CONSILIUL UNIUNII EUROPENE

Bruxelles, 30 august 2011 (04.10)
(OR. en)

13039/11

SCH-EVAL 126
SIRIS 79
COMIX 484

NOTĂ

Sursă:	Președinția
Destinatar:	Grupul de lucru pentru chestiuni Schengen (evaluarea Schengen)
Nr. doc. ant.:	18161/10 SCHEVAL 158 SIRIS 181 COMIX 837 7289/2/11 REV 2 SIRIS 17 ENFOPOL 47 COPEN 36 SCH-EVAL 77 COMIX 148
Subiect:	Versiune revizuită a Catalogului actualizat al recomandărilor în vederea aplicării corecte a acquis-ului Schengen și al celor mai bune practici (Sistemul de informații Schengen), cu definirea mai detaliată a celor mai bune practici din domeniul prioritar „alerte de arestare în vederea predării sau extrădării” (articolul 95) propuse de Grupul de lucru pentru chestiuni Schengen (SIS/SIRENE)

În continuare, se pune la dispoziția delegațiilor o nouă versiune a Catalogului actualizat al recomandărilor în vederea aplicării corecte a acquis-ului Schengen și al celor mai bune practici (Sistemul de informații Schengen), care cuprinde o nouă secțiune în capitolul 4.3, în care se definesc în mod mai detaliat cele mai bune practici din domeniul prioritar „alerte de arestare în vederea predării sau extrădării” (articolul 95).

Această modificare a fost acceptată de Grupul de lucru pentru chestiuni Schengen (evaluarea Schengen) în cadrul reuniunii sale din 30 mai 2011.

2009

CATALOGUL SCHENGEN

RECOMANDĂRI ȘI CELE MAI BUNE PRACTICI

S I S

CUPRINS

Prefața Președinției cehe

Cu ocazia reuniunii sale din 17 iulie 2008, Grupul de lucru pentru evaluarea Schengen și-a stabilit drept obiectiv revizuirea și actualizarea cataloagelor Schengen de recomandări în scopul aplicării corecte a acquis-ului Schengen și ale celor mai bune practici, având în vedere necesitatea de a ține seama de evoluția juridică, organizațională și tehnică care a intervenit în domeniile reglementate de cataloage din momentul publicării lor inițiale.

Lucrările consacrate actualizării catalogului privind Sistemul de informații Schengen și SIRENE au început în cursul președinției franceze și s-au încheiat în cursul președinției cehe. A fost instituit un grup de experți prezidat de Italia, cu participarea Comisiei europene, a Austriei, Republicii Cehe, Franței, Germaniei, Ungariei, Țărilor de Jos, Portugaliei, Poloniei, Sloveniei și a Elveției. Președinția cehă dorește să adreseze mulțumiri experților pentru profesionalismul de care au dat dovadă în cadrul actualizării catalogului.

Noua versiune a catalogului ține seama de toate evoluțiile care au intervenit în domeniul SIS și SIRENE, inclusiv de inițiativele adoptate recent pentru a spori utilizarea acestor instrumente esențiale în vederea asigurării controlului persoanelor la frontierele externe și pentru a ameliora securitatea și justiția în spațiul Schengen. Experiența dobândită în cursul evaluărilor celor zece noi state membre, care sunt conectate la SIS și care aplică pe deplin acquis-ul Schengen, a fost de asemenea luată în considerație , ca și rezultatele seminarelor organizate periodic în atenția operatorilor SIRENE precum și ale conferințelor responsabililor SIRENE. Viitoarea versiune a catalogului va trebui să țină seama de noua versiune SIS din momentul punerii sale în aplicare.

Astfel, statele membre și țările asociate la spațiul Schengen dispun de acum înainte de culegerea cea mai recentă de recomandări și de cele mai bune practici în ceea ce privește SIS și SIRENE. Obiectivul prezentului catalog, care nu are forță juridică obligatorie, este explicat de titlul său. Cu toate acestea, ar fi necesară examinarea aprofundată a recomandărilor și celor mai bune practici reunite în acest catalog, în conformitate cu acquis-ul Schengen însuși, întrucât un sprijin ferm nu poate fi adus spațiului extins UE/Schengen de libertate, justiție și de securitate decât prin aplicarea normelor cele mai stricte de utilizare a SIS, precum și prin instituirea birourilor SIRENE și cooperarea între acestea.

Președinția cehă este convinsă că pe de o parte, catalogul actualizat va ajuta țările candidate să își asigure o integrare reușită și, pe de altă parte, va stimula statele membre să amelioreze în continuare utilizarea SIS, consolidând totodată funcționarea propriilor birouri SIRENE.

Aprilie 2009

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 în cadrul următoarelor evaluări care vor fi efectuate în țările candidate. Acesta va avea, în ceea ce privește aceste țări, și un rol de indicator al sarcinilor care le vor fi atribuite și în acest sens, trebuie citit coroborat cu manualul SIRENE.

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. Din 2002, anul în care a fost publicată versiunea precedentă a catalogului, integrarea politicilor de securitate ale UE a fost consolidată și a evoluat datorită adoptării a mai multor instrumente juridice, mai ales Regulamentul (CE) nr. 871/2004 al Consiliului și Decizia 2005/211/JAI a Consiliului privind introducerea unor noi funcții ale Sistemului de informații Schengen, inclusiv în combaterea terorismului (ca urmare a unei inițiative a Spaniei), Deciziile 2006/757/CE și 2006/758/CE de modificare a Manualului SIRENE, Decizia-cadru 2002/584/JAI a Consiliului privind mandatul european de arestare și procedurile de predare între statele membre, Regulamentul (CE) nr. 562/2006 de instituire a unui Cod comunitar privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen), Decizia-cadru 2002/475/JAI a Consiliului (ca urmare a unei inițiative a Suediei). De asemenea, între timp au fost prezentate mai multe inițiative care au drept scop ameliorarea utilizării SIS, și anume inițiativa Franței cu privire la lupta împotriva terorismului și inițiativa Cehiei privind o exploatare mai eficientă a SIS și a SIRENE în ceea ce privește protecția minorilor. Pentru a păstra spiritul concluziilor Consiliului de la Tampere și al programului de la Haga, statele membre depun eforturi pentru a asigura integrarea și a ameliora cooperarea pentru a garanta faptul că Uniunea Europeană este un spațiu de libertate, securitate și justiție. Aceste noi dispoziții legislative și inițiative, precum și evoluția tehnologiilor IT, au avut un impact major asupra cooperării în cadrul SIS și SIRENE.

4. Extinderea spațiului Schengen la zece țări noi în 2007 și în 2008, respectiv Republica Cehă, Republica Estonia, Republica Letonia, Republica Lituania, Republica Ungaria, Republica Malta, Republica Polonia, Republica Slovenia, Republica Slovacă și Elveția, a reprezentat cea mai mare extindere a cooperării în cadrul SIS și SIRENE. Au fost identificate numeroase bune practici și au fost formulate numeroase recomandări în cadrul procesului de evaluare a acestor țări.

5. Seminarele operatorilor și conferințele responsabililor SIRENE organizate periodic au permis obținerea a numeroase rezultate importante în ceea ce privește cooperarea în cadrul SIS și al SIRENE, aprobate ulterior de către Grupul de lucru SIS/SIRENE.

6. Șase țări se pregătesc să adopte SIS și să adere la spațiul Schengen. Acestea ar trebui să dispună de catalogul actualizat. De asemenea, actualele state membre ar trebui informate cu privire la recomandări și la cele mai bune practici, pentru a le stimula să amelioreze utilizarea SIS și buna funcționare a birourilor lor SIRENE.

7. Structura prezentului catalog nu a cunoscut modificări semnificative de la ultima ediție. O scurtă parte generală descrie conceptele fundamentale care stau la baza recomandărilor și a celor mai bune practici. Acestea sunt dispuse într-un tabel, recomandările figurând în coloana din stânga, iar cele mai bune practici corespunzătoare în coloana din dreapta. Recomandările au fost actualizate în mod corespunzător pentru a corespunde cu stadiul actual al cooperării în cadrul SIS și al SIRENE, din punct de vedere legislativ, operațional și tehnic. Cele mai bune practici au fost strânse și prezentate în vederea descrierii soluțiilor optimale, în funcție de experiența dobândită în noile și vechile state membre.

PARTEA III: SISTEMUL DE INFORMAŢII SCHENGEN ŞI SIRENE

RECOMANDĂRILE ŞI CELE MAI BUNE PRACTICI DETALIATE

SECŢIUNEA GENERALĂ

Lista recomandărilor şi a bunelor practici prezentate în continuare a fost stabilită în principal pe baza rezultatelor diferitelor evaluări realizate în ultimii ani.

Conţinutul catalogului are drept rol de a servi la crearea bazelor de date naţionale care vor furniza informaţiile pentru SIS, precum şi la pregătirea secţiunii naţionale a SIS şi a SIRENE.

Se reaminteşte faptul că în cazul în care informaţii UE clasificate sunt prelucrate de utilizatorii sistemelor informatice Schengen, se aplică Decizia 2001/264/CE a Consiliului de adoptare a regulamentului de securitate al Consiliului (JO L 101 din 11.4.2001, p. 1). În acel caz, măsurile de securitate aplicate ar trebui să fie proporţionale cu nivelul de clasificare al informaţiilor deţinute, cu volumul acestora şi cu gradul de ameninţare pe care le prezintă.

În ceea ce priveşte introducerea alertelor în SIS, acesta conţine numai acele categorii de date care sunt furnizate de fiecare parte contractantă în parte, astfel cum este necesar pentru scopurile prevăzute la articolele 95-100 din Convenţia Schengen. Partea contractantă care emite o alertă stabileşte dacă respectivul caz este destul de important pentru a se justifica introducerea alertei în SIS. Cu toate acestea, ar trebui să se ţină seama în mod sistematic de principiul disponibilităţii informaţiilor.

Rolul birourilor SIRENE în cadrul funcţionării SIS este absolut esenţial. Statele membre, în conformitate cu legislaţia internă, îşi furnizează reciproc, prin autorităţile desemnate în acest scop (SIRENE), toate informaţiile suplimentare necesare în legătură cu introducerea alertelor şi pentru a permite adoptarea măsurilor corespunzătoare în cazurile în care persoanele şi obiectele pentru care au fost introduse date în Sistemul de informaţii Schengen sunt găsite ca urmare a consultării acestui sistem [a se vedea articolul 92 alineatul (2) din Convenţia Schengen]. În acest scop, birourile SIRENE dispun de un acces adecvat la totalitatea informaţiilor naţionale şi la avizele experţilor pertinente. Informaţiile suplimentare schimbate se utilizează numai în scopul în care au fost transmise.

Fiecărui birou Sirene îi revine rolul de coordonator în ceea priveşte asigurarea calităţii informaţiilor introduse în SIS. În acest scop, este necesar ca birourile SIRENE să dispună de competenţele necesare la nivel naţional pentru a îndeplini această funcţie, care le revine.

RECOMANDĂRI	CELE MAI BUNE PRACTICI
1. Secţiunea naţională a SIS	
1.1. Sisteme şi organizare	
- se impune crearea unei secţiuni naţionale a SIS, operaţională 24 ore din 24 şi 7 zile din 7 şi care beneficiază permanent de un suport tehnic suficient - este necesară garantarea integrităţii datelor între N.SIS şi fiecare dintre eventualele copii tehnice naţionale existente	- ar trebui prevăzute angajamente privind nivelul de întreţinere şi de servicii, atât pentru hardware, cât şi pentru software pentru a asigura o funcţionare 24 ore din 24 şi 7 zile din 7 - ar trebui efectuată o sincronizare a copiilor în timp real - ar fi necesară compararea periodică a bazelor de date
1.2. *Infrastructura de comunicaţii*	
- ar trebui să existe o reţea naţională stabilă - ar trebui asigurată un timp de răspuns scurt în ceea ce priveşte interogările - ar trebui să fie disponibile soluţii de comunicare adecvate şi sigure pentru a permite efectuarea căutărilor în SIS de la terminale mobile	- ar trebui prevăzute angajamente privind nivelul de întreţinere şi de servicii adecvate pentru a asigura o bună disponibilitate a reţelei - timpul de răspuns ar trebui să fie sub 5 secunde - cea mai bună soluţie constă în acordarea în ceea ce priveşte posturile consulare a unui acces on-line la datele pertinente din SIS

2. SIRENE	
2.1 Structura naţională	
- un birou SIRENE trebuie creat în fiecare stat Schengen şi desemnat drept unicul punct de contact în ceea ce priveşte alertele SIS şi procedura de urmat în cazul unui rezultat pozitiv - operatorii SIRENE ar trebui să dispună de un acces 24 ore din 24 şi 7 zile din 7 la sursele de informare sau la bazele de date care transmit alertele către SIS sau care conţin informaţii necesare pentru informaţiile suplimentare sau pentru a soluţiona problemele pe care le pot prezenta alertele - ar trebui respectat şi aplicat principiul conform căruia alertele Schengen sunt prioritare faţă de alertele Interpol	- toate birourile responsabile cu cooperarea poliţienească internaţională ar trebui să fie accesibile printr-un punct de contact unic, să facă parte din aceeaşi structură de gestionare şi să fie localizate în acelaşi punct

- ținând seama de principiul conform căruia alertele SIS sunt prioritare, în cazurile excepționale în care birourile SIRENE, Interpol sau orice altă autoritate în materie de cooperare polițienească (de exemplu, ofițerii de legătură) recurg la propriile lor canale pentru a comunica aceeași informație, cu privire la o aceeași persoană sau același obiect, este necesar să se prevadă un sistem de referințe încrucișate, pentru a garanta o bună coordonare în celelalte state membre	
- birourile SIRENE trebuie să dispună de personal suficient în funcție de numărul de alerte și de rezultate, precum și de volumul de muncă, de comunicații și de sarcini specifice care decurg din acestea	- personalul și serviciile auxiliare ale birourilor SIRENE ar trebui să facă obiectul unei revizuiri periodice care să țină seama de evoluția volumului de muncă și a metodelor de lucru
2.2 Organizare și sistem	
- biroul SIRENE trebuie să asigure 24 ore din 24 și 7 zile din 7 comunicarea cu toate celelalte birouri SIRENE și autorități naționale - toți membrii personalului, inclusiv cei care lucrează în afara programului de birou, ar trebui să dețină competențele și experiența necesare pentru a fi în măsură să ofere serviciile necesare celorlalte birouri SIRENE și să trateze alertele primite - în afară de personalul administrativ și operațional, este necesar personalul capabil să asigure suportul informatic - biroul SIRENE trebuie să fie echipat cu un sistem automatizat și eficient de gestionare a fluxului de date, care este conform cu normele prevăzute în versiunea actuală a „Schimbului de date între birourile SIRENE”	- în vederea asigurării unei funcționări optime, este necesară asigurarea continuității aspectelor legate de gestionare și de personal, precum și a aspectelor tehnice - flexibilitatea în ceea ce privește modalitățile de lucru poate contribui la gestionarea volumului de muncă în perioade de vârf - ar trebui prevăzute angajamente privind nivel de întreținere și de servicii, atât pentru hardware, cât și pentru software pentru a asigura o funcționare 24 ore din 24 și 7 zile din 7 - s-a constatat că un sistem electronic de gestionare a fluxului de date/a dosarelor destinat operatorilor SIRENE permite ameliorarea calității muncii și reducerea riscului de eroare transmiterea automată a mesajelor primite către sistemul de gestionare a fluxului de date contribuie la îndeplinirea acestor obiective - sistemul electronic de gestionare a fluxului de date/a dosarelor ar trebui să fie în interacțiune cu aplicația N.SIS și cu sistemele naționale în ceea ce privește gestionarea alertelor primite și trimise; ar trebui prevăzute avertismente automate pentru a semnala: • că un reper solicitat a fost adăugat • sau șters • modificarea unei alerte • sau intrarea unei noi alerte reglementate de articolul 95 • ștergerea unei alerte, atunci când în sistemul electronic de gestionare a fluxului de date/a dosarelor există un dosar referitor la respectiva alertă

- în afara procedurilor convenite în ceea ce privește schimbul de formulare, birourile SIRENE trebuie să folosească cutiile poștale adecvate pentru schimburile de e-mailuri operaționale și transmiterile de amprente digitale pe rețeaua specializată SIRENE	- în cazurile în care comunicarea trebuie efectuată via internet, este necesar să se utilizeze adresa de e-mail oficială a biroului SIRENE - ar trebui evitată utilizarea unor adrese de e-mail necertificate
- ar fi necesară aplicarea recomandării Consiliului privind SIRPIT, o metodă folosită pentru schimbul electronic de fotografii și de amprente digitale între serviciile de aplicare a legii (doc. 9696/01/06) - ar trebui ca biroul SIRENE să fie conectat direct la baza de date națională AFIS în vederea accesului la datele disponibile în format electronic care intră în competențele sale	- pentru astfel de transmiteri electronice, procedurile SIRPIT ar trebui să fie disponibile în fiecare birou SIRENE
2.3 Recrutare și formare profesională	
- biroul SIRENE ar trebui să dispună de efective capabile de luarea de inițiative și tratarea dosarelor într-un mod eficient - toți operatorii ar trebui să aibă cunoștințe bune în materie de legislație națională, privind sistemul național de aplicare a legii (inclusiv cunoștințe teoretice privind activitățile polițienești), justiție și gestionare a imigrației, precum și cunoștințe de bază în materie de chestiuni care țin de drept internațional proprii spațiului Schengen	- personalul ar trebui să beneficieze de sprijinul superiorilor și să poată apela, chiar și în afara programului de birou, la avizul experților juridici sau altui tip de experți, pentru a permite delegarea responsabilităților - o atenție deosebită ar trebui acordată gestionării resurselor umane pentru a asigura continuitatea efectivelor, în scopul de a ameliora calitatea activității biroului SIRENE - ar trebui să existe un sistem de formare în ceea ce privește gestionarea automatizată a fluxului de date SIRENE

- ar trebui să fie disponibili experţi juridici cu bune cunoştinţe în domeniul legislaţiei naţionale şi internaţionale, cu excelente cunoştinţe privind Convenţia Schengen, Manualul SIRENE şi regulamentele conexe şi cunoştinţe teoretice privind activităţile poliţieneşti	- expertiza juridică poate fi oferită prin recrutarea de consilieri juridici interni sau prin organizarea de formare juridică pentru personalul SIRENE
- personalul care a beneficiat de formare în domeniul aplicării legii este necesar pentru a furniza experienţa care s-a dovedit a fi extraordinar de importantă şi pentru a reduce timpul necesar pentru formare - ar trebui să fie stabilite standardele comune şi interpretarea comună	- ar trebui iniţiată o sesiune de formare comună puţin o dată pe an - ar trebui luat în considerare schimbul periodic de operatori, începând dinaintea utilizării operaţionale a SIS
- nivelurile de recrutare ar trebui să ţină seama de numărul de alerte naţionale şi de reexaminarea acestor alerte la sfârşitul perioadei de validitate, precum şi de numărul de rezultate pe teritoriul naţional şi de legătura cu alte birouri SIRENE referitoare la rezultate privind alertele SIS din alte state Schengen - strategia de recrutare SIRENE ar trebui să prevadă validarea actualelor dosare în conformitate cu articolul 95 înainte de utilizarea operaţională a SIS	- acesta ar trebui să reprezinte elementul-cheie în procesul de recrutare şi în formarea continuă pentru personalul SIRENE
- personalul ar trebui să aibă competenţe lingvistice suficiente	- personalul SIRENE ar trebui să aibă prioritate în ceea ce priveşte formarea lingvistică
- operatorii SIRENE ar trebui să fie capabili să comunice cel puţin în engleză	- este în mod clar de dorit ca operatorii să cunoască cât mai multe dintre limbile de circulaţie internaţională, atât pentru comunicarea directă cât şi pentru capacitatea de a gestiona documentaţia în absenţa asistenţei pentru traducere
2.4 Persoana de contact SIRENE (SIRCoP)	
- birourile SIRENE ar trebui să aibă capacitatea de a soluţiona dosare problematice, sensibile sau complexe	- birourile SIRENE ar trebui să pună la dispoziţie, în cadrul structurilor lor existente, o persoană sau mai multe persoane care să îndeplinească rolul de persoană de contact SIRENE (SIRCoP). Aplicarea SIRCoP la nivel naţional intră exclusiv în sfera de competenţă a fiecărui stat membru. În cazurile în care procedurile standard se dovedesc insuficiente, persoana/persoanele desemnată(e) poate/pot lucra cu dosare în privinţa cărora progresele sunt complexe, problematice sau

	sensibile și, în vederea soluționării chestiunii, poate fi necesar un anumit nivel de asigurare a calității și/sau un contact pe termen mai lung cu un alt birou SIRENE. De asemenea, SIRCoP poate identifica o problemă recurentă și poate avea o perspectivă generală asupra acesteia. SIRCoP ar fi în măsură să formuleze propuneri de îmbunătățire a calității și să analizeze opțiunile de soluționare pe termen mai lung a unor astfel de chestiuni. Această funcție nu este destinată cazurilor urgente, în care sunt utilizate în principiu serviciile de asistență non-stop. Dacă personalul biroului național SIRENE constată că un anumit caz necesită asistență din partea SIRCoP, aceştia vor contacta SIRCoP pentru a-i solicita să ia legătura cu SIRCoP din celălalt stat membru. Ca regulă generală, SIRCoP pot fi contactați de un alt SIRCoP numai în timpul programului de lucru.
3. Utilizatorii finali	
3.1 Interfață utilizator de interogare	
- există nevoia de interogare sau de căutare care depășește căutările pe bază de concordanțe perfecte	- printre exemplele de acest tip se numără interogările fonetice, interogările cu caractere generice, interogările conform logicii fuzzy, interogările bazate pe codul Soundex - ar trebui să se garanteze că astfel de interogări unice nu sunt interzise de legislația națională precum și că aceste interogări unice se pot efectua rapid și simplu
- interogările pe terminalele fixe și mobile ar trebui să includă interogările SIS. interogarea unică simultană în sistemele naționale și internaționale este cel mai eficient mod de a garanta consultarea sistematică a SIS - este preferabil accesul direct	- utilizatorilor finali ar trebui să li se furnizeze cel mai mare număr posibil de dispozitive de interogare a datelor, pentru a permite interogările directe
- informațiile cu privire la alertele naționale și internaționale ar trebui să fie afișate simultan	
- semnalele de avertizare cu privire la persoane, obiecte, vehicule ar trebui să fie disponibile pentru utilizatorii finali de la prima afișare pe ecran	
- atunci când sunt introduse alertele naționale, introducerea alertei in SIS ar trebui să fie setată ca funcție implicită, astfel încât introducerea acesteia să nu necesite o acțiune	- alertele ar trebui să fie verificate în prealabil la nivelul bazei de date naționale și de acolo să fie transferate automat către N.SIS

suplimentară din partea utilizatorului final - pe ecran ar trebui să fie afișate informații și instrucțiuni clare privind acțiunile pe care utilizatorul final trebuie să le efectueze în cazul obținerii unui rezultat	- în cazul unei uzurpări de identitate, procedura de abordare a unui rezultat privind un caz de uzurpare de identitate și investigațiile ulterioare care ar trebui să fie efectuate pentru a stabili dacă persoana este victima sau autorul uzurpării de identitate ar trebui să fie afișate în mod clar pe ecran
- ar trebui să fie dezvoltate aplicații cu o interfață accesibilă pentru public, care să permită modalități rapide și eficiente de efectuare a sarcinilor SIS	- atunci când se introduce un nume pe parcursul unei interogări, sistemul ar trebui să verifice atât datele privind persoanele, cât și datele privind documentele - interfața pentru utilizatori ar trebui să permită și să încurajeze introducerea simultană a numelui și, după caz, a numărului documentului, iar aplicația ar trebui să le verifice pe ambele în aceeași căutare
3.2 Formare profesională	
- administrațiile naționale ar trebui să asigure sensibilizarea părților interesate din SIS: poliția și alte agenții (de aplicare a legii), magistrații și autoritățile responsabile de urmărirea penală - formarea privind SIS ar trebui să fie inclusă în formarea inițială a utilizatorilor finali, precum și în formarea continuă, chiar înainte de utilizarea operațională a SIS	Administrațiile naționale ar trebui: - să furnizeze formare permanentă părților respective - să pună la dispoziția utilizatorilor finali un sistem de formare - să asigure contactul strâns al părților interesate cu SIRENE prin intermediul ofițerilor de legătură - să promoveze conștientizarea prin intermediul grupurilor de lucru relevante (cooperarea polițienească, controlul la frontieră, forța de reacție a șefilor polițiilor, cooperarea judiciară, Grupul de lucru pentru probleme de terorism) sau prin intermediul CEPOL - să se asigure că autoritățile responsabile de securitatea publică sunt sensibilizate (mai mult) în legătură cu posibilitatea introducerii de alerte conform articolului 96 alineatul (2) litera (b) - să explice efectul pe care îl are eliminarea controalelor la frontierele interne asupra activității poliției - să explice utilizarea SIS ca instrument polițienesc cotidian - să se asigure că în formare sunt incluse atât interogarea sistemului cât și introducerea de alerte

	- să vizeze participarea personalului SIRENE la formarea SIS din cadrul şcolilor de poliţie
- ar trebui elaborate manuale privind procedurile interne - ar trebui formulate instrucţiuni actualizate care să reflecte noile funcţii - înainte de aplicarea dispoziţiilor Schengen, ar trebui organizată o formare în cascadă - în momentul în care utilizatorii finali ajung la un anumit nivel de experienţă, ar trebui să fie furnizate cursuri de perfecţionare	- manualele, inclusiv manualul SIRENE, informaţiile şi materialele de formare şi de perfecţionare ar trebui să fie disponibile pe intranetul poliţiei sau pe alte tipuri de suport - înainte de utilizarea operaţională a SIS, un buletin de informare care să le prezinte utilizatorilor finali stadiul proiectului poate asigura şi garanta interesul acestora - punerea în aplicare a SIS ar trebui să reprezinte o simplă extindere a actualelor metode naţionale de interogare, astfel încât să se reducă nevoia de formare
4. Tratarea datelor	
4.1 Introducerea, modificarea şi eliminarea alertelor	
- toate alertele introduse ar trebui să satisfacă criteriile pentru a asigura luarea măsurilor necesare în cazul identificării unui rezultat - SIRENE ar trebui să examineze dosarele privind alertele existente în temeiul articolului 95 înainte ca acestea să fie disponibile pentru utilizatorul final - informaţiile suplimentare privind MEA/MIA (formularele A+M) ar trebui să fie transmise fără întârziere la introducerea alertei - normele de prioritate şi incompatibilitate trebuie să fie respectate	- este important să fie informate autorităţile care introduc alerte în SIS în legătură cu consecinţele acestor introduceri şi în special cu obligaţia de a lua măsurile necesare în cazul identificării unui rezultat - ar trebui să fie stabilite proceduri naţionale cuprinzătoare pentru definirea responsabilităţilor ca urmare a identificării unui rezultat în străinătate (de exemplu, predare, extrădare, recuperarea vehiculelor furate) - în cazul în care nu este posibil să se valideze în prealabil toate dosarele cu privire la alerte conforme cu articolul 95, aceste alerte ar trebui totuşi să fie puse la dispoziţia utilizatorilor finali de îndată ce sistemul este deschis utilizatorilor finali, fără a se aştepta rezultatul examinării formularului A de către SIRENE; în acest caz, trebuie stabilite proceduri pentru a asigura o examinare rapidă a dosarului în cazul în care este executată alerta - operatorilor SIRENE ar trebui să li se permită să elimine manual alertele care nu respectă normele de prioritate şi incompatibilitate - ar trebui să se menţină disponibilitatea alertelor „secundare” cu privire la o persoană, astfel încât acestea să fie inserate în cazul în care expiră prima

	semnalare cu privire la persoana în cauză, cu care a doua semnalare nu era compatibilă
SIRENE ar trebui să fie abilitat să asigure crearea, modificare și/sau eliminarea alertelor SIS	- operatorii SIRENE ar trebui să poată crea, modifica și/sau elimina alertele lor SIS naționale
- SIRENE ar trebui să inițieze un proces prin care alertele în conformitate cu articolul 95 care au fost emise înainte de intrarea în vigoare a legislației naționale de transpunere a Deciziei-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre să fie modificate pentru a fi conforme cu decizia-cadru (se aplică pentru statele Schengen care aplică MEA)	- după conversie toate reperele necesare în temeiul articolului 95 ar trebui să fie revizuite pentru a deschide drumul către o aplicare eficientă a MEA
- În cazul în care alerta în conformitate cu articolul 96 privind resortisantul unei terțe țări a fost introdusă de o autoritate pentru imigrație, cunoscându-se faptul că acesta este un beneficiar al dreptului la libera circulație în conformitate cu Directiva 2004/38/CE, autoritatea în cauză ar trebui să transmită biroului SIRENE din statul membru în care se află informații suplimentare la momentul creării alertei	- atunci când un MEA a fost trimis direct autorității judiciare de executare, iar locul în care se află persoana căutată este cunoscut* („cunoscut” ar trebui să reflecte faptul că locul în care se află persoana căutată este fix și neschimbat, de exemplu de află în închisoare pentru o perioadă de timp cunoscută - un loc „presupus” este insuficient), SIRENE ar trebui să informeze orice autoritate juridică care solicită crearea unei alerte SIS că nu este nevoie de aceasta într-un astfel de context. Cu toate acestea, autoritatea judiciară de executare poate, în orice caz, decide dacă trebuie să fie emisă sau nu o alertă SIS.”
- numărul de identificare a vehiculului (VIN) ar trebui să fie introdus în alerta SIS cu privire la vehicul, deoarece reprezintă cel mai important criteriu de căutare.	* Articolul 9 alineatul (1) din Decizia-cadru a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (2002/584/JAI)
- alertele privind documentele ar trebui să fie introduse în SIS, chiar dacă nu conțin toate datele , dar pe cât de complete posibil, în conformitate cu principiul disponibilității	
4.2 Schimbul de formulare și alte mijloace de comunicare	
- pentru eficiență maximă în comunicarea bilaterală, se folosesc limbi cunoscute de ambele părți	- în practica privind schimbul multilateral de formulare, formularele trebuie trimise cel puțin în engleză
- Răspunsul ar trebui să fie furnizat biroului SIRENE solicitant cât mai curând posibil	- atunci când nu se poate da curs cererilor urgente în termen de 12 ore, biroul SIRENE solicitant ar trebui să fie notificat și informat în consecință cu privire la motivele întârzierii. În cazul în care nu se primește un răspuns, șefii birourilor SIRENE ar trebui să se implice în rezolvarea chestiunii

Alertele în conformitate cu articolul 97 privind persoane dispărute expuse unor riscuri ridicate ar trebui să fie introduse în SIS cât mai curând posibil, iar orice informații suplimentare care pot ajuta în căutare (fotografii, descriere, informații suplimentare privind eventuala rută, răpitorul, vehiculul utilizat), inclusiv - în cazul minorilor - solicitarea unei „alerte privind răpirea copiilor”[1], ar trebui să fie furnizate imediat biroului SIRENE pentru a fi transmise mai departe birourilor SIRENE selectate, după caz.	Răpitorul copilului dispărut și vehiculele utilizate eventual ar trebui să fie introduse în SIS utilizând tipul potrivit de alertă și notificând în același timp alte birouri SIRENE în privința legăturii dintre alerte pe un formular M
Fără a aduce atingere responsabilităților statelor membre privind emiterea alertelor în conformitate cu articolul 97 și nici dreptului intern al acestora, cazurile în care apar următoarele circumstanțe ar putea fi considerate drept dispariții cu risc ridicat: • Circumstanțele dispariției: factori care indică natura forțată a dispariției sau existența unui risc pentru viața sau siguranța fizică a persoanei dispărute, cum ar fi: - existența unor dovezi privind o posibilă răpire, detenție ilegală, extorcare sau alte infracțiuni grave similare, care indică o legătură între dispariția în cauză și activitatea infracțională a unor părți terțe; - informații care oferă motive rezonabile pentru a presupune că există un risc pentru viața sau siguranța fizică a persoanei dispărute. • Circumstanțe referitoare la persoană: atunci când există circumstanțe personale, cum ar fi: - persoana dispărută este foarte tânără; - persoana dispărută poate constitui un pericol pentru siguranța personală a altor oameni (caracter violent, amenințări la adresa altor persoane etc.); - persoana dispărută are un handicap fizic sau mental grav care o face vulnerabilă în circumstanțele dispariției sale (persoană în vârstă, boală psihică etc.);	- introducerea alertelor ar trebui să fie efectuată de preferință în timp real - introducerea alertelor ar trebui să fie descentralizată (în special cu privire la obiecte) în măsura posibilului pentru a evita întârzierile datorate procedurii administrative interne, precum transmiterea alertelor către centrele de introducere a datelor - atunci când introducerea directă nu este posibilă, un mijloc rapid de transmitere ar trebui să fie furnizat pentru a transfera informația de la nivel local la nivelul la care sunt inserate datele, în special pentru alertele privind copiii dispăruți și vehiculele furate

[1] Inclusiv mecanismele de alertă privind răpirea copiilor pentru avertizarea publicului larg în cazul răpirii copiilor” - 15084/08 CRIMORG 177 CATS 87.

- persoana dispărută necesită tratament medical sau medicamente, fapt care o face vulnerabilă în circumstanţele dispariţiei sale. - Pentru a ajuta operatorul care completează diferitele subcâmpuri ale câmpului 083 de pe formularul M pentru dispariţii cu risc ridicat, va fi elaborat un afiş cu titlurile subcâmpurilor din acest formular. Nu este necesar să se completeze toate subcâmpurile, ci numai cele pentru care există informaţii relevante. - înaintea prelungirii unei alerte, ar trebui să fie reexaminate validitatea şi relevanţa actuale ale acesteia - numerele de identificare Schengen nu ar trebui să fie reutilizate pentru date diferite. - timpul scurs între incidentul care a condus la adoptarea deciziei şi introducerea unei alerte în SIS ar trebui să fie minimizat - alertele care corespund cerinţelor stabilite în Convenţia Schengen ar trebui, în măsura posibilului, să fie introduse automat în SIS: în cazul în care SIRENE trebuie să copieze manual astfel de alerte din sistemele naţionale pentru a le introduce în SIS, această operaţiune cauzează deseori întârzieri		

- ar trebui să fie instituite măsuri care vizează garantarea calității datelor pentru a se evita alertele SIS care au un efect advers asupra persoanelor pe care nu le vizează alerta	- o alertă ar trebui să fie eliminată din SIS atunci când se stabilește că un vehicul furat a fost obținut în mod legal de către un proprietar de bună credință
- introducerea sistematică de alerte în SIS ar trebui să fie intensificată pe cât posibil și ar trebui să fie stabilite criterii naționale pentru o asemenea introducere - la introducere, ar trebui să se verifice că nu există o alertă multiplă - biroul SIRENE ar trebui să poată rezolva fără întârziere cazurile de uzurpare de identitate	utilizarea alertei în conformitate cu articolul 99 ar trebui să fie întotdeauna una din măsurile luate în considerare în momentul în care este vorba de infracțiuni grave și/sau pericolele pentru ordinea publică sau ca măsură de sprijin în momentul în care sunt urmărite persoanele căutate - legislația națională ar trebui să permită adoptarea tuturor măsurilor în conformitate cu Convenția Schengen, în special a „controalelor specifice” în temeiul articolului 99 - formularul M ar trebui să urmeze alertele în conformitate cu articolul 99 care necesită un control specific, după caz, specificând motivele alertei și furnizând orice detalii utile - sistemul ar trebui să verifice automat dacă există alerte multiple prin căutări care depășesc căutările pe bază de concordanțe exacte
4.3 Monitorizarea rezultatelor	
- biroul SIRENE trebuie să reprezinte singurul punct de contact și intermediarul pentru transmiterea tuturor informațiilor legate de procedurile legate de identificarea unui rezultat - pentru alertele în temeiul articolului 95, biroul SIRENE trebuie să reprezinte singurul punct de contact și este responsabil de schimbul de informații de după identificarea rezultatului cel puțin până la inițierea procedurii formale de predare/extrădare	- schimbul tuturor informațiilor care nu necesită o scrisoare rogatorie ar trebui să fie efectuat prin intermediul biroului SIRENE - atunci când este posibil și/sau potrivit, biroul SIRENE poate facilita orice schimb suplimentar de informații ulterior arestării
- ar trebui să fie evitată transmiterea MEA în original sau a cererii de extrădare prin intermediul biroului SIRENE, cu excepția cazurilor în care biroul SIRENE a fost de asemenea desemnată drept autoritate centrală - pentru o perioadă tranzitorie, până în momentul în care SIS va avea capacitatea să transmită toate informațiile menționate într-un formular MEA, alerta are valoare de MEA, până la primirea originalului, în bună și cuvenită formă, de către autoritatea judiciară de executare (cf Deciziei-cadru 2002/584/JAI a Consiliului).	- biroul SIRENE ar trebui să furnizeze, într-un formular G, toate informațiile disponibile privind adresa autorității judiciare competente, termenul și limba în care trebuie să fie prezentat MEA

Autoritățile judiciare naționale ar trebui să fie familiarizate cu formularele A și M pentru a accepta alerta SIS împreună cu informațiile suplimentare furnizate în formularele respective, ca temei juridic preliminar pentru deținerea ulterioară a persoanei căutate, până la primirea originalului MEA. - pentru a permite biroului SIRENE să își ducă la îndeplinire sarcinile în mod eficient, deciziile juridice privind procedurile de predare sau de extrădare ar trebui să fie comunicate, fără întârziere, după ce au fost adoptate. - o răspuns, sau cel puțin un preliminar privind stadiul dosarului ar trebui să fie trimis(ă) în termenele stabilite	
- o alertă va fi eliminată din SIS din momentul în care nu mai este necesară - procedurile ar trebui să fie stabilite pentru a se asigura că măsurile privind obiectele pierdute sunt puse în aplicare rapid	- alertele în temeiul articolului 95 ar trebui să fie eliminate după predare sau extrădare - ar trebui să se garanteze că autoritățile responsabile de aplicarea legislației privind resortisanții unei țări terțe sunt disponibile 24 de ore din 24 și 7 zile din 7 sau sunt organizate astfel încât termenele pentru furnizarea de informații suplimentare să poată fi respectate: biroului SIRENE i se poate acorda acces, respectând competențele acestuia, la baza de date a acestor autorități - alertele privind adulții în temeiul articolului 97, care nu trebuie să fie plasate sub protecție, ar trebui să fie eliminate la identificarea unui rezultat - alte alerte în temeiul articolului 97 ar trebui să fie eliminate după executarea măsurilor de protecție - alertele în temeiul articolului 98 ar trebui să fie eliminate din momentul în care informațiile cu privire la locul în care se află persoana căutată sunt clar identificate și comunicate biroului SIRENE din statul solicitant - o semnalare privind un vehicul furat (inclusiv alertele multiple) ar trebui să fie eliminată pentru a coincide cu restituirea vehiculului proprietarului legal - ar trebui să fie clar identificate rolurile și responsabilitățile tuturor părților interesate în raport cu rezultatele privind obiectele și procedurile de după primirea răspunsurilor pozitive

- fiecare stat membru ar trebui să poată furniza statistici cu privire la rezultate	- fiecare răspuns pozitiv ar trebui să fie înregistrat cu acuratețe într-un mod care să faciliteze extragerea de statistici precise în rândul diverșilor utilizatori
Pentru a facilita un schimb de informații structurat privind procedurile de predare și extrădare, ar trebui utilizat formularul SIRENE M.	O *listă de control opțională* ar trebui pusă la dispoziția birourilor SIRENE și a altor birouri de poliție implicate în procedurile de predare sau extrădare, în conformitate cu legislația națională. (Nu este obligatorie menționarea numerelor și literelor în mesaj.) 1. NOTIFICAREA PRIVIND EXECUTAREA PREDĂRII - STATUL MEMBRU DE EXECUTARE a) biroul competent (persoana de contact în biroul corespunzător: nume și număr de telefon) b) locul/punctul exact de întâlnire (aeroportul și terminalul sau punctul exact de întâlnire la frontiera terestră) c) ora și locul exact de întâlnire înainte de predare (ora sau intervalul exact înaintea plecării) d) restricții privind data, ora sau zborul e) datele de contact ale agenților responsabili (unității responsabile) de executare f) confirmarea orarului de zbor sugerat *sau* propunerea unei date noi 2. DATELE PERSOANEI CARE URMEAZĂ SĂ FIE PREDATE - STATUL MEMBRU DE EXECUTARE a) gradul de risc, comportament agresiv și alte circumstanțe relevante b) documente de călătorie (numărul și termenul de valabilitate al documentului sau menționarea eventualelor probleme pentru executarea predării în cazul în care aceste informații nu sunt disponibile) c) condiții medicale speciale d) efecte personale neobișnuite e) limba maternă (limbile materne) vorbită(e) de persoana care urmează să fie predată f) menționarea cazului în care persoana a fost arestată sub un nume fals 3. NOTIFICAREA PRIVIND EXECUTAREA PREDĂRII - STATUL MEMBRU EMITENT a) biroul competent (persoana de contact în biroul corespunzător: nume și număr de telefon)

b) detaliile zborului
b1) numărul zborului la sosire/plecare, compania de zbor
b2) data, ora, terminalul
b3) confirmarea faptului că va fi informată compania aeriană cu privire la transportul persoanei
c) agenții însoțitori (numele, numerele de pașaport și numerele de telefon mobil)
d) solicitarea aplicării anumitor proceduri (arme de foc, cătușe etc.)
e) solicitarea de asistență suplimentară
f) acordarea sau nu a permisiunii de tranzit (statul membru implicat, aeroportul)
g) solicitarea confirmării și precizarea termenului
h) convoi militar/colectiv
i) alte informații

4. DATELE PERSOANEI CARE URMEAZĂ SĂ FIE PREDATE - STATUL MEMBRU EMITENT
a) solicitarea emiterii unui permis de liberă trecere
b) informații medicale sau psihiatrice relevante
c) gradul de risc, comportament agresiv
d) alte informații

5. NOTIFICAREA PRIVIND DECIZIA (*DACĂ AUTORITATEA JUDICIARĂ A FURNIZAT INFORMAȚII*) - STATUL MEMBRU DE EXECUTARE
a) autoritatea care a luat decizia
b) data emiterii deciziei
c) numărul MEA/MIA
d) decizia privind fiecare MEA/MIA (dacă a fost acordat, refuzat sau nu s-a luat încă o decizie)
e) dacă decizia este sau nu finală
f) procedură de predare simplificată sau nu (informații privind acceptarea/refuzul predării de către persoana în cauză)
g) informații privind principiul specialității (acceptarea/refuzul de către persoana în cauză sau aplicabilitatea la nivel național în cazul procedurii simplificate)
h) caracterul deciziei: temporară, definitivă
i) termenul de executare a predării sau precizarea inexistenței unui astfel de termen
j) dacă persoana este deținută până la predare sau este pe cauțiune
k) data exactă la care persoana a fost arestată în statul membru de executare în vederea predării/extrădării

	Orientări privind secțiunea 1: În cazul predării la o frontieră terestră, toate informațiile, cu excepția secțiunii 1 literele d) și f), vor fi furnizate de statul membru de executare. În cazul predării la o frontieră aeriană, numai informațiile din secțiunea 1 literele a) și d) vor fi furnizate de statul membru de executare în prima etapă. În urma informațiilor primite de la statul membru emitent, vor fi furnizate și informațiile prevăzute la literele b), c), e) și f).
4.4 Măsuri care vizează garantarea calității datelor	
- ar trebui să existe introducerea automată a datelor SIS, prin intermediul unei legături între bazele naționale de date relevante și baza de date N.SIS, respectând, în același timp, principiul proporționalității - introducerea automată a alertelor ar trebui să fie însoțită de modificarea/eliminarea automată, în timp real, în SIS, după o modificare/eliminare efectuată în sistemul național	- această recomandare este satisfăcută atunci când introducerea în SIS este setată ca opțiune implicită, după cum s-a recomandat în capitolul 3.1
- alertele ar trebui să fie pe cât de complete posibil - alertele ar trebui să fie actualizate în momentul în care devin disponibile date suplimentare precum numărul de înregistrare al unui document emis sau numărul de identificare a vehiculului (VIN) pentru un vehicul furat	- datele privind alertele ar trebui să fie verificate, de preferință în mod automat, în registrele naționale - biroul SIRENE al statului membru de origine a unui obiect furat introdus în SIS de alt stat membru ar trebui să furnizeze biroului SIRENE din statul membru care a introdus semnalarea toate informațiile disponibile pentru completarea/actualizarea/corectarea alertei, imediat de ce este informat în legătură cu o astfel de alertă
- biroul SIRENE ar trebui să coordoneze asigurarea calității informațiilor - SIRENE trebuie să valideze fiecare semnalare în temeiul articolului 95	- SIRENE ar trebui să aibă, la nivel național competența și mijloacele tehnice și operaționale de a asigura calitatea datelor, inclusiv prin accesul la bazele naționale de date, în limita competenței proprii - SIRENE ar trebui să fie implicat în formarea utilizatorilor - lista de rezultate ar trebui să fie confruntată cu lista de alerte eliminate

- ar trebui să fie respectate regulile de transliterare - utilizatorilor finali ar trebui să li se pună la dispoziție informații specifice privind regulile de transliterare - utilizatorii finali ar trebui să beneficieze de formare pentru a asigura aplicarea corectă a măsurilor care vizează garantarea calității datelor	- raportul alerte/ rezultate ar trebui să fie revizuit și analizat - ar trebui să se efectueze controale periodice împreună cu autoritățile locale cu privire la necesitatea de a reține o alertă cu privire la un minor dispărut - nu este permisă introducerea informațiilor fără valoare adăugată, precum „necunoscut” sau „?”, nici în rubricile obligatorii, nici în cele facultative
5. Securitatea	
5.1 Organizarea lucrărilor privind securitatea datelor	
- hotărârea unei politici de securitate pentru sistemele IT Schengen (N.SIS, C.SIS, SIRENE și sistemele utilizatorilor finali) ar trebui să facă parte din definiția politicii generale de securitate a autorităților în cauză - politica de securitate adoptată trebuie sprijinită prin documente, în scris, de către autoritățile competente - este esențial să se aloce resursele necesare pentru pregătirea și menținerea măsurilor de securitate - la nivel național, ar trebui să fie stabilite procedurile și domeniile de responsabilitate pentru a se asigura actualizarea și revizuirea continuă a măsurilor de securitate - actualizarea sau revizuire politicii și procedurilor ar trebui, în măsura în care este posibil, să fie efectuate o dată pe an, astfel încât să fie în permanență adaptate scopului și să reflecte condițiile existente - în plus, actualizarea și revizuirea ar trebui să fie realizate ca urmare a unor incidente semnificative sau serioase sau ca urmare a unor modificări ale sistemului care au un anumit impact asupra securității datelor	

5.2 Organizarea securității și controlul activelor	
- eforturile de asigurare a securității datelor ar trebui - oricând este posibil - să fie planificate în cadrul unei organizații de securitate, care poate include una sau mai multe autorități - trebuie să se garanteze identificarea corectă a tuturor părților (activelor) importante ale sistemelor, astfel încât acestea să poată fi protejate în conformitate cu importanța lor - prin urmare, un registru sau un echipament IT relevant ar trebui să fie menținut în permanență - în plus, ar trebui să fie furnizată documentație actualizată privind rețeaua și sistemul, fiind prezentate, de exemplu, legăturile dintre elementele specifice ale sistemului și funcționalitatea acestora - responsabilitățile și competențele delegate persoanelor implicate în activități legate de securitatea datelor ar trebui să fie clar definite, eventual în cadrul fișelor postului persoanelor respective. - în mod normal, ar fi util ca informațiile privind organizarea activității de securitate să fie puse la dispoziție printr-o organigramă.	
5.3 Securitatea personalului	
- numai persoanele autorizate pot avea acces la datele SIS și la echipamentele utilizate pentru a prelucra datele SIS. - utilizatorii pot căuta numai datele de care au nevoie pentru îndeplinirea atribuțiilor lor.	- ar trebui să aibă loc o anchetă de securitate privind membrii personalului, atât în cadrul procedurii inițiale de recrutare, cât și ulterior la fiecare 5 ani de activitate.
- fișele postului membrilor personalului care au acces la datele SIS și la echipamentele utilizate pentru prelucrarea datelor SIS ar trebui să conțină informații privind respectarea cerințelor în materie de securitate.	
- în cadrul procedurilor de recrutare a personalului ar trebui să se acorde importanță cunoștințelor în materie de securitate a datelor. - personalul trebuie să participe la programul necesar de formare a utilizatorilor, cuprinzând toate normele aplicabile în materie de securitate a datelor. - trebuie încheiate acorduri de confidențialitate sau privind secretul de serviciu cu toate persoanele care nu aparțin niciunei autorități naționale.	

- aceste persoane trebuie să aibă autorizația sau certificarea de securitate necesară. - ele ar trebui să aibă acces la datele SIS numai atunci când au nevoie pentru îndeplinirea atribuțiilor lor. - trebuie definite structuri ierarhice și proceduri, pentru a asigura raportarea cât mai rapidă a incidentelor reale sau bănuite în materie de securitate. - procedurile în materie de securitate a datelor trebuie să fie cunoscute de tot personalul intern și de toți contractorii externi. - trebuie puse în aplicare mecanisme de informare astfel încât, după soluționarea și finalizarea unui incident, să se asigure comunicarea informațiilor cu privire la rezultate și la sesiunea de informare. - orice încălcare a normelor de securitate trebuie să facă obiectul unor măsuri disciplinare corespunzătoare, în conformitate cu legislația națională.	
5.4 Securitatea fizică	
- instalațiile de prelucrare a datelor SIS (N.SIS, C.SIS și SIRENE), precum și alte resurse esențiale sau sensibile, cum ar fi zonele de depozitare a suporturilor electronice, trebuie să fie amenajate în zone securizate și fiecare astfel de zonă să fie protejată printr-un perimetru de securitate delimitat de bariere fizice corespunzătoare și supus controlului accesului. - fiecare zonă trebuie prevăzută cu protecție corespunzătoare împotriva oricărei forme de pătrundere neautorizată.	- instalațiile de prelucrare a datelor SIS și alte resurse esențiale sau sensibile ar trebui amenajate într-o zonă de securitate de clasa a II-a, astfel cum este definită în Decizia 2001/264/CE a Consiliului[1] (gradul de securitate depinzând de cantitatea și formatul informațiilor stocate). - calculatoarele ar trebui instalate în subteran (sau ar trebui asigurat un alt nivel de securitate comparabil). - ar trebui prevăzute diferite zone de securitate, inclusiv: - carduri de acces (sau alt nivel de securitate comparabil); - agenți de pază; - monitorizare prin sisteme de televiziune cu circuit închis (CCTV). - intrările și ieșirile ar trebui monitorizate.

[1] Decizia 2001/264/CE a Consiliului de adoptare a regulamentului de securitate al Consiliului, publicată în JO L 101 din 11.4.2001, p. 1.

- pereții exteriori trebuie să aibă o structură solidă, iar ușile de acces trebuie prevăzute cu protecție corespunzătoare împotriva accesului neautorizat, de exemplu cu mecanisme de control, de blocare, de încuiere sau cu alarme. - clădirile sau spațiile care adăpostesc instalații de prelucrare a datelor SIS trebuie să dispună de zone de recepție prevăzute cu personal suficient sau cu alte mijloace de control al accesului fizic. - accesul în zonele securizate în care se află instalațiile de prelucrare a datelor SIS și de depozitare a suporturilor electronice trebuie să fie supus controlului și permis numai persoanelor autorizate.	
- vizitatorii în zonele securizate ar trebui supravegheați sau deținători ai unei autorizații de securitate. - vizitatorilor ar trebui să li se acorde accesul numai în scopuri precise și autorizate. - personalului părților terțe care asigură servicii de asistență ar trebui să i se acorde acces restrâns în zonele securizate și numai în caz de necesitate. - acest acces trebuie să fie autorizat și monitorizat.	
5.5 Securitatea echipamentelor	
- toate echipamentele utilizate pentru prelucrarea sau stocarea datelor SIS trebuie protejate împotriva avariilor sau pierderilor accidentale și împotriva accesului neautorizat.	
5.5.1 Echipamente de prelucrare a datelor SIS	
- echipamentele de prelucrare a datelor SIS trebuie să fie instalate în zone cu acces limitat la minim și strict controlat. - trebuie asigurată o monitorizare continuă în vederea reducerii la minim a riscurilor posibile, inclusiv atacuri criminale sau teroriste, incendiu, supraîncălzire provocată de o avarie la instalația de climatizare, prăbușire în urma unei explozii sau infiltrația apei. - pentru a asigura continuitatea alimentării cu energie electrică, următoarele echipamente trebuie să fie în stare de funcționare și trebuie verificate și o sursă neîntreruptă de alimentare cu energie electrică testate periodic: un generator de rezervă, care să (UPS), care	Printre instalațiile IT ar trebui să se numere: - sisteme de detectare a incendiilor, a căldurii și a fumului; - sisteme automate de stingere a incendiilor; - climatizare suficientă.

să mențină funcțiile esențiale; asigure continuitatea prelucrării în cazul unei întreruperi prelungite a alimentării cu energie electrică. - cablurile de telecomunicații trebuie protejate oricât de mult este necesar.	

- echipamentele rețelelor electronice trebuie instalate în încăperi sau dulapuri încuiate.	
- numai personalul de întreținere autorizat poate efectua lucrări de reparații și întreținere a echipamentelor. - ar trebui prevăzut un sistem de rezervă separat, precum și verificări periodice ale comutatorului dintre sistemul de rezervă și cel operațional.	Instalațiile de rezervă ar trebui să prevadă: - dispozitive de rezervă manuale/automate sau situri duble; - localizare la distanță, astfel încât un dezastru care afectează un sit să nu îl afecteze și pe celălalt.
5.5.2 Terminale și posturi de lucru PC	
- terminalele, posturile de lucru PC și imprimantele trebuie să fie instalate astfel încât datele înscrise să nu poată fi citite de persoane neautorizate. - ar trebui stabilite proceduri de monitorizare a imprimărilor efectuate de pe ecran și după datele SIS. - sesiunile la PC sau la terminal trebuie să efectueze o deconectare automată („log off") sau să expire („time out") după o perioadă de inactivitate, iar echipamentele respective trebuie protejate prin dispozitive de închidere, parole sau prin alte măsuri de control atunci când nu sunt utilizate. - terminalele, posturile de lucru PC și imprimantele instalate în încăperi accesibile publicului trebuie monitorizate continuu.	
5.6 Gestionarea comunicațiilor și a funcționării	
5.6.1 Proceduri operaționale și responsabilități	
- procedurile operaționale stabilite de fiecare stat Schengen în parte trebuie să fie documentate și trebuie revizuite și actualizate periodic. - acestea trebuie să cuprindă cel puțin următoarele: • proceduri de funcționare cotidiană, cum ar fi efectuarea copiilor de rezervă, actualizarea programelor antivirus, monitorizarea rețelei etc. • proceduri de gestionare a suporturilor de date și a altor bunuri; • proceduri privind restricționarea accesului; • instrucțiuni privind tratarea erorilor și a altor situații excepționale; • contacte de sprijin în cazul unor dificultăți de funcționare sau tehnice neașteptate;	

• proceduri de repornire sau de restabilire a sistemului în urma unei avarii; • ar trebui asigurat un control satisfăcător al tuturor modificărilor efectuate la instalațiile de prelucrare a datelor SIS și la sisteme, inclusiv la hardware, software și la proceduri; • se impune stabilirea unor responsabilități, instrucțiuni și proceduri clare pentru gestionarea acestor modificări.	
5.6.2 Proceduri de gestionare a incidentelor	
- trebuie stabilite planuri de urgență și proceduri de intervenție în etape în vederea soluționării incidentelor care pot întrerupe funcționarea sistemului și din cauza cărora sistemele IT Schengen pot deveni complet sau parțial inaccesibile. - trebuie definite proceduri de detectare și de gestionare a incidentelor care nu compromit accesul la întregul sistem, dar pun în pericol securitatea datelor.	
5.6.3 Protejare împotriva produselor software dăunătoare	
- în vederea protejării integrității software și a datelor, ar trebui aplicate în mod periodic o serie de măsuri de securitate pentru a preveni și a detecta pătrunderea produselor software dăunătoare și pentru a contribui la restabilirea ulterioară a sistemelor. - printre acestea ar trebui să se numere măsuri de control în vederea protecției împotriva virușilor, a „viermilor informatici”, a programelor disimulate („Trojan horses”) și a altor produse software dăunătoare. - ar trebui prevăzute cel puțin următoarele elemente: • o politică formală care să impună respectarea licențelor informatice și să interzică utilizarea produselor software neautorizate; • ar trebui instalate pe toate calculatoarele produse software de detectare a virușilor și de reparare și ar trebui efectuate actualizări periodice ale definiției virușilor, precum și scanări ale serverelor, PC-urilor și laptopurilor; excepțiile de la această regulă, în cazul în care există, trebuie justificate; • tot ceea ce se primește ca atașament la emailuri și tot ceea ce trebuie descărcat trebuie verificat înainte de utilizare în vederea detectării de produse software dăunătoare; ar	- atașamentele sub formă de fișiere cu extensia .exe, criptate sau prevăzute cu macro-uri, parole sau alte proceduri similare suspecte nu trebuie deschise.

trebui stabilit momentul efectuării acestei verificări: de exemplu pe serverele de email sau la intrarea în rețea; • trebuie să existe proceduri formale de răspuns la incidentele legate de viruși.	
5.6.4 Copii de rezervă	
- trebuie făcute în mod periodic copii de rezervă ale datelor SIS, ale fișierelor de configurare și ale aplicațiilor.	- ar trebui făcute zilnic astfel de copii.
- toate sistemele de rezervă trebuie testate periodic pentru a le asigura conformitatea cu cerințele planurilor de funcționare. - datele de rezervă trebuie să beneficieze de protecția fizică necesară și trebuie păstrate în locații geografice distincte. - procedurile de restabilire trebuie verificate și testate periodic.	- copiile trebuie păstrate în cel puțin două locații diferite. - procedurile de restabilire ar trebui testate de două ori pe an.
5.6.5 Gestionarea rețelei	
- pentru transmisiile de date SIS la nivel național pot fi utilizate numai rețele protejate împotriva accesului neautorizat. - rețelele trebuie monitorizate constant. - trebuie luate măsuri de protecție a datelor SIS în cursul transmiterii prin rețele de comunicații. - accesarea datelor SIS de pe rețele publice precum internetul nu trebuie să fie posibilă. - transmiterea parolelor și a altor elemente de securitate trebuie protejată prin metode de criptare.	- ar trebuie utilizate rețele/radio/faxuri criptate. - pentru schimbul de date cu caracter personal ar trebui utilizate mijloace securizate de comunicații între birourile SIRENE și birourile de pe teren / agenții operaționali. - ar trebui evitat accesul la internet prin intermediul rețelei polițienești.
5.6.6 Gestionarea suporturilor de date	
- numărul de copii tehnice ale datelor SIS trebuie redus la strictul necesar [a se vedea articolul 102 alineatul (2) din Convenția Schengen]. – Trebuie stabilite proceduri de gestionare și de stocare a datelor SIS, în vederea protejării acestora împotriva retransmisiei neautorizate sau a utilizării abuzive. - printre aceste proceduri ar trebui să se numere următoarele:	

• numai personalul autorizat ar trebui să aibă acces la suporturile informatice de stocare a datelor SIS; • toate suporturile care conțin date SIS trebuie să fie marcate și protejate corespunzător în timpul transportului; • suporturile învechite sau care nu mai sunt necesare trebuie făcute inutilizabile sau, în cazul în care sunt reutilizate, trebuie tratate în așa fel încât toate datele SIS să fie eliminate; • arhivele ar trebui să fie securizate; • accesul la arhive ar trebui să fie controlat și restrâns la personalul autorizat; • accesul la arhive ar trebui să fie monitorizat și înregistrat; • în gestionarea arhivelor ar trebui să se asigure aplicarea politicilor de ștergere.	- toate comunicațiile cu posturile consulare privind datele SIS trebuie să fie securizate. - ar trebui prevenită distribuirea eronată a datelor prin materiale reciclate necorespunzător, inclusiv hârtie. - înlocuirea suporturilor ar trebui efectuată de autoritățile competente sau de întreprinderi agreate/autorizate. - ar trebui instituite proceduri de stocare și de distrugere a materialelor și/sau de menținere a politicii „birourilor curate”. - arhivele electronice ar trebui să dispună de cele mai bune garanții de securitate, inclusiv înregistrarea accesului la fișiere și a utilizării acestora, precum și mecanisme de control. - se recomandă includerea în arhivele electronice a unor funcții automate de curățare și de ștergere. - în cazul arhivelor fizice, se consideră că cea mai bună soluție este fie o combinație între un card magnetic și un cod personal de acces la arhive, fie alte proceduri cu un nivel de securitate comparabil. - ar trebui evitate imprimările din arhivele electronice și, în orice caz, materialele respective ar trebui distruse după utilizare.
5.7 Controlul accesului utilizatorilor	
- trebuie instituită o procedură de înregistrare a utilizatorului, precum și una de anulare a înregistrării, în vederea acordării accesului la diferite sisteme și servicii. - această procedură trebuie să prevadă: • utilizarea de ID-uri unice pentru fiecare utilizator, pentru ca aceștia din urmă să își poată justifica acțiunile și să poată fi răspunzători pentru acestea; prin urmare, utilizarea ID-urilor de grup nu trebuie permisă; • fiecare utilizator trebuie să dispună numai de un număr minim de drepturi de acces necesare îndeplinirii obișnuite a sarcinilor care îi revin; • *retragerea imediată a drepturilor de acces la datele SIS atunci când utilizatorii în cauză nu își mai exercită funcțiile care necesitau accesul respectiv; • verificarea periodică a faptului că nivelul de acces acordat este în concordanță cu profilul utilizatorului; • verificarea periodică în vederea anulării ID-urilor și conturilor inutile.	- ar trebui să existe un sistem de validare a interogărilor pe bază de eșantioane. - aplicația poate avea o funcție tehnică prin care un cont de utilizator să fie închis automat dacă nu a fost utilizat o anumită perioadă, de exemplu două săptămâni. - ID-ul și contul de utilizator pot fi conectate automat la statutul personalului.

- alocarea și gestionarea parolelor trebuie controlate printr-o procedură formală, care să asigure că: • utilizatorii sunt informați și sunt conștienți parolele sunt comunicate de obligațiile lor în ceea ce privește parolele; * utilizatorilor prin mijloace sigure; • se solicită utilizatorilor să își schimbe periodic parola și se resping parolele reutilizate; • parolele nu sunt păstrate niciodată în sistemul informatic fără protecție. - trebuie instituită o procedură de asigurare a revizuirii periodice a tuturor drepturilor de acces ale utilizatorilor.	- parolele ar trebui schimbate la intervale de 60-90 de zile.
5.8 Monitorizarea accesului la sistem și a utilizării acestuia	
- utilizarea la nivel național a sistemelor IT Schengen trebuie monitorizată, în vederea asigurării detectării activităților neautorizate. - transmiterile de date cu caracter personal trebuie înregistrate în conformitate cu articolul 103 din Convenția Schengen. - jurnalul cu procedurile utilizatorilor de conectare și, în măsura posibilului, de deconectare, cu tentativele de conectare sau cu tentativele nereușite de conectare, precum și cu tentativele de utilizare neautorizată a datelor ar trebui păstrate pe perioada prevăzută la articolul 103 din Convenția Schengen. - datele înregistrate ar trebui să cuprindă ID-ul utilizatorului, data și ora incidentului și, dacă este posibil, identitatea și locația terminalului.	- jurnalele și pistele de audit referitoare la fișierele SIRENE ar trebui monitorizate proactiv și păstrate în conformitate cu legislația națională. - sistemele electronice de gestionare a fluxurilor de date / a dosarelor reprezintă cel mai bun mijloc de garantare a faptului că toate acțiunile întreprinse asupra unui fișier SIRENE sunt înregistrate și controlate.
5.9 Dezvoltare și întreținere	
- în vederea reducerii riscului de avariere a sistemelor operaționale, trebuie instituite măsuri de control al securității datelor și programelor.	
- ar trebui să se asigure, de exemplu, faptul că actualizarea sistemelor operaționale, inclusiv a bibliotecilor de programe, este efectuată numai cu aprobare prealabilă.	

- înainte de această aprobare, trebuie să se asigure faptul că au fost efectuate suficiente teste și documentări corespunzătoare în ceea ce privește actualizarea în cauză.	
- sistemele de testare trebuie prevăzute separat de mediul de producție, astfel încât schimbările să poată fi testate înainte de a deveni operaționale și nicio dată de test să nu fie introdusă în sistemul operațional. - trebuie să se evite orice utilizare a datelor SIS reale în scopuri de testare.	
5.10 Planurile de urgență	
- fiecare stat Schengen trebuie să stabilească și să pună în aplicare măsuri corespunzătoare de planificare în caz de urgență, ținând seama, de exemplu, de următoarele situații: • se semnalează imposibilitatea de a accesa N.SIS sau rețeaua; • toți utilizatorii sau o parte dintre ei nu pot căuta date SIS ca urmare a unor probleme în infrastructura IT națională. - planurile de urgență trebuie să se bazeze pe o evaluare a riscului amenințărilor care pot duce la imposibilitatea de a accesa sistemul și a impactului acestor amenințări asupra celorlalte state Schengen. - planurile de urgență trebuie să cuprindă cel puțin următoarele: • criteriile de punere în aplicare a planurilor și măsurile care trebuie luate imediat în vederea evaluării situației; • proceduri de prioritizare, în conformitate cu procedurile convenite pentru statele Schengen, în vederea informării administrațiilor naționale, C.SIS și a altor state Schengen; • proceduri de urgență care descriu măsurile ce trebuie luate în urma unui incident care perturbează accesul la sistem; • proceduri de rezervă care descriu măsurile ce trebuie luate în vederea transferării operațiilor esențiale ale N.SIS către alte servere provizorii; • proceduri de restabilire a sistemului, care descriu măsurile ce trebuie luate în vederea restabilirii funcționării normale.	

- planurile de urgență trebuie actualizate periodic, iar procedurile de intervenție a personalului trebuie testate de asemenea periodic.	
5.11 Controlul	
- trebuie instituite proceduri care să asigure controlul continuu al respectării legislației europene și naționale în vigoare, precum și a normelor administrative.	- ar trebui efectuate audituri periodice de securitate de către persoane externe departamentului IT.