Europos Sąjungos
Taryba

Briuselis, 2021 m. sausio 25 d.
(OR. en)

5534/21

Tarpinstitucinė byla:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	14250/20
Dalykas:	Tarybos įgyvendinimo sprendimas, kuriame pateikiama rekomendacija dėl trūkumų, nustatytų 2019 m. vertinant, kaip **Slovakija** taiko Šengeno *acquis* nuostatas **duomenų apsaugos** srityje, šalinimo

Delegacijoms priede pateikiamas 2021 m. sausio 21 d. taikant rašytinę procedūrą priimtas Tarybos įgyvendinimo sprendimas, kuriame pateikiama rekomendacija dėl trūkumų, nustatytų 2019 m. vertinant, kaip Slovakija taiko Šengeno *acquis* nuostatas duomenų apsaugos srityje, šalinimo.

Pagal 2013 m. spalio 7 d. Tarybos reglamento (ES) Nr. 1053/2013 15 straipsnio 3 dalį ši rekomendacija bus perduota Europos Parlamentui ir nacionaliniams parlamentams.

Tarybos įgyvendinimo sprendimas, kuriame pateikiama

REKOMENDACIJA

dėl trūkumų, nustatytų 2019 m. vertinant, kaip Slovakija taiko Šengeno *acquis* nuostatas duomenų apsaugos srityje, šalinimo

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2013 m. spalio 7 d. Tarybos reglamentą (ES) Nr. 1053/2013, kuriuo sukuriamas tikrinimo, kaip taikoma Šengeno *acquis*, vertinimo ir stebėsenos mechanizmas ir panaikinamas 1998 m. rugsėjo 16 d. Vykdomojo komiteto sprendimas, įsteigiantis Šengeno įvertinimo ir įgyvendinimo nuolatinį komitetą[1], ypač į jo 15 straipsnį,

atsižvelgdama į Europos Komisijos pasiūlymą,

kadangi:

(1) šio sprendimo tikslas – rekomenduoti Slovakijos Respublikai imtis taisomųjų veiksmų trūkumams, nustatytiems 2019 m. atliekant Šengeno vertinimą duomenų apsaugos srityje, pašalinti. Atlikus vertinimą, Komisijos įgyvendinimo sprendimu C(2020) 8160 priimta ataskaita, kurioje pateiktos išvados bei įvertinimas ir nurodyta atliekant vertinimą nustatyta geriausia praktika ir trūkumai;

[1] OL L 295, 2013 11 6, p. 27.

(2) gerąja praktika, be kita ko, laikoma tai, kad nuo paskutinio Šengeno vertinimo 2012 m. duomenų apsaugos institucija (DAI) reguliariai pagal metinį planą vykdė SIS II priežiūros veiklą, ir tai, kad buvo parengta ateinančių ketverių metų SIS II patikrinimų koncepcija; kad DAI atliko daug VIS patikrinimų konsulatuose; kad DAI ir Vidaus reikalų ministerija (VRM) stengėsi teikti duomenų subjektams elektroninę ir spausdintą informaciją; kad DAI interneto svetainėje ir lankstinukuose informacija su Šengeno erdve susijusiomis temomis pateikiama įvairiomis kalbomis; kad DAI yra parengusi SIS ir VIS duomenų subjektų prašymų šablonus; kad SIRENE biuras teikia atsakymus į prašymus ne tik slovakų, bet ir anglų kalba; kad Slovakijos valdžios institucijos informuoja duomenų subjektus, jei SIS II nėra saugoma duomenų apie juos; kad VRM Inspekcijos tarnybos inspekcijos skyrius labai aktyviai tikrina VIS ir SIS II žurnalus; kad du Užsienio ir Europos reikalų ministerijos (UERM) Saugumo departamento darbuotojai labai aktyviai sprendžia su duomenų apsauga susijusius klausimus; kad UERM savo darbuotojams rengia mokymus duomenų apsaugos klausimais, visų pirma prieš juos laikinai komandiruodama konsulinėms užduotims atlikti, ir kad šiuos mokymus rengia Saugumo departamentas (kaip duomenų apsaugos pareigūno (DAP) tarnyba); kad SIS II duomenų apsaugos procedūrinė ir fizinė saugumo sistema yra aukšto lygio; kad VRM Inspekcijos biuro Inspekcijos skyriaus Duomenų apsaugos departamento DAP ir DAP pavaduotojas labai aktyviai atlieka savo vaidmenis, be kita ko, kiek tai susiję su gairių teikimu ir žurnalų tikrinimu SIS II srityje; kad VRM rengia duomenų apsaugos mokymus visiems N.SIS II galutiniams naudotojams;

(3) atsižvelgiant į tai, kad svarbu laikytis Šengeno *acquis* duomenų apsaugos srityje, kiek tai susiję su VIS, pirmiausia turėtų būti įgyvendintos 7 ir 24 rekomendacijos;

(4) šis sprendimas turėtų būti perduotas Europos Parlamentui ir valstybių narių parlamentams. Per tris mėnesius nuo jo priėmimo Slovakijos Respublika pagal Reglamento (ES) Nr. 1053/2013 16 straipsnio 1 dalį turėtų parengti veiksmų planą dėl visų rekomendacijų pašalinti vertinimo ataskaitoje nustatytus trūkumus ir pateikti jį Komisijai ir Tarybai,

REKOMENDUOJA:

Slovakijos Respublikai imtis toliau nurodytų veiksmų.

Duomenų apsaugos institucija

1. Užtikrinti, kad siekiant pagerinti DAI veiklos rezultatus ir veiksmingumą, DAI biudžetas ir darbuotojų skaičius turėtų būti toliau didinami.

2. Užtikrinti, kad DAI numatyta bendro valstybės biudžeto dalis būtų aiškiai matoma, siekiant užtikrinti, kad DAI turėtų atskirą viešąjį metinį biudžetą.

3. Užtikrinti, kad vykdant biudžeto procedūrą Nacionalinė taryba būtų informuota apie DAI poziciją dėl jos biudžeto poreikių ir DAI bei Finansų ministerijos diskusijas dėl biudžeto.

4. Imtis priemonių, kad Finansų ministerija negalėtų susieti biudžeto ir DAI surinktinų baudų sumos, nes tai galėtų turėti įtakos DAI darbo pobūdžiui ir prioritetų nustatymui, taigi ir jos nepriklausomumui. Turėtų būti užtikrinta, kad DAI biudžeto nebūtų galima sumažinti per kalendorinius metus tais atvejais, kai DAI surinko ne visas numatytas baudas.

5. Užtikrinti, kad DAI būtų suteiktos visos BDAR 57 ir 58 straipsniuose numatytos duomenų apsaugos institucijų užduotys ir galios.

6. Užtikrinti, kad, be įprastos N.SIS tarnyboje ir SIRENE biure vykdomos priežiūros veiklos, DAI taip pat prižiūrėtų daugiau institucijų, kurios yra galutinės SIS II naudotojos.

7. Užtikrinti, kad DAI, vykdydama VIS priežiūros veiklą, atliktų centrinės vizų institucijos patikrinimą, susijusį su N.VIS duomenų tvarkymo operacijomis. Kadangi pirmojo nacionalinės vizų sistemos audito terminas buvo 2015 m. spalio mėn., DAI turėtų kuo greičiau atlikti šią vis dar trūkstamą audito dalį.

8. Užtikrinti, kad DAI taip pat reguliariai tikrintų išorės paslaugų teikėjus.

Duomenų subjektų teisės

9. Turėtų būti rastas tinkamas būdas DAI, VRM ir UERM informuoti duomenų subjektus apie galimą riziką, kai jie teikia asmens tapatybės kortelių kopijas ir neskelbtiną informaciją atvirame internete. VRM ir UERM raginamos apsvarstyti galimybę duomenų subjektams pasiūlyti saugų elektroninį perdavimo kanalą tokiems dokumentams teikti.

10. Užtikrinti, kad būtų laikomasi 60 dienų atsakymo į SIS II duomenų subjektų prašymus termino, nustatyto SIS II reglamento 41 straipsnio 6 dalyje ir SIS II sprendimo 58 straipsnio 6 dalyje, kol bus visiškai pradėta taikyti nauja SIS *acquis*[1] (vėliausiai 2021 m. gruodžio 28 d.), kurioje pateikiamos kryžminės nuorodos į BDAR numatytą atsakymo į duomenų subjektų prašymus terminą (30 dienų su galimybe prireikus pratęsti dar dviem mėnesiais).

11. Apsvarstyti galimybę policijos nuovadų patalpose matomai ir lengvai prieinamai pateikti duomenų subjektams skirtos spausdintos informacijos (lankstinukų, plakatų ir pan.).

12. Apsvarstyti galimybę pateikti, pavyzdžiui, neoficialią DAI sprendimų dėl skundų dėl SIS II duomenų subjektų prašymų versiją anglų kalba. Tai padėtų duomenų subjektams geriau suprasti sprendimą ir sustiprintų duomenų subjektų teises.

13. Užtikrinti, kad UERM interneto svetainėje būtų lengviau rasti informaciją apie VIS duomenų subjektų teises. Svetainėje taip pat turėtų būti pateikti VIS duomenų subjektų naudojimosi savo teisėmis šablonai.

---

[1] 2018 m. lapkričio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1862 dėl Šengeno informacinės sistemos (SIS) sukūrimo, eksploatavimo ir naudojimo policijos bendradarbiavimui ir teisminiam bendradarbiavimui baudžiamosiose bylose, kuriuo iš dalies keičiamas ir panaikinamas Tarybos sprendimas 2007/533/TVR ir panaikinamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1986/2006 ir Komisijos sprendimas 2010/261/ES, OL L 312, 2018 12 7, p. 56 (ypač 66–71 straipsniai). 2018 m. lapkričio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1861 dėl Šengeno informacinės sistemos (SIS) sukūrimo, eksploatavimo ir naudojimo patikrinimams kertant sieną, kuriuo iš dalies keičiama Konvencija dėl Šengeno susitarimo įgyvendinimo ir iš dalies keičiamas bei panaikinamas Reglamentas (EB) Nr. 1987/2006, OL L 312, 2018 12 7, p. 14 (ypač 51–57 straipsniai).

14. Užtikrinti, kad prašymo išduoti vizą formoje būtų pateikta aiški informacija apie įvairias institucijas, kurios tvarko asmens duomenis nacionalinėje vizų sistemoje. Visų pirma turėtų būti nurodyta, kad UERM yra duomenų valdytojas.

15. Oro uostų ir kitų sienų kontrolės punktų patalpose matomai ir lengvai prieinamai pateikti VIS duomenų subjektams skirtą fizinę informaciją (lankstinukus, plakatus ir pan.).

16. Užtikrinti, kad atsakymuose duomenų subjektams dėl VIS laikomų asmens duomenų būtų pateikiama informacija apie galimybę dėl atsakymo pateikti skundą DAI ir kompetentingam teismui.

17. Imtis būtinų priemonių paaiškinti UERM ir centrinės vizų institucijos (VRM) atsakomybę už VIS duomenų subjektų prašymų tvarkymą ir parengti vidaus arba metodines gaires abiem subjektams. Ši informacija turėtų būti prieinama duomenų subjektams.

Vizų informacinė sistema

18. Imtis būtinų priemonių, kad būtų padidintas prieigos prie vyriausybinės aplinkos, ypač prie nacionalinių prašymų išduoti vizą UERM ir VRM (centrinėje vizų institucijoje), saugumo lygis, visų pirma užtikrinti, kad prie nacionalinių vizų duomenų bazių būtų jungiamasi naudojant daugiaveiksnio tapatumo nustatymo technologiją.

19. Imtis būtinų priemonių UERM N.VIS duomenų centro fiziniam ir organizaciniam saugumui padidinti, visų pirma šiais aspektais:

    – užtikrinti, kad prie duomenų centro įėjimo būtų lankytojų registracijos žurnalas, skirtas ribotą prieigą turintiems IRT darbuotojams, lankytojams arba tiekėjams;

    – įrengti gaisro gesinimo dujomis (argonitu) sistemą;

    – įrengti vandens nuotėkio aptikimo įrangą;

    – užtikrinti, kad grindys būtų nedulkėtos ir tvarkingos;

    – užrakinti ES serverių apsauginę užtvarą.

20. Sparčiau vykdyti naujo N.VIS duomenų centro kitoje vietoje įrengimo ir duomenų centro perkėlimo procesą.

21. Apsvarstyti galimybę pakeisti N.VIS žurnalo failų vietos saugojimo diplomatinėse ir konsulinėse atstovybėse laikotarpį – nustatyti laikotarpį, o ne MB dydį.

22. Apsvarstyti galimybę UERM naudoti automatines žurnalų kontrolės sistemas.

23. Imtis būtinų priemonių, kad diplomatinės atstovybės arba UERM reguliariai tikrintų išorės paslaugų teikėjus.

24. Imtis būtinų priemonių, kad vietos konsuliniam personalui būtų sistemingiau ir vienodžiau rengiami mokymai duomenų apsaugos klausimais.

25. Užtikrinti, kad elektroniniame prašyme išduoti vizą būtų prašoma tos pačios informacijos kaip ir popierinėje prašymo išduoti vizą formoje (kaip nustatyta ES vizų kodekso I priede[1]).

Antrosios kartos Šengeno informacinė sistema

26. Imtis būtinų priemonių prieigos prie N.SIS II saugumo lygiui pagerinti, visų pirma prieigai prie N.SIS II naudojant daugiaveiksnio tapatumo nustatymo metodą ir tik *https* ryšį.

27. Užtikrinti, kad VRM informuotų DAI apie bet kokį duomenų saugumo pažeidimą, dėl kurio gali kilti pavojus fizinių asmenų teisėms ir laisvėms. Be to, VRM turėtų sukurti asmens duomenų saugumo pažeidimų registrą.

[1] 2009 m. liepos 13 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 810/2009, nustatantis Bendrijos vizų kodeksą (Vizų kodeksas), OL L 243, 2009 9 15, p. 1.

Visuomenės informavimas

28. Apsvarstyti galimybę duomenų subjektams pateikti DAI lankstinukus, be kita ko, prieinamesnėse vietose, pavyzdžiui, policijos nuovadose, pasienio kontrolės zonose ir konsulinėse patalpose.

29. Apsvarstyti galimybę DAI pristatymus, seminarus ir atvirų durų renginius padaryti prieinamus ir plačiajai visuomenei, ypač duomenų subjektams, nes informacija SIS II ir VIS yra su jais susijusi.

Priimta Briuselyje

Tarybos vardu
Pirmininkas