Consiliul
Uniunii Europene

Bruxelles, 25 ianuarie 2021
(OR. en)

5534/21

Dosar interinstituțional:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Destinatar:	Delegațiile
Nr. doc. ant.:	14250/20
Subiect:	Decizie de punere în aplicare a Consiliului de formulare a unei recomandări privind remedierea deficiențelor identificate în cadrul evaluării din 2019 referitoare la aplicarea de către **Slovacia** 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 remedierea deficiențelor identificate în cadrul evaluării din 2019 referitoare la aplicarea de către Slovacia a acquis-ului Schengen în domeniul protecției datelor, adoptată prin procedură scrisă la 21 ianuarie 2021.

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 remedierea deficiențelor identificate în cadrul evaluării din 2019 referitoare la aplicarea de către Slovacia 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 acela de a recomanda Republicii Slovace să întreprindă acțiuni de remediere menite să elimine deficiențele identificate în cursul evaluării Schengen efectuate în 2019 în domeniul protecției datelor. În urma evaluării a fost adoptat, prin Decizia de punere în aplicare (2020)8160 a Comisiei, un raport care cuprinde constatări și evaluări și prezintă bunele practici și deficiențele identificate în cursul evaluării.

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

(2) Sunt considerate bune practici, printre altele, faptul că, de la ultima evaluare Schengen din 2012, Autoritatea pentru protecția datelor (APD) a desfășurat în mod regulat activități de supraveghere a SIS II, în conformitate cu o planificare anuală, și faptul că a fost elaborat un concept pentru inspecțiile SIS II pentru următorii patru ani; faptul că APD a efectuat un număr considerabil de inspecții referitoare la VIS în consulate; eforturile depuse de APD și de Ministerul de Interne (MI) pentru a furniza informații persoanelor vizate, pe suporturi electronice și tipărite; existența unor versiuni multilingve ale informațiilor referitoare la subiecte legate de Schengen pe site-ul web al APD și în broșuri; faptul că APD a furnizat modele pentru cererile formulate de persoanele vizate ale căror date sunt stocate în SIS și în VIS; faptul că biroul SIRENE oferă răspunsuri la cereri nu numai în limba slovacă, ci și în limba engleză; faptul că autoritățile slovace informează persoanele vizate dacă nu există date referitoare la acestea stocate în SIS II; controlul foarte activ al jurnalelor VIS și SIS II de către unitatea „Inspecții” a serviciului Biroului de inspecție din cadrul MI; rolul foarte activ al celor doi membri ai personalului din cadrul Departamentului de securitate al Ministerului Afacerilor Externe și Europene (MAEE), care se ocupă de chestiuni legate de protecția datelor; faptul că MAEE oferă formare în domeniul protecției datelor personalului său, în special înainte de detașarea temporară pentru sarcini consulare, și că Departamentul de securitate (în calitatea sa de birou responsabil de protecția datelor) oferă această formare; nivelul ridicat de securitate procedurală și fizică instituit pentru protejarea datelor SIS II; rolul foarte activ al responsabilului cu protecția datelor și al responsabilului adjunct cu protecția datelor în cadrul Departamentului pentru protecția datelor din unitatea „Inspecții” a serviciului Biroului de inspecție din cadrul MI, inclusiv în materie de orientări și de control al jurnalelor în ceea ce privește SIS II; faptul că MI oferă formare în materie de protecție a datelor tuturor utilizatorilor finali ai sistemului național de SIS II (N.SIS II).

(3) Având în vedere importanța respectării acquis-ului Schengen în ceea ce privește protecția datelor în contextul VIS, ar trebui să se acorde prioritate punerii în aplicare a recomandărilor 7 și 24.

(4) Prezenta decizie ar trebui să fie transmisă Parlamentului European și parlamentelor statelor membre. În termen de trei luni de la adoptarea acesteia, Republica Slovacă ar trebui să elaboreze, în temeiul articolului 16 alineatul (1) din Regulamentul (UE) nr. 1053/2013, un plan de acțiune care să cuprindă o listă cu toate recomandările pentru remedierea deficiențelor identificate în raportul de evaluare și să transmită Comisiei și Consiliului respectivul plan de acțiune,

RECOMANDĂ:

Republicii Slovace, cu privire la:

Autoritatea pentru protecția datelor

1. să se asigure că, pentru a consolida performanța și eficacitatea APD, se suplimentează în continuare bugetul și efectivele de personal ale APD;

2. să se asigure că partea din bugetul general de stat prevăzută pentru APD este clar vizibilă pentru a garanta că APD dispune de un buget anual public separat;

3. să se asigure că, în cadrul procedurii bugetare, Consiliul național este informat cu privire la poziția APD referitoare la nevoile sale bugetare și la discuțiile purtate între APD și Ministerul Finanțelor (MF) cu privire la buget;

4. să ia măsuri astfel încât MF să nu poată face nicio corelație între buget și cuantumul amenzilor care urmează să fie colectate de către APD, întrucât acest lucru ar putea avea un impact asupra naturii și a prioritizării activității APD și, prin urmare, i-ar afecta independența. Ar trebui să se garanteze că bugetul APD nu poate fi diminuat în cursul anului calendaristic în situația în care amenzile estimate nu au fost integral colectate de APD;

5. să se asigure că toate sarcinile și competențele conferite autorităților pentru protecția datelor la articolele 57 și 58 din RGPD vor fi acordate APD;

6. să se asigure că, pe lângă activitățile periodice de supraveghere desfășurate la biroul N.SIS și la biroul SIRENE, APD supraveghează mai multe autorități care sunt utilizatori finali și care au acces la SIS II;

7. să se asigure că activitățile de supraveghere ale APD referitoare la VIS includ inspectarea Autorității centrale în materie de vize (ACV) în ceea ce privește operațiunile de prelucrare a datelor în N.VIS. Întrucât termenul pentru primul audit al sistemului național de vize a fost octombrie 2015, APD ar trebui să efectueze această parte a auditului care nu a fost încă finalizată, cât mai curând posibil;

8. să se asigure că APD inspectează, de asemenea, în mod regulat prestatorii externi de servicii (PES);

Drepturile persoanelor vizate

9. să găsească o modalitate adecvată pentru APD, MI și MAEE de a informa persoanele vizate cu privire la riscurile potențiale generate de transmiterea de copii ale cărților de identitate și de informații sensibile prin intermediul internetului deschis. MI și MAEE sunt invitate să ia în considerare posibilitatea de a oferi persoanelor vizate un canal de transmisie electronică securizat pentru comunicarea unor astfel de documente;

10. să se asigure că termenul de 60 de zile pentru transmiterea răspunsului la o cerere SIS II din partea unei persoane vizate, prevăzut la articolul 41 alineatul (6) din Regulamentul SIS II și la articolul 58 alineatul (6) din Decizia SIS II, este respectat până când noul acquis SIS[1] va deveni pe deplin aplicabil (cel mai târziu la 28 decembrie 2021), acesta conținând referințe încrucișate la termenul de răspuns la cererile din partea persoanelor vizate prevăzut în RGPD (30 de zile cu posibilitatea prelungirii cu alte două luni dacă este necesar);

11. să aibă în vedere furnizarea anumitor informații imprimate (broșuri/postere etc.) destinate persoanelor vizate în incinta secțiilor de poliție, precum și să asigure faptul că acestea sunt vizibile și ușor accesibile;

12. să aibă în vedere să pună la dispoziție, de exemplu, o versiune informală în limba engleză a deciziilor APD referitoare la plângerile legate de cererile SIS II din partea persoanelor vizate; acest lucru ar ajuta persoanele vizate să înțeleagă mai bine decizia și ar consolida astfel drepturile persoanelor vizate;

13. să se asigure că informațiile privind drepturile persoanelor vizate ale căror date sunt stocate în VIS sunt mai ușor de găsit pe site-ul MAEE; site-ul respectiv ar trebui să conțină, de asemenea, modele-standard pe baza cărora persoanele vizate să își poată exercita drepturile;

---

[1] Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei, JO L 312, 7.12.2018, p. 56 (a se vedea, în special, articolele 66-71); Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției de punere în aplicare a Acordului Schengen și de modificare și abrogare a Regulamentului (CE) nr. 1987/2006, JO L 312, 7.12.2018, p. 14 (a se vedea, în special, articolele 51-57).

14. să se asigure că formularul de cerere de viză conține informații clare cu privire la diferitele autorități care prelucrează datele cu caracter personal în cadrul sistemului național de vize. În special, ar trebui să se indice faptul că MAEE este operatorul de date;

15. să furnizeze persoanelor vizate ale căror date sunt stocate în VIS informații fizice (broșuri/postere etc.) în incinta aeroporturilor și a altor puncte de control la frontieră și să asigure faptul că acestea sunt vizibile și ușor accesibile;

16. să se asigure că răspunsurile adresate persoanelor vizate referitoare la datele cu caracter personal stocate în VIS oferă informații cu privire la posibilitatea de a introduce o cale de atac împotriva răspunsului în fața APD și a instanței competente;

17. să ia măsurile necesare pentru a clarifica responsabilitățile MAEE și ale ACV (MI) în ceea ce privește tratarea solicitărilor persoanelor vizate ale căror date sunt stocate în VIS și să elaboreze orientări interne sau metodologice pentru ambele entități; aceste informații ar trebui să fie puse la dispoziția persoanelor vizate;

Sistemul de informații privind vizele

18. să ia măsurile necesare pentru a spori nivelul de securitate pentru accesul la mediul guvernamental și, în special, la cererile naționale referitoare la vize din cadrul MAEE și al MI (ACV), în special printr-un acces la bazele de date naționale privind vizele prin intermediul tehnologiei multifactor;

19. să ia măsurile necesare pentru a îmbunătăți securitatea fizică și organizațională în centrul de date N.VIS al MAEE, în special cu privire la următoarele aspecte:

   - - instituirea unui registru pentru vizitatori la intrarea în centrul de date pentru personalul TIC, vizitatori sau furnizori al căror acces ar trebui să fie limitat;
   - - instalarea unui sistem de stingere a incendiilor cu gaz (aragonit);
   - - instalarea unui sistem de detectare a scurgerilor de apă;
   - - asigurarea unei podele curate și fără praf;
   - - blocarea barierei de protecție a serverelor UE;

20. să accelereze procedura de înființare a unui nou centru de date N.VIS într-un alt loc și relocarea centrului de date;

21. să aibă în vedere modificarea perioadei de păstrare locală a fișierelor-jurnal ale N.VIS la misiunile diplomatice și consulare, stabilind o perioadă de timp în locul unui volum de MB;

22. să aibă în vedere utilizarea sistemelor pentru controlul automat al jurnalelor în cadrul MAEE;

23. să ia măsurile necesare astfel încât misiunile diplomatice sau MAEE să inspecteze PES în mod regulat;

24. să ia măsurile necesare pentru a asigura o formare în domeniul protecției datelor pentru personalul consular local într-un mod mai sistematic și uniform;

25. să se asigure că în cererea de viză electronică se solicită aceleași informații ca și în formularul de cerere de viză pe hârtie (astfel cum se prevede în anexa I la Codul de vize al UE[1]);

Sistemul de informații Schengen II

26. să ia măsurile necesare pentru a îmbunătăți nivelul de securitate al accesului la N.SIS II, în special prin utilizarea autentificării multifactor și recurgerea numai la conexiuni https pentru accesul la N.SIS II;

27. să se asigure că MI informează APD cu privire la orice încălcare a securității datelor care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. De asemenea, MI ar trebui să instituie un registru al încălcărilor securității datelor cu caracter personal;

[1] Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului din 13 iulie 2009 privind instituirea unui Cod comunitar de vize (Codul de vize). JO L 243, 15.9.2009, p. 1.

Sensibilizarea publicului

28. să ia în considerare posibilitatea de a pune broșurile APD la dispoziția persoanelor vizate și în locuri mai accesibile, cum ar fi secțiile de poliție, zonele de control la frontiere și sediile consulare;

29. să aibă în vedere permiterea accesului la prezentările, seminarele și evenimentele de tipul porților deschise organizate de APD și pentru publicul larg, în special pentru persoanele vizate, întrucât acestea sunt interesate de informațiile privind SIS II și VIS.

Adoptată la Bruxelles,

Pentru Consiliu,
Președintele