Consiliul
Uniunii Europene

Bruxelles, 14 mai 2018
(OR. en)

8792/18

Dosar interinstituțional:
2018/0051 (NLE)

SCH-EVAL 102
COMIX 244

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	14 mai 2018
Destinatar:	Delegațiile
Nr. doc. ant.:	8285/18
Subiect:	Decizie de punere în aplicare a Consiliului de formulare a unei recomandări privind abordarea deficiențelor identificate în evaluarea din 2017 a aplicării de către **Portugalia** a acquis-ului Schengen în domeniul **protecției datelor**

În anexă, se pune la dispoziția delegațiilor decizia de punere în aplicare a Consiliului de formulare a unei recomandări privind abordarea deficiențelor identificate în evaluarea din 2017 a aplicării de către Portugalia a acquis-ului Schengen în domeniul protecției datelor, adoptată de Consiliu în cadrul reuniunii sale din 14 mai 2018.

În conformitate cu articolul 15 alineatul (3) din Regulamentul (UE) nr. 1053/2013 al Consiliului din 7 octombrie 2013, prezenta recomandare va fi înaintată Parlamentului European și parlamentelor naționale.

ANEXĂ

Decizie de punere în aplicare a Consiliului de formulare a unei

RECOMANDĂRI

privind abordarea deficiențelor identificate în evaluarea din 2017 a aplicării de către Portugalia a acquis-ului Schengen în domeniul protecției datelor

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) nr. 1053/2013 al Consiliului din 7 octombrie 2013 de instituire a unui mecanism de evaluare și monitorizare în vederea verificării aplicării acquis-ului Schengen și de abrogare a Deciziei Comitetului executiv din 16 septembrie 1998 de instituire a Comitetului permanent pentru evaluarea și punerea în aplicare a Acordului Schengen[1], în special articolul 15,

având în vedere propunerea Comisiei Europene,

întrucât:

(1) Scopul prezentei decizii este de a invita Portugalia să întreprindă acțiuni de remediere pentru a soluționa deficiențele identificate în cursul evaluării Schengen efectuate în 2017 în domeniul protecției datelor. În urma evaluării, s-a adoptat, prin Decizia de punere în aplicare [C(2018)1190] a Comisiei, un raport privind constatările și analizele, care enumeră bunele practici și deficiențele identificate în cursul evaluării.

(2) Echipa de la fața locului a salutat investiția continuă în formarea personalului tehnic realizată de autoritatea privind protecția datelor, considerând acest lucru ca fiind o bună practică.

[1] JO L 295, 6.11.2013, p. 27.

(3) Având în vedere importanța conformității cu acquis-ul Schengen, în special cu obligațiile de a garanta și a realiza o supraveghere eficace și de a asigura măsurile de securitate necesare, ar trebui să se acorde prioritate punerii în aplicare a recomandărilor 1, 4, 14, 17 și 22 de mai jos.

(4) Prezenta decizie ar trebui transmisă Parlamentului European și parlamentelor statelor membre. În termen de trei luni de la adoptarea acesteia, Portugalia elaborează, în temeiul articolului 16 alineatul (1) din Regulamentul (UE) nr. 1053/2013, un plan de acțiune privind remedierea deficiențelor identificate în raportul de evaluare și îl prezintă Comisiei și Consiliului,

RECOMANDĂ:

Portugaliei

Autoritatea de supraveghere în materie de protecție a datelor

1. să aloce autorității privind protecția datelor (denumită în continuare „APD”) suficiente resurse financiare și umane pentru ca aceasta să își poată îndeplini toate sarcinile care îi sunt încredințate în temeiul acquis-ului Sistemului de informații Schengen II (denumit în continuare „SIS II”) și al acquis-ului Sistemului de informații privind vizele (denumit în continuare „VIS”), având în vedere totodată și responsabilitățile sale sporite viitoare;

2. pentru a garanta independența deplină a APD, să acorde autonomie financiară APD în ceea ce privește execuția bugetului său anual și procesul de recrutare a personalului, cel puțin prin armonizarea normelor sale cu cele aplicabile în cadrul altor autorități independente din Portugalia;

3. să se asigure că ADP finalizează fără întârziere procedura referitoare la adoptarea rapoartelor în urma inspecției privind prelucrarea datelor cu caracter personal în cadrul SIS II;

4. să se asigure că ADP finalizează auditul VIS fără întârziere;

Drepturile persoanelor vizate

5. să se asigure că persoanele vizate sunt informate cu privire la drepturile lor în ceea ce privește SIS II prin intermediul site-ului web al *Serviço de Estrangeiros e Fronteiras* (Serviciul pentru Imigrație și Frontiere, denumit în continuare „SEF”);

6. să se asigure că persoanele vizate, în urma solicitărilor acestora de a-și accesa datele cu caracter personal, sunt informate cu privire la categoriile de date prelucrate efectiv în SIS II;

7. să se asigure că persoanele vizate beneficiază de informații clare cu privire la identitatea operatorului care prelucrează datele lor cu caracter personal în cadrul procesului de eliberare a vizelor Schengen;

Sistemul de informații privind vizele

8. să clarifice situația privind controlul asupra prelucrării datelor cu caracter personal în N.VIS [prin includerea aplicațiilor utilizate atât de Ministerul Afacerilor Externe (denumit în continuare „MAE”), cât și de SEF și centrele de date relevante], în special prin clarificarea rolului MAE și a procesului de alocare a responsabilităților legate de prelucrarea datelor cu caracter personal între SEF și MAE;

9. să se asigure că MAE efectuează activități de supraveghere sistematice care permit o evaluare pertinentă a aspectelor legate de prelucrarea datelor cu caracter personal de către prestatorul extern de servicii (denumit în continuare „PES”). În această privință, Portugalia este încurajată să extindă chestionarul pe care MAE îl trimite PES pentru a acoperi mai detaliat aspectele legate de protecția datelor și să consolideze activitățile de supraveghere ale MAE legate de protecția datelor efectuată de PES și de subcontractant, după caz;

10. să asigure o procedură care să permită verificarea rezultatelor pozitive furnizate de SIS II în cadrul procedurii de acordare a vizelor;

11. să se asigure că parolele tuturor utilizatorilor N.VIS sunt criptate;

12. să se asigure că SEF și MAE analizează în mod regulat fișierele-jurnal pentru a garanta monitorizarea protecției datelor;

13. să se asigure că MAE efectuează în mod regulat automonitorizarea prelucrării datelor cu caracter personal în cadrul sistemului RPV și al centrelor de date;

14. să se asigure că MAE adoptă fără întârziere un plan de securitate pentru sistemul RPV și pentru centrele de date relevante;

15. să pună în aplicare pe deplin Decizia 2008/633/JAI a Consiliului din 23 iunie 2008 privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave și să se asigure că accesul la datele N.VIS respectă cerințele și procedura stabilite în actul respectiv;

16. să se asigure că PES șterge datele cu caracter personal ale solicitanților care sunt stocate în sistemele sale, în concordanță cu termenele prevăzute în anexa X partea A litera (d) din Codul de vize, solicitând ca astfel de date să fie șterse imediat după transmiterea acestora către consulat;

Sistemul de informații Schengen II

17. să asigure un amplasament de siguranță complet pentru N.SIS II, care să pună la dispoziție funcționalități complete, inclusiv conectarea la infrastructura de comunicații sTESTA;

18. să clarifice responsabilitățile părților implicate în prelucrarea datelor N.SIS II, în special ale operatorului și ale autorităților care accesează și utilizează SIS II, în ceea ce privește securitatea informatică, controlul și automonitorizarea sistemului, de exemplu prin încheierea de acorduri între operator și autoritățile care accesează SIS II;

19. să pună în aplicare un sistem de gestionare a utilizatorilor care să permită o automonitorizare eficace pe baza registrelor centrale ale operatorului care prelucrează datele N.SIS II, fără a fi necesară consultarea registrelor deținute de autoritățile care utilizează sistemul;

20. să se asigure că SEF analizează în mod regulat fișierele-jurnal pentru a garanta monitorizarea protecției datelor;

21. să se asigure că mediile informatice folosite de utilizatorii cu drepturi extinse de acces sau de editare în ceea ce privește N.SIS II (cum ar fi membrii Biroului SIRENE) sunt separate logic sau fizic de accesul la internet;

22. să se asigure că operatorul criptează benzile de siguranță și hard diskurile N.SIS;

23. să se asigure că profilurile de utilizatori cu drepturi extinse de acces sau de editare în ceea ce privește datele N.SIS II (cum ar fi membrii Biroului SIRENE) sunt securizate printr-o metodă obligatorie de autentificare bazată pe doi factori;

24. să se asigure că SEF își consolidează activitățile legate de automonitorizarea prelucrării datelor cu caracter personal în cadrul N.SIS și desfășoară în mod regulat astfel de activități; Portugalia este încurajată să aloce SEF suficiente resurse financiare și umane pentru a asigura eficacitatea și continuitatea auditării interne și ale securității informatice, în special asigurându-se că este ocupat postul privind securitatea informatică din cadrul Diviziei de tehnologia informației a SEF;

Sensibilizarea publicului

25. să se asigure că site-ul web al SEF furnizează linkuri către site-ul web al ADP.

Adoptată la Bruxelles,

Pentru Consiliu,
Președintele