a jurnalelor și de acces și modul în care sunt respectate aceste proceduri.
5.3. **Drepturile solicitanților de viză**	
- Consulatele ar trebui să dispună în mod clar permiterea accesului fiecărui solicitant la propriile date în SIS, dreptul de a solicita ștergerea sau corectarea datelor și dreptul de a apela la autoritatea națională de control; - solicitantul de viză ar trebui să fie informat în legătură cu procedura de exercitare a drepturilor sale de a solicita corectarea sau ștergerea datelor, înclusiv căile de atac instituite prin legislația națională în conformitate cu Instrucțiunile consulare comune privind vizele adresate misiunilor diplomatice și oficiilor consulare (i.e. la cererea expresă a solicitantului de viză, consulatul îi oferă informații privind drepturile sale și	- Siturile web ale consulatelor includ informații speciale privind drepturile persoanelor vizate, inclusiv drepturile solicitanților (cărora li s-a refuzat acordarea) de viză (dreptul de acces la SIS, drepturile de formulare a unor căi de atac etc.); - notificarea refuzului vizei conține informații privind normele de exercitare a dreptului de acces la SIS; - la consulate sau pe siturile acestora, sunt disponibile în mai multe limbi broșuri care oferă informații generale privind exercitarea drepturilor persoanelor vizate (solicitanților de viză).

procedura); solicitantul ar trebui, de asemenea, să fie informat cu privire la faptul că datele sale ar putea fi stocate în bazele de date naționale, care sunt accesibile autorităților relevante din statele membre; - orice străin ar trebui să poată obține la consulat informații complete privind modul de exercitare a drepturilor sale în legătură cu SIS; - autoritatea națională de control ar trebui să fie implicată în furnizarea acestor informații privind drepturile solicitanților de viză.	
6. SENSIBILIZAREA PUBLICULUI	
- Autoritățile responsabile cu N.SIS și autoritatea națională de control ar trebui să ia măsuri pentru a asigura faptul că publicul este bine informat cu privire la existența SIS și la drepturile sale legate de acesta; - este deosebit de important să se furnizeze informații referitoare la dreptul de acces la date, la dreptul de corectare sau de ștergere a datelor în legătură cu datele din SIS, precum și la dreptul de a solicita autorității naționale de control să verifice datele și utilizarea acestora; de asemenea, ar trebui descrisă clar procedura de exercitare a acestor drepturi; - autoritățile responsabile cu N.SIS și autoritatea națională de control ar trebui să organizeze facilități permanente (site-uri internet etc.) de informare a publicului cu privire la obiectivele, datele, autoritățile și toate drepturile persoanelor vizate în ceea ce privește SIS (site-urile internet reprezintă unul dintre mijloacele de informare vitale; broșurile cu informații generale ar putea fi o opțiune pentru zonele cu o mai mare vizibilitate, cum ar fi consulatele sau aeroporturile);	- Autoritățile responsabile cu N.SIS și autoritatea națională de control desfășoară o campanie de informare permanentă; se oferă informații privind legislația națională și internațională, o descriere generală a SIS, precum și toate informațiile necesare privind modul în care publicul își poate exercita drepturile în calitate de persoane vizate, privind funcționarea autorității naționale de control, privind datele de contact etc.; - informațiile adresate publicului se actualizează în funcție de noile evoluții; - toate autoritățile care accesează SIS se implică în campania de informare (de exemplu, coordonarea pregătirii broșurilor sau a formularelor, interconectarea tuturor site-urilor internet relevante, inclusiv cel al autorității naționale de control); - se elaborează și se pun la dispoziție elemente de asistență (precum modele de scrisori, formulare, proceduri de reclamație, orientări și meniuri de întrebări frecvente) pe site-urile internet ale autorităților responsabile cu N.SIS și pe cel al autorității naționale de control, în alte limbi (mai multe/toate) ale statelor Schengen;

- toate autoritățile responsabile cu SIS ar trebui să ofere o imagine clară și neechivocă a dispozițiilor legale, în orice moment și pentru orice utilizator sau persoană vizată; se recomandă cooperarea reciprocă între aceste autorități și autoritatea națională de control.	- broșuri de informare cu privire la SIS și la drepturile persoanelor vizate se pun la dispoziție la punctele de trecere a frontierei, la secțiile de poliție și la consulate; - autoritatea națională de control publică rezultatele rapoartelor de investigație și ale rapoartelor de activitate.
7. COOPERAREA INTERNAȚIONALĂ *articolul 106 alineatul (3), articolele 109 și 110, articolul 111 alineatul (2), articolul 114 alineatul (2) din CISA*	
- Autoritatea națională de control ar trebui să coopereze cu alte autorități de control în măsura în care este necesar pentru îndeplinirea atribuțiilor lor; - în cazul cooperării cu alte autorități de protecție a datelor, ar trebui să se convină asupra unor termene fixe și a unui regim lingvistic; - dacă nu se aplică sau nu se stabilesc termene, ar trebui să se aplice principiul „în cel mai scurt timp posibil”; - în cazul în care o autoritate națională de control este implicată într-o procedură în temeiul articolelor 106, 109 și 110 și în cazul în care alerta este emisă de un alt stat Schengen, această autoritate ar trebui să informeze autoritatea de control a statului respectiv cu privire la avizul său; - în cazul în care o persoană vizată își utilizează dreptul de acces în statul în care locuiește și în cazul în care există indicații precise că datele sale au făcut obiectul unui schimb cu alte state Schengen sau cu diferite organizații (precum Interpol), persoana vizată poate solicita asistență din partea autorității naționale de control a statului în care își exercită dreptul de acces. Această asistență poate consta într-o investigație prin care să se ateste dacă a avut loc într-	- Autoritatea națională de control participă la activități organizate de Autoritatea comună de control sau de alte organisme comune de control sau împreună cu Autoritatea Europeană pentru Protecția Datelor; - solicitărilor de cooperare din străinătate li se răspunde în cel mai scurt timp posibil (interesul persoanei vizate are prioritate); - comunicarea dintre autoritățile naționale de control se desfășoară într-o limbă care poate fi înțeleasă de ambele părți (în cazul în care se utilizează o singură limbă, se recomandă engleza sau o altă limbă asupra căreia au convenit ambele autorități naționale de control); - în cazul în care legislația națională nu permite comunicarea formală într-o limbă străină, autoritatea respectivă trebuie să furnizeze destinatarului o traducere adecvată; - în momentul selectării regimului lingvistic trebuie să se țină seama de faptul că unele materiale sau informații ar putea fi prezentate și persoanei vizate; - se întocmește și se pune la dispoziția publicului o listă cu datele de contact ale autorităților competente responsabile cu tratarea cererilor legate de drepturile persoanelor vizate;

adevăr un schimb de date cu alte state Schengen sau cu diferite organizații. Dacă în acest caz specific se aplică excepții de la dreptul de acces, o astfel de investigație ar putea avea loc *ex officio*. Autoritatea națională de control ar trebui să transmită autorităților naționale de control ale statelor respective sau organizațiilor respective o solicitare de demarare a procedurii privind dreptul de acces. Autoritățile naționale de control solicitate ar trebui să trateze o astfel de solicitare în același mod ca o cerere de acces în temeiul dreptului lor național și să transmită decizia lor autorității naționale de control solicitante. Persoana vizată ar trebui informată cu privire la rezultate; - în cazul în care o procedură dintr-un stat Schengen se încheie printr-o hotărâre definitivă a unei instanțe, iar această hotărâre include (și) obligația de a corecta sau de a șterge anumite date transmise de un alt stat sau de o organizație, statul care le-a transmis ar trebui să fie informat cu privire la hotărârea respectivă. Persoanele responsabile cu prelucrarea acestor date și autoritatea de control din statul care a transmis datele ar trebui informate cu privire la faptul că hotărârea instanței cuprinde un ordin de corectare sau de ștergere a datelor. Dacă o autoritate națională de control este implicată într-un astfel de caz sau este informată cu privire la rezultat, aceasta ar trebui să informeze autoritatea națională de control a statului care a transmis datele cu privire la hotărârea instanței. În schimb, o autoritate națională de control care primește astfel de informații ar trebui să informeze autoritatea care le-a transmis în cazul în care datele respective sunt corectate sau șterse.	- poate fi utilizat un formular specific în vederea facilitării cooperării între autoritățile naționale de control; - în cazul în care statele Schengen nu pot să ajungă la un acord cu privire la corectarea sau ștergerea anumitor date din SIS [articolul 106 alineatul (3) din CISA], autoritatea națională de control implicată contactează autoritatea națională de control a celuilalt stat membru; - în cazul în care, din cauza diferențelor dintre legislațiile naționale, în tratarea cererii de acces este implicată o singură autoritate națională de control (pe baza accesului indirect sau atunci când își prezintă avizul la solicitarea organismului responsabil cu tratarea cererii), aceasta informează autoritatea națională de control a celuilalt stat Schengen cu privire la avizul său (articolul 109 din CISA); - dacă este cazul, se poate solicita autorității naționale de control să transmită o cerere de aviz referitor la dreptul de acces aplicat în celălalt stat Schengen (articolul 109 din CISA); - în cazul în care este necesară cooperarea dintre autoritățile naționale de control pentru tratarea unei cereri de corectare sau de ștergere (articolul 110 din CISA), se aplică în mod similar principiile prevăzute la articolul 114 alineatul (2) din CISA; - în cazul în care autoritatea națională de control este informată cu privire la o procedură judiciară în temeiul articolului 111 din CISA referitor la o alertă introdusă într-un alt stat Schengen sau este implicată într-o astfel de procedură, aceasta informează autoritatea națională de control a statului respectiv (transmițând, după caz, și propriul aviz); în cazul în care trebuie efectuată o verificare, cooperarea se desfășoară în conformitate cu articolul 114 alineatul (2) din CISA; - autoritatea națională de control transmite hotărârea instanței referitoare la alerta introdusă de un alt stat Schengen autorității naționale de control a statului respectiv;

	- autoritatea națională de control monitorizează modul în care se dă curs hotărârilor definitive ale instanței (inclusiv hotărârilor pronunțate într-un alt stat membru) referitoare la alertele introduse în statul Schengen respectiv.
8. UTILIZAREA ALERTELOR *Articolele 96, 97, 98, 99 din CISA*	
8.1 Articolul 96	
- Autoritățile naționale competente, responsabile cu alertele în temeiul articolului 96, ar trebui să controleze aceste alerte în mod periodic; - autoritățile naționale de control ar trebui să investească în continuare în elaborarea unui model comun de control care să fie folosit pentru controlarea alertelor în cadrul SIS; - autoritățile responsabile de alertele în temeiul articolului 96 ar trebui să elaboreze proceduri formale și scrise pentru a garanta că datele în temeiul articolului 96 sunt exacte, actualizate și legale; - în cazul în care diferite autorități sunt responsabile pentru calitatea și integritatea datelor, ar trebui să se asigure faptul că aceste responsabilități diferite sunt organizate și interconectate astfel încât datele să fie în permanență exacte, actualizate și legale, precum și faptul că aceste date sunt verificate; - ar trebui puse în aplicare sau dezvoltate în continuare măsuri de prevenire a alertelor în temeiul articolului 96 care vizează resortisanți ai statelor membre ale UE;	- În cazul în care datele sunt prelucrate de diferite organizații sau de servicii diferite ale aceleiași organizații ca părți ale unui singur lanț de prelucrare, este esențial să existe proceduri specifice pentru a menține datele exacte, actualizate și legale. Manualul SIRENE, care cuprinde normele și procedurile care reglementează schimburile bilaterale sau multilaterale de informații suplimentare, nu poate fi considerat drept o procedură prin care să se asigure că datele sunt în permanență exacte, actualizate și legale.
8.2 Articolul 97	
- Toate statele Schengen ar trebui să aibă proceduri scrise formale pentru toate autoritățile implicate în emiterea de alerte în temeiul articolului 97. - În cazurile în care mai multe autorități	

sunt implicate în emiterea de alerte în temeiul articolului 97, procedurile ar trebui să fie consecvente și ar trebui aplicate în mod uniform. - Atunci când sunt comunicate date despre o persoană care face obiectul unei alerte, este necesar consimțământul persoanei respective. Consimțământul unei persoane care face obiectul unei alerte ar trebui să fie dat în scris sau, cel puțin, ar trebui să existe o probă scrisă. - În cazurile în care este refuzat consimțământul, acest refuz ar trebui să fie întotdeauna dat în scris sau înregistrat oficial. - Datele privind minorii ar trebui controlate întotdeauna prin mijloace automate și proceduri formale pentru a preveni păstrarea acestora cu statutul de persoană care face obiectul unei alerte atunci când devin majori. - Formularul M ar trebui utilizat de toate statele Schengen. - Toate statele Schengen ar trebui să verifice dacă autoritățile naționale care au acces la alertele în temeiul articolului 97 sunt considerate autorități în conformitate cu articolul 101 alineatul (1) din CISA.	
8.3 Articolul 98	
- În toate statele Schengen ar trebui să existe proceduri scrise formale pentru toate autoritățile implicate în emiterea de alerte în temeiul articolului 98. - În cazurile în care mai multe autorități sunt implicate în emiterea de alerte în temeiul articolului 98, procedurile ar trebui să fie consecvente și ar trebui aplicate în mod uniform. - Ar trebui îmbunătățită conformitatea cu articolele 112 și 112A din CISA în cazul revizuirii datelor și al perioadelor de reținere. - Formularul G ar trebui utilizat de toate	

statele Schengen. - Toate statele Schengen ar trebui să verifice dacă autoritățile naționale care au acces la alertele în temeiul articolului 98 sunt considerate autorități în conformitate cu articolul 101 alineatul (1) din CISA.	
8.4 Articolul 99	
- Autoritățile responsabile de alertele în temeiul articolului 99 ar trebui să elaboreze proceduri structurate formale și scrise pentru a garanta că datele în temeiul articolului 99 sunt exacte, actualizate și legale; - autoritățile naționale competente, responsabile cu alertele în temeiul articolului 99, ar trebui să controleze și să inspecteze alertele respective la fiecare șase luni. Ar trebui stabilite noi orientări; - în cazul în care diferite autorități sunt responsabile cu calitatea și integritatea datelor, ar trebui să se asigure faptul că aceste responsabilități diferite sunt organizate și interconectate astfel încât datele să fie în permanență exacte, actualizate și legale, precum și faptul că aceste date sunt verificate; - o alertă vizând persoane de contact nu este acceptabilă, având în vedere formularea articolului 99 alineatul (2); - autoritățile naționale de control ar trebui să controleze periodic alertele în temeiul articolului 99.	- Manualul SIRENE, care cuprinde normele și procedurile care reglementează schimburile bilaterale sau multilaterale de informații suplimentare, nu poate fi considerat drept o procedură prin care să se asigure că datele sunt în permanență exacte, actualizate și legale.