Vijeće
Europske unije

Bruxelles, 24. rujna 2019.
(OR. en)

12469/19

Međuinstitucijski predmet:
2019/0169(NLE)

SCH-EVAL 158
DATAPROTECT 217
COMIX 428

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	20. rujna 2019.
Za:	Delegacije
Br. preth. dok.:	11906/1/19 REV 1
Predmet:	Provedbena odluka Vijeća o utvrđivanju preporuke o uklanjanju nedostataka utvrđenih u evaluaciji iz 2018. o primjeni schengenske pravne stečevine u području **zaštite podataka** u **Latviji**

Za delegacije se u Prilogu nalazi Provedbena odluka Vijeća o utvrđivanju preporuke o uklanjanju nedostataka utvrđenih u evaluaciji iz 2018. o primjeni schengenske pravne stečevine u području zaštite podataka u Latviji, koju je Vijeće donijelo na sastanku održanome 20. rujna 2019.

U skladu s člankom 15. stavkom 3. Uredbe Vijeća (EU) br. 1053/2013 od 7. listopada 2013. ta preporuka proslijedit će se Europskom parlamentu i nacionalnim parlamentima.

Provedbena odluka Vijeća o utvrđivanju

PREPORUKE

o uklanjanju nedostataka utvrđenih u evaluaciji iz 2018. o primjeni schengenske pravne stečevine u području zaštite podataka u Latviji

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu Vijeća (EU) br. 1053/2013 od 7. listopada 2013. o uspostavi mehanizma evaluacije i praćenja za provjeru primjene schengenske pravne stečevine i stavljanju izvan snage Odluke Izvršnog odbora od 16. rujna 1998. o uspostavi Stalnog odbora za ocjenu i provedbu Schengena[1], a posebno njezin članak 15.,

uzimajući u obzir prijedlog Europske komisije,

budući da:

(1) Svrha je ove Odluke preporučiti Latviji korektivne mjere za uklanjanje nedostataka utvrđenih tijekom schengenske evaluacije provedene 2018. u području zaštite podataka. Nakon evaluacije Provedbenom odlukom Komisije C(2019)5720 doneseno je izvješće o nalazima i procjenama u kojemu se navode najbolje prakse i nedostaci utvrđeni tijekom evaluacije.

(2) Dobrom praksom smatraju se, među ostalim, uspješna prijava za financiranje Europske komisije za potrebe podizanja svijesti javnosti, dostupnost odgovora Ureda SIRENE na raznim jezicima te odgovaranje u kratkom roku.

[1] SL L 295, 6.11.2013., str. 27.

(3) S obzirom na važnost usklađivanja sa schengenskom pravnom stečevinom o zaštiti podataka u vezi s drugom generacijom Schengenskog informacijskog sustava (SIS II), prednost bi trebalo dati preporukama od 15. do 18.

(4) S obzirom na važnost usklađivanja sa schengenskom pravnom stečevinom o zaštiti podataka u vezi s viznim informacijskim sustavom (VIS), prednost bi trebalo dati preporukama 9. i 11.

(5) Ovu bi Odluku trebalo proslijediti Europskom parlamentu i parlamentima država članica. U skladu s člankom 16. stavkom 1. Uredbe (EU) br. 1053/2013 Latvija bi trebala izraditi akcijski plan koji uključuje sve preporuke za uklanjanje nedostataka utvrđenih u izvješću o evaluaciji te ga podnijeti Komisiji i Vijeću u roku od tri mjeseca od donošenja ove Odluke,

PREPORUČUJE:

da bi Latvija trebala:

Nadzorno tijelo za zaštitu podataka

1. osigurati potpunu neovisnost tijela za zaštitu podataka donošenjem nacionalnog zakonodavstva usklađenog s poglavljem VI. Opće uredbe o zaštiti podataka, osobito u pogledu postupka za razrješenje direktora;

2. osigurati dostatna sredstva za tijelo za zaštitu podataka te dovoljan broj zaposlenika kako bi moglo izvršavati sve zadaće koje su mu povjerene u skladu s drugom generacijom Schengenskog informacijskog sustava (dalje u tekstu: „SIS II”) i viznim informacijskim sustavom (dalje u tekstu „VIS”);

3. osigurati pravodobno provođenje revizije nad postupcima obrade podataka u N.SIS-u kako je propisano člankom 44. stavkom 2. Uredbe o SIS-u II i člankom 60. stavkom 2. Odluke Vijeća o SIS-u II;

4. osigurati da se revizija aktivnosti obrade podataka u N-VIS-u provodi kako je propisano člankom 41. stavkom 2. Uredbe o VIS-u i člankom 8. stavkom 6. Odluke Vijeća o VIS-u;

5. osigurati da buduće revizije SIS-a II i VIS-a budu sveobuhvatne te da se provode u skladu s međunarodnim standardima revizije, kako je predviđeno pravnom stečevinom koja se odnosi na SIS II i VIS, te osigurati upotrebu potrebnih informatičkih znanja u okviru tih revizija;

6. osigurati da nadzorne aktivnosti tijela za zaštitu podataka u vezi sa SIS-om II uključuju redovite kontrole upozorenja u sustavu SIS II;

7. osigurati da nadzorne aktivnosti tijela za zaštitu podataka u vezi s VIS-om uključuju redovite inspekcije konzularnih ureda;

8. osigurati da višegodišnji plan inspekcija tijela za zaštitu podataka uz obvezne revizije sustava SIS II i VIS uključuje i druge inspekcijske aktivnosti;

Vizni informacijski sustav

9. osigurati redovito analiziranje evidencija za potrebe nadzora zakonitosti aktivnosti obrade podataka u skladu s člankom 34. stavcima 1. i 2. Uredbe o VIS-u;

10. razjasniti ulogu Ministarstva vanjskih poslova (izvršitelj obrade ili zajednički voditelj obrade) u odnosu na Ured za pitanja državljanstva i migracija;

11. osigurati da Ured za pitanja državljanstva i migracija provodi češću samoreviziju aktivnosti obrade u sustavu VIS;

12. preispitati ugovore s vanjskim pružateljima usluga kako bi se uskladili sa zahtjevima iz Opće uredbe o zaštiti podataka;

13. jasno definirati zadaće i ovlasti službenika za zaštitu podataka iz Ureda za pitanja državljanstva i migracija i iz Ministarstva vanjskih poslova;

14. osigurati da internetski obrasci koji se upotrebljavaju u kontekstu zahtjeva za vizu uključuju obavijest o zaštiti podataka kojom se ispitanici informiraju o aktivnostima obrade podataka i primjenjivim individualnim pravima,

Schengenski informacijski sustav

15. osigurati da policija redovito provodi samoreviziju, posebice samopraćenje evidencija;

16. uspostaviti nacionalne evidencije sustava SIS II na središnjoj razini i osigurati da se iz evidencije može utvrditi razlog za upit;

17. osigurati redovitu reviziju evidencija kako bi se provjerila zakonitost obrade podataka u skladu s člankom 12. stavkom 2. Uredbe o SIS-u II i Odluke Vijeća o SIS-u II;

18. na najmanju moguću razinu svesti sigurnosni rizik koji predstavlja mobilna aplikacija kojom se omogućuje pristup sustavu SIS II, primjerice omogućujući pristup samo putem usluge VPN-a;

19. uspostaviti dvofaktorski autentifikacijski sustav;

20. osigurati da se produkcijski podaci ne upotrebljavaju za testiranje te da samo ovlašteni korisnici mogu pretraživati N.SIS;

21. jasno definirati zadaće i ovlasti službenika za zaštitu podataka iz policije, među ostalim u pogledu njegova sudjelovanja u aktivnostima internog nadzora, npr. nadzora učinkovitosti sigurnosnih mjera;

Prava ispitanika i podizanje svijesti

22. redovito dostavljati tijelu za zaštitu podataka statističke podatke o ostvarivanju prava ispitanika u vezi sa sustavima SIS II i VIS;

23. povećati dostupnost informativnih materijala, kao što je brošura „Personal Data in the Schengen Information System” (Osobni podaci u Schengenskom informacijskom sustavu) u zračnoj luci te na drugim javnim mjestima.

Sastavljeno u Bruxellesu

Za Vijeće
Predsjednik