Svet
Evropske unije

Bruselj, 24. september 2019
(OR. en)

12469/19

Medinstitucionalna zadeva:
2019/0169(NLE)

SCH-EVAL 158
DATAPROTECT 217
COMIX 428

IZID POSVETOVANJA

Pošiljatelj:	generalni sekretariat Sveta
Datum:	20. september 2019
Prejemnik:	delegacije
Št. predh. dok.:	11906/1/19 REV 1
Zadeva:	Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih med ocenjevanjem **Latvije,** opravljenem leta 2018, glede uporabe schengenskega pravnega reda na področju **varstva podatkov**

V prilogi vam pošiljamo Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih med ocenjevanjem Latvije, opravljenem leta 2018, glede uporabe schengenskega pravnega reda na področju varstva podatkov, ki ga je Svet sprejel na seji 20. septembra 2019.

V skladu s členom 15(3) Uredbe Sveta (EU) št. 1053/2013 z dne 7. oktobra 2013 bo to priporočilo poslano Evropskemu parlamentu in nacionalnim parlamentom.

Izvedbeni sklep Sveta o

PRIPOROČILU

za odpravo pomanjkljivosti, ugotovljenih leta 2018 med ocenjevanjem uporabe schengenskega pravnega reda na področju varstva podatkov v Latviji

SVET EVROPSKE UNIJE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe Sveta (EU) št. 1053/2013 z dne 7. oktobra 2013 o vzpostavitvi ocenjevalnega in spremljevalnega mehanizma za preverjanje uporabe schengenskega pravnega reda in razveljavitvi Sklepa Izvršnega odbora z dne 16. septembra 1998 o ustanovitvi stalnega odbora o ocenjevanju in izvajanju Schengenskega sporazuma[1] ter zlasti člena 15 Uredbe,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Namen tega sklepa je Latviji priporočiti ukrepe za odpravo pomanjkljivosti, ugotovljenih leta 2018 med schengenskim ocenjevanjem na področju varstva podatkov. Po ocenjevanju je bilo z Izvedbenim sklepom Komisije C(2019) 5720 sprejeto poročilo z ugotovitvami in ocenami, v katerem so navedene dobre prakse in pomanjkljivosti, ugotovljene med ocenjevanjem.

(2) Za dobro prakso štejeta med drugim uspešna uporaba sredstev Evropske komisije za boljšo ozaveščenost javnosti ter dejstvo, da so odgovori urada SIRENE na voljo v različnih jezikih in večinoma podani v kratkem času.

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

(3) Glede na pomen spoštovanja schengenskega pravnega reda na področju varstva podatkov v zvezi s schengenskim informacijskim sistemom II (SIS II) bi bilo treba prednost dati izvajanju priporočil 15 do 18.

(4) Glede na pomen spoštovanja schengenskega pravnega reda na področju varstva podatkov v zvezi z vizumskim informacijskim sistemom (VIS) bi bilo treba prednost dati izvajanju priporočil 9 in 11.

(5) Ta sklep bi bilo treba poslati Evropskemu parlamentu in parlamentom držav članic. Latvija bi morala v skladu s členom 16(1) Uredbe (EU) št. 1053/2013 v treh mesecih od sprejetja sklepa pripraviti akcijski načrt, ki obravnava vsa priporočila za odpravo pomanjkljivosti, ugotovljenih v ocenjevalnem poročilu, ter ga predložiti Komisiji in Svetu –

PRIPOROČA:

da bi Latvija morala:

Nadzorni organ za varstvo podatkov

1. zagotoviti popolno neodvisnost organa za varstvo podatkov s sprejetjem nacionalne zakonodaje, ki je v skladu s poglavjem VI Splošne uredbe o varstvu podatkov, zlasti glede postopka za razrešitev direktorja;

2. zagotoviti, da je organ za varstvo podatkov zadostno financiran in ima ustrezno raven zaposlenih, da bo lahko izpolnil vse naloge, ki so mu zaupane v skladu s pravnim redom v zvezi s schengenskim informacijskim sistemom II (v nadaljnjem besedilu: SIS II) in vizumskim informacijskim sistemom (v nadaljnjem besedilu: VIS);

3. zagotoviti pravočasno opravljanje revizije postopkov obdelave podatkov v sistemu N.SIS, kakor je določeno s členom 44(2) Uredbe SIS II in členom 60(2) sklepa Sveta SIS II;

4. zagotoviti, da se revizija postopkov obdelave podatkov v sistemu NVIS opravlja v skladu s členom 41(2) Uredbe VIS in členom 8(6) sklepa Sveta VIS;

5. zagotoviti, da bodo prihodnje revizije sistemov SIS II in VIS povsem celovite in da se bodo opravljale v skladu z mednarodnimi revizijskimi standardi, kot jih zahteva pravni red v zvezi s sistemoma SIS II in VIS, ter zagotoviti, da se za te revizije uporablja potrebno strokovno znanje na področju IT;

6. zagotoviti, da nadzorne dejavnosti organa za varstvo podatkov v zvezi s SIS II vključujejo redne kontrole razpisov ukrepov v SIS II;

7. zagotoviti, da nadzorne dejavnosti organa za varstvo podatkov v zvezi z VIS vključujejo redne preglede konzulatov;

8. zagotoviti, da večletni načrt za preglede, ki jih izvaja organ za varstvo podatkov, poleg obveznih revizij SIS II in VIS vključuje tudi druge dejavnosti pregledovanja;

Vizumski informacijski sistem

9. zagotoviti, da se bodo dnevniške datoteke redno analizirale zaradi spremljanja zakonitosti dejavnosti obdelave podatkov v skladu s členom 34(1) in (2) Uredbe VIS;

10. pojasniti vlogo (obdelovalca podatkov ali skupnega upravljavca) ministrstva za zunanje zadeve – v zvezi z uradom za državljanstvo in migracije;

11. zagotoviti, da bo urad za državljanstvo in migracije pogosteje opravljal notranjo revizijo dejavnosti obdelave v sistemu VIS;

12. prenoviti pogodbe z zunanjimi ponudniki storitev zaradi upoštevanja in uskladitve z zahtevami iz splošne uredbe o varstvu podatkov;

13. jasno opredeliti naloge in pooblastila uradnikov za varstvo podatkov urada za državljanstvo in migracije ter ministrstva za zunanje zadeve;

14. zagotoviti, da spletni obrazci, ki se uporabljajo v zvezi z vlogo za izdajo vizuma, vsebujejo obvestilo o varstvu podatkov, ki posameznike, na katere se nanašajo osebni podatki, seznanja z dejavnostmi obdelave podatkov in ustreznimi pravicami posameznikov;

Schengenski informacijski sistem

15. zagotoviti, da policija redno izvaja notranje revizije, zlasti notranji nadzor dnevniških datotek;

16. pripravljati nacionalne dnevniške datoteke za SIS II na centralni ravni in zagotoviti, da je utemeljitev za poizvedbo razvidna iz dnevniške datoteke;

17. zagotoviti, da se bodo dnevniške datoteke redno pregledovale zaradi preverjanja zakonitosti obdelave podatkov v skladu s členom 12(2) Uredbe SIS II in sklepom Sveta SIS II;

18. čim bolj zmanjšati varnostno tveganje, ki ga predstavlja mobilna aplikacija, ki omogoča dostop do SIS II, na primer z omogočanjem dostopa samo prek storitve VPN;

19. vzpostaviti sistem dvofaktorske avtentikacije;

20. zagotoviti, da se produkcijski podatki ne uporabljajo za preskuse in da lahko po NSIS iščejo le ustrezno pooblaščeni uporabniki;

21. jasno opredeliti naloge in pooblastila pooblaščene osebe za varstvo podatkov na policiji, vključno z njeno udeležbo pri dejavnostih notranjega spremljanja, kot je spremljanje učinkovitosti varnostnih ukrepov;

Pravice posameznikov, na katere se nanašajo podatki, in ozaveščanje

22. organu za varstvo podatkov redno posredovati statistične podatke o uveljavljanju pravic posameznikov, na katere se nanašajo osebni podatki, v zvezi s SIS II in VIS;

23. izboljšati dostopnost informativnega gradiva, kot je brošura „Osebni podatki v schengenskem informacijskem sistemu“, na letališčih in na drugih javnih mestih.

V Bruslju,

Za Svet
Predsednik