Consiliul
Uniunii Europene

Bruxelles, 22 februarie 2022
(OR. en)

6426/22

Dosar interinstituțional:
2021/0392(NLE)

SCH-EVAL 21
DATAPROTECT 42
COMIX 87

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	21 februarie 2022
Destinatar:	Delegațiile
Nr. doc. ant.:	5893/22
Subiect:	Decizie de punere în aplicare a Consiliului de formulare a unei recomandări privind soluționarea deficiențelor identificate în evaluarea din 2019 referitoare la aplicarea de către **Polonia** a acquis-ului Schengen în domeniul **protecției datelor**

În continuare, se pune la dispoziția delegațiilor Decizia de punere în aplicare a Consiliului de formulare a unei recomandări privind soluționarea deficiențelor identificate în evaluarea din 2019 referitoare la aplicarea de către Polonia a acquis-ului Schengen în domeniul protecției datelor, adoptată de Consiliu în cadrul reuniunii sale din 21 februarie 2022.

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

Decizie de punere în aplicare a Consiliului de formulare a unei

RECOMANDĂRI

privind soluționarea deficiențelor identificate în evaluarea din 2019 referitoare la aplicarea de către Polonia 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) În conformitate cu Regulamentul (UE) nr. 1053/2013, în 2019 a fost efectuată o evaluare în vederea verificării aplicării acquis-ului Schengen în domeniul protecției datelor cu caracter personal în Polonia. În urma evaluării s-a adoptat, prin Decizia de punere în aplicare C(2021)9100 a Comisiei, un raport privind constatările și analizele, care include bunele practici și deficiențele identificate în cursul evaluării.

(2) Având în vedere rezultatele evaluării, este oportun să se recomande Poloniei anumite acțiuni de remediere pentru soluționarea deficiențelor identificate.

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

(3) Sunt considerate bune practici, în special: cadrul juridic național, care îi permite președintelui autorității poloneze pentru protecția datelor (APD) să își numească în mod independent adjuncții, precum și membrii Consiliului consultativ; obligația candidaților la funcția de președinte al APD de a se supune unei audieri publice în Parlament, care este transmisă și pe internet prin intermediul canalului oficial al Parlamentului; activitățile frecvente de control în ceea ce privește prestatorii externi de servicii, cu implicarea responsabilului cu protecția datelor, și controalele frecvente ale consulatelor; angajamentul de a asigura formarea și perfecționarea profesională a personalului, inclusiv în ceea ce privește protecția datelor, pentru utilizatorii finali ai Sistemului național de informații Schengen (N.SIS) și pentru personalul biroului SIRENE; măsurile de securitate puse în aplicare la sediile celor două centre de date care găzduiesc N.SIS și Sistemul național de informații privind vizele (N.VIS).

(4) Având în vedere importanța respectării acquis-ului Schengen privind protecția datelor cu caracter personal în ceea ce privește Sistemul de informații privind vizele (VIS) și Sistemul de informații Schengen (SIS), ar trebui să se acorde prioritate punerii în aplicare a recomandărilor 11, 12, 13, 20, 21 și 22 prevăzute în prezenta decizie.

(5) În temeiul Regulamentului (UE) nr. 1053/2013, prezenta decizie ar trebui să fie transmisă Parlamentului European și parlamentelor statelor membre, iar Polonia ar trebui să elaboreze, în termen de trei luni de la adoptarea sa, un plan de acțiune care să cuprindă o listă cu toate recomandările de remediere a eventualelor deficiențe identificate în raportul de evaluare și să transmită planul de acțiune respectiv Comisiei și Consiliului,

RECOMANDĂ:

Poloniei:

Legislație

1. să clarifice explicit aplicabilitatea Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor - RGPD) în cazul prelucrării datelor cu caracter personal în sistemele N.VIS și N.SIS, acolo unde este relevant;

Autoritatea de protecție a datelor

2. să se asigure că articolul 174 din Legea privind protecția datelor din 2018 și articolul 106 din Legea privind protecția datelor în materie de asigurare a respectării legii din 2018, care prevede limita maximă a cheltuielilor pentru fiecare an, nu limitează bugetul autorității poloneze pentru protecția datelor (APD) la un nivel inferior sumelor alocate în bugetul de stat pentru anul respectiv;

3. să se asigure că APD își planifică și își organizează mai bine numeroasele inspecții ale N.SIS II, astfel încât să garanteze că sunt acoperite toate operațiunile de prelucrare ale N.SIS II și toate entitățile relevante și că inspecțiile au drept rezultat un audit cuprinzător al N.SIS II, astfel cum se prevede la articolul 44 alineatul (2) din Regulamentul (CE) nr. 1987/2006;

4. să se asigure că APD efectuează o inspecție cuprinzătoare a N.VIS, astfel încât să își îndeplinească pe deplin sarcinile în conformitate cu articolul 41 alineatul (2) din Regulamentul (CE) nr. 767/2008;

Drepturile persoanelor vizate

5. să se asigure că statisticile APD referitoare la exercitarea drepturilor persoanelor vizate sunt îmbunătățite și disting clar plângerile de cereri, sistemul la care se referă (SIS sau VIS), obiectul și tipul cererii (corectare, ștergere, acces);

6. să se asigure că operatorul de date adoptă o abordare mai proactivă în furnizarea de informații privind drepturile persoanelor vizate în legătură cu datele VIS;

7. să se asigure că operatorul de date SIS și VIS [Poliția Națională Poloneză – Autoritatea Tehnică Centrală pentru Sistemul Informatic Național (CTA NITS)] publică formulare standard pentru cererile de exercitare a drepturilor persoanelor vizate;

Sistemul de informații privind vizele

8. să se asigure că registrele de acces la VIS conțin, de asemenea, informații cu privire la justificarea accesului în cauză;

9. să reevalueze lista autorităților care au acces la VIS și drepturile lor de acces la datele VIS, având în vedere competențele acestora și utilizarea în practică a datelor respective;

10. având în vedere multitudinea de operatori VIS, generată de legislația națională și de dispozițiile contractuale, precum și multitudinea de actori implicați, să clarifice relația dintre autoritățile implicate în procesul de eliberare a vizelor și autoritățile care prelucrează datele VIS, precum și responsabilitățile acestor autorități în ceea ce privește prelucrarea datelor;

11. să se asigure că, pentru a utiliza pe deplin fișierele-jurnal păstrate, fișierele-jurnal VIS sunt analizate în mod regulat în vederea monitorizării protecției datelor;

12. să adopte un plan de securitate VIS care să vizeze securitatea fizică a celui de al doilea centru de date, precum și alte aspecte de securitate informatică a sistemului informatic național, inclusiv a sistemului N.VIS;

13. să alinieze perioada de păstrare a fișierelor-jurnal ale aplicațiilor legate de VIS (în special aplicațiile „Pobyt” și „ZSE 6”) la perioadele prevăzute la articolul 34 alineatul (2) din Regulamentul (CE) nr. 767/2008 și la articolul 16 din Decizia 2008/633/JAI a Consiliului;

Sistemul de informații Schengen II

14. să se asigure că operatorul N.SIS II instituie un sistem central de gestionare a utilizatorilor care permite o automonitorizare eficace, fără să fie necesară consultarea fișierelor-jurnal ale instituțiilor care sunt utilizatori finali ai sistemului N.SIS II;

15. să se asigure că, pentru a utiliza pe deplin fișierele-jurnal păstrate, fișierele-jurnal din SIS sunt analizate în mod regulat în vederea monitorizării protecției datelor;

16. să asigure o notificare automată a evenimentelor de securitate informatică și a activităților de automonitorizare ale operatorului de date, pentru a îmbunătăți și mai mult securitatea;

17. să se asigure că măsurile tehnice includ și blocarea utilizării dispozitivelor sau a unităților flash pentru USB, prin blocarea tuturor porturilor USB de pe stațiile de lucru SIS;

18. să aibă în vedere implicarea proactivă și regulată a responsabilului cu protecția datelor (RPD) din cadrul Ministerului de Interne în monitorizarea prelucrării datelor SIS și VIS prin monitorizarea registrelor de audit;

19. să se asigure că operatorul de date SIS pune la dispoziția APD profilurile membrilor personalului tuturor autorităților care au acces la SIS;

20. să se asigure că perioada de păstrare a fișierelor-jurnal ale aplicațiilor care au acces la datele SIS este conformă cu articolul 12 alineatul (4) din Regulamentul (CE) nr. 1987/2006 și cu articolul 12 alineatul (4) din Decizia 2007/533/JAI a Consiliului;

21. să se asigure că, în conformitate cu articolul 10 din Regulamentul (CE) nr. 1987/2006 și cu articolul 10 din Decizia 2007/533/JAI a Consiliului, operatorul de date SIS adoptă un plan de securitate SIS;

22. să se asigure că se reevaluează paleta largă de instituții care au acces la datele din SIS II, astfel încât să garanteze că numai instituțiile care au nevoie de acces, având în vedere competențele și nevoile lor practice, pot accesa datele;

Sensibilizarea publicului

23. să se asigure că pe site-urile web ale APD și ale poliției se furnizează informații cu privire la drepturile persoanelor vizate în legătură cu datele VIS.

Adoptată la Bruxelles,

Pentru Consiliu
Președintele