Eiropas Savienības
Padome

Briselē, 2021. gada 25. janvārī
(OR. en)

5534/21

Starpiestāžu lieta:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Saņēmējs:	delegācijas
Iepr. dok. Nr.:	14250/20
Temats:	Padomes Īstenošanas lēmums, kurā izklāsta ieteikumu par to trūkumu novēršanu, kas konstatēti 2019. gada izvērtēšanā par to, kā **Slovākija** piemēro Šengenas *acquis* **datu aizsardzības** jomā

Pielikumā ir pievienots Padomes Īstenošanas lēmums, kurā izklāsta ieteikumu par to trūkumu novēršanu, kas konstatēti 2019. gada izvērtēšanā par to, kā Slovākija piemēro Šengenas *acquis* datu aizsardzības jomā, ko ar rakstisko procedūru pieņēma 2021. gada 21. janvārī.

Saskaņā ar Padomes Regulas (ES) Nr. 1053/2013 (2013. gada 7. oktobris) 15. panta 3. punktu šis ieteikums tiks nosūtīts Eiropas Parlamentam un valstu parlamentiem.

Padomes Īstenošanas lēmums, kurā izklāsta

IETEIKUMU

par to trūkumu novēršanu, kas konstatēti 2019. gada izvērtēšanā par to, kā Slovākija piemēro Šengenas *acquis* datu aizsardzības jomā

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Padomes Regulu (ES) Nr. 1053/2013 (2013. gada 7. oktobris), ar ko izveido izvērtēšanas un uzraudzības mehānismu, lai pārbaudītu Šengenas *acquis* piemērošanu, un ar ko atceļ Izpildu komitejas lēmumu (1998. gada 16. septembris), ar ko izveido Šengenas izvērtēšanas un īstenošanas pastāvīgo komiteju [1], un jo īpaši tās 15. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

tā kā:

(1) Šā lēmuma mērķis ir ieteikt Slovākijas Republikai korektīvas darbības, lai novērstu trūkumus, kas konstatēti 2019. gadā veiktajā Šengenas izvērtēšanā datu aizsardzības jomā. Pēc izvērtēšanas pabeigšanas ar Komisijas Īstenošanas lēmumu C(2020) 8160 tika pieņemts ziņojums par konstatējumiem un izvērtējumiem, kurā norādīta izvērtēšanas laikā konstatētā paraugprakse un trūkumi.

[1] OV L 295, 6.11.2013., 27. lpp.

(2) Par labu praksi cita starpā tiek uzskatīts tas, ka kopš pēdējā Šengenas izvērtējuma 2012. gadā Datu aizsardzības iestāde (DAI) ir regulāri veikusi *SIS II* uzraudzības darbības saskaņā ar gada plānošanu un ir izstrādāta *SIS II* pārbaužu koncepcija nākamajiem četriem gadiem; DAI ir veikusi ievērojamu skaitu VIS pārbaužu konsulātos; DAI un Iekšlietu ministrijas (IM) centieni sniegt datu subjektiem informāciju, izmantojot elektroniskus un drukātus materiālus; DAI tīmekļa vietnē un brošūrās pieejamās informācijas par tematiem, kas saistīti ar Šengenu, daudzvalodu versijas; ka DAI nodrošina veidnes *SIS* un VIS datu subjektu pieprasījumiem; ka *SIRENE* birojs sniedz atbildes uz pieprasījumiem ne tikai slovāku valodā, bet arī angļu valodā; ka Slovākijas iestādes informē datu subjektus, ja *SIS II* netiek glabāti dati par tiem; ļoti aktīvā VIS un *SIS II* reģistra kontrole, ko veic Iekšlietu ministrijas Inspekcijas dienesta biroja pārbaužu nodaļa; Ārlietu un Eiropas lietu ministrijas (*MFEA*) Drošības departamenta abu darbinieku ļoti aktīvā loma datu aizsardzības jautājumos; ka *MFEA* nodrošina datu aizsardzības apmācību saviem darbiniekiem, jo īpaši pirms pagaidu norīkošanas konsulāro uzdevumu veikšanai, un ka Drošības departaments (darbojoties kā datu aizsardzības speciālista birojs) nodrošina šo apmācību; ka procesuālā un fiziskā drošība, kas izveidota *SIS II* datu aizsardzībai, ir augstā līmenī; datu aizsardzības speciālista un viņa vietnieka ļoti aktīvā loma Iekšlietu ministrijas Inspekcijas dienesta biroja pārbaužu nodaļas Datu aizsardzības departamentā, tai skaitā attiecībā uz norādījumiem un reģistra kontroli saistībā ar *SIS II*; ka Iekšlietu ministrija nodrošina datu aizsardzības apmācību visiem *N.SIS II* galalietotājiem.

(3) Ņemot vērā to, cik svarīgi ir ievērot Šengenas *acquis* par datu aizsardzību saistībā ar VIS, prioritārā kārtā būtu jāīsteno 7. un 24. ieteikums.

(4) Šis lēmums būtu jānosūta Eiropas Parlamentam un dalībvalstu parlamentiem. Trīs mēnešu laikā pēc lēmuma pieņemšanas Slovākijas Republikai, ievērojot Regulas (ES) Nr. 1053/2013 16. panta 1. punktu, būtu jāizstrādā rīcības plāns – kurā norādīti visi ieteikumi – par to, kā novērst izvērtēšanas ziņojumā konstatētos trūkumus, un jāiesniedz tas Komisijai un Padomei,

IESAKA.

ka Slovākijas Republikai būtu:

Datu aizsardzības iestāde

1. jānodrošina, ka nolūkā pastiprināt DAI darbību un efektivitāti tiktu vēl vairāk palielināts DAI budžets un personāls;

2. jānodrošina, ka daļa no kopējā valsts budžeta, kas paredzēts DAI, būtu skaidri redzama, lai garantētu, ka DAI ir atsevišķs, publisks gada budžets;

3. jānodrošina, ka budžeta procedūrā Valsts padome tiktu informēta par DAI nostāju attiecībā uz tās budžeta vajadzībām un diskusijām starp DAI un Finanšu ministriju par budžetu;

4. jāveic pasākumi, lai Finanšu ministrija nevarētu veikt nekādu korelāciju starp budžetu un DAI iekasējamo naudas sodu summu, jo tas varētu ietekmēt DAI darba būtību un prioritātes un tādējādi ietekmēt tās neatkarību. Būtu jāgarantē, ka DAI budžetu nevar samazināt kalendārā gada laikā situācijā, kad DAI nav pilnībā iekasējusi aplēstos naudas sodus;

5. jānodrošina, ka DAI tiek piešķirti visi uzdevumi un pilnvaras, kas datu aizsardzības iestādēm paredzēti VDAR 57. un 58. pantā;

6. jānodrošina, ka papildus regulārajām uzraudzības darbībām, ko veic *N.SIS* birojā un *SIRENE* birojā, DAI uzrauga vairāk galalietotāju iestāžu, kurām ir piekļuve *SIS II*;

7. jānodrošina, ka DAI veiktās uzraudzības darbības saistībā ar VIS ietver Centrālās vīzu iestādes pārbaudi attiecībā uz datu apstrādes darbībām N.VIS. Tā kā valsts vīzu sistēmas pirmās revīzijas termiņš bija 2015. gada oktobris, DAI pēc iespējas ātrāk būtu jāveic šī vēl trūkstošā revīzijas daļa;

8. jānodrošina, ka DAI regulāri pārbauda arī ārpakalpojumu sniedzējus (*ESP*);

Datu subjektu tiesības

9. būtu jārod piemērots veids, kādā DAI, Iekšlietu ministrija un *MFEA* informē datu subjektus par iespējamiem riskiem, kas saistīti ar personas apliecību kopiju un sensitīvas informācijas iesniegšanu, izmantojot atklātu internetu. Iekšlietu ministrija un *MFEA* tiek aicinātas apsvērt iespēju piedāvāt datu subjektiem drošu elektroniskās informācijas pārraides kanālu šādu dokumentu iesniegšanai;

10. jānodrošina, ka *SIS II* regulas 41. panta 6. punktā un *SIS II* lēmuma 58. panta 6. punktā noteiktais 60 dienu termiņš atbildes sniegšanai uz *SIS II* datu subjektu pieprasījumiem tiek ievērots līdz brīdim, kad pilnībā sāks piemērot jauno *SIS acquis* [1] (vēlākais, līdz 2021. gada 28. decembrim), kurā ir savstarpējas atsauces uz VDAR paredzēto termiņu atbildes sniegšanai uz datu subjektu pieprasījumiem (30 dienas ar iespēju vajadzības gadījumā pagarināt vēl par diviem mēnešiem);

11. jāapsver iespēja daļu drukātās informācijas (brošūras/norādes utt.) sniegt datu subjektiem policijas iecirkņu telpās, kā arī padarīt to redzamu un viegli pieejamu;

12. jāapsver iespēja nodrošināt, piemēram, neoficiālu versiju angļu valodā DAI lēmumiem par sūdzībām saistībā ar *SIS II* datu subjektu pieprasījumiem; tas palīdzētu datu subjektiem labāk izprast lēmumu un tādējādi stiprinātu datu subjektu tiesības;

13. jānodrošina, ka *MFEA* tīmekļa vietnē ir vieglāk atrast informāciju par VIS datu subjektu tiesībām; tīmekļa vietnē būtu jāparedz arī veidnes VIS datu subjektu tiesību īstenošanai;

---

[1] Eiropas Parlamenta un Padomes Regula (ES) 2018/1862 (2018. gada 28. novembris) par Šengenas Informācijas sistēmas (*SIS*) izveidi, darbību un izmantošanu policijas sadarbībā un tiesu iestāžu sadarbībā krimināllietās un ar ko groza un atceļ Padomes Lēmumu 2007/533/TI un atceļ Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1986/2006 un Komisijas Lēmumu 2010/261/ES (OV L 312, 7.12.2018., 56. lpp.) (skatīt jo īpaši 66.–71. pantu); Eiropas Parlamenta un Padomes Regula (ES) 2018/1861 (2018. gada 28. novembris) par Šengenas Informācijas sistēmas (*SIS*) izveidi, darbību un izmantošanu robežpārbaužu jomā un ar kuru groza Konvenciju, ar ko īsteno Šengenas nolīgumu, un groza un atceļ Regulu (EK) Nr. 1987/2006 (OV L 312, 7.12.2018., 14 lpp.) (skatīt jo īpaši 51.–57. pantu).

14. jānodrošina, ka vīzas pieteikuma veidlapā ir skaidra informācija par dažādajām iestādēm, kas apstrādā personas datus valsts vīzu sistēmas ietvaros. Jo īpaši vajadzētu būt informācijai, ka *MFEA* ir datu pārzinis;

15. jāsniedz fiziska informācija (brošūras/norādes utt.) VIS datu subjektiem lidostu un citu robežkontroles punktu telpās un jāpadara tā pamanāma un viegli pieejama;

16. jānodrošina, ka atbildēs datu subjektiem par VIS personas datiem tiktu sniegta informācija par iespēju šo atbildi pārsūdzēt DAI un kompetentajā tiesā;

17. jāveic nepieciešamie pasākumi, lai precizētu *MFEA* un Centrālās vīzu iestādes (Iekšlietu ministrija) pienākumus attiecībā uz VIS datu subjektu pieprasījumu izskatīšanu un sniegtu iekšējus vai metodiskus norādījumus abām struktūrām; šai informācijai vajadzētu būt pieejamai datu subjektiem;

Vīzu informācijas sistēma

18. jāveic vajadzīgie pasākumi, lai paaugstinātu drošības līmeni piekļuvei valdības videi un it īpaši valsts vīzu pieteikumiem *MFEA* un Iekšlietu ministrijā (Centrālajā vīzu iestādē), proti, nodrošinot piekļuvi valsts vīzu datubāzēm, izmantojot daudzfaktoru tehnoloģiju;

19. jāveic nepieciešamie pasākumi, lai uzlabotu fizisko un organizatorisko drošību *MFEA* N.VIS datu centrā, jo īpaši attiecībā uz šādiem aspektiem:

   – apmeklētāju žurnāla nodrošināšana pie ieejas datu centrā IKT darbiniekiem, apmeklētājiem vai piegādātājiem, kuriem piekļuve būtu jāierobežo;

   – ugunsdzēšanas sistēmas ar gāzi (aragonītu) uzstādīšana;

   – ūdens sūces noteikšanas sistēmas ierīkošana;

   – no putekļiem brīvas un sakārtotas grīdas nodrošināšana;

   – ES serveru aizsargžoga slēgšana;

20. jāpaātrina procedūra jauna N.VIS datu centra izveidei citā vietā un datu centra pārvietošanai;

21. jāapsver iespēja mainīt N.VIS žurnāldatņu vietējās uzglabāšanas periodu diplomātiskajās un konsulārajās pārstāvniecībās, paredzot laika periodu, nevis MB apjomu;

22. jāapsver iespēja *MFEA* izmantot automātiskas reģistra kontroles sistēmas;

23. jāveic vajadzīgie pasākumi, lai diplomātiskās pārstāvniecības vai *MFEA* regulāri pārbaudītu ārpakalpojumu sniedzējus;

24. jāveic vajadzīgie pasākumi, lai sistemātiskāk un vienoti nodrošinātu datu aizsardzības apmācību vietējiem konsulārajiem darbiniekiem;

25. jānodrošina, ka elektroniskais vīzas pieteikums pieprasa tādu pašu informāciju kā vīzas pieteikuma veidlapa papīra formātā (kā noteikts ES Vīzu kodeksa [1] I pielikumā);

Šengenas Informācijas sistēma II

26. jāveic vajadzīgie pasākumi, lai uzlabotu drošības līmeni piekļuvei *N.SIS II*, jo īpaši izmantojot daudzfaktoru autentifikāciju un tikai https-savienojumus piekļuvei *N.SIS II*;

27. jānodrošina, ka Iekšlietu ministrija informē DAI par visiem datu aizsardzības pārkāpumiem, kas varētu radīt risku fizisku personu tiesībām un brīvībām. Turklāt Iekšlietu ministrijai būtu jāizveido personas datu aizsardzības pārkāpumu reģistrs;

[1] Eiropas Parlamenta un Padomes Regula (EK) Nr. 810/2009 (2009. gada 13. jūlijs), ar ko izveido Kopienas Vīzu kodeksu (Vīzu kodekss); OV L 243/1, 15.9.2009.

Sabiedrības informētība

28. jāapsver iespēja DAI brošūras nodot datu subjektu rīcībā arī pieejamākās vietās, piemēram, policijas iecirkņos, robežkontroles zonās un konsulārajās telpās;

29. jāapsver iespēja darīt pieejamas DAI prezentācijas, seminārus un atvērto durvju pasākumus arī plašai sabiedrībai, jo īpaši datu subjektiem, jo uz tiem attiecas informācija par *SIS II* un VIS.

Briselē,

Padomes vārdā –
priekšsēdētājs