Svet
Evropske unije

Bruselj, 14. maj 2018
(OR. en)

8792/18

Medinstitucionalna zadeva:
2018/0051 (NLE)

SCH-EVAL 102
COMIX 244

IZID POSVETOVANJA

Pošiljatelj:	generalni sekretariat Sveta
Datum:	14. maj 2018
Prejemnik:	delegacije
Št. predh. dok.:	8285/18
Zadeva:	Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih med ocenjevanjem **Portugalske**, opravljenim leta 2017, glede uporabe schengenskega pravnega reda na področju **varstva podatkov**

V prilogi vam pošiljamo Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih med ocenjevanjem Portugalske, opravljenim leta 2017, glede uporabe schengenskega pravnega reda na področju varstva podatkov, ki ga je Svet sprejel na seji 14. maja 2018.

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.

PRILOGA

Izvedbeni sklep Sveta o

PRIPOROČILU

za odpravo pomanjkljivosti, ugotovljenih med ocenjevanjem Portugalske, opravljenim leta 2017, glede uporabe schengenskega pravnega reda na področju varstva podatkov

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 Portugalski priporočiti ukrepe za odpravo pomanjkljivosti, ugotovljenih leta 2017 med schengenskim ocenjevanjem na področju varstva podatkov. Po ocenjevanju je bilo z Izvedbenim sklepom Komisije [C(2018) 1190] sprejeto poročilo, ki vključuje ugotovitve in ocene ter navaja dobre prakse in pomanjkljivosti, ugotovljene med ocenjevanjem.

(2) Kot dobra praksa se odraža, da je skupina za obiske na kraju samem pozitivno sprejela stalno vlaganje organa za varstvo podatkov v usposabljanje svojega tehničnega osebja.

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

(3) Glede na pomen spoštovanja schengenskega pravnega reda, zlasti zahteve, da se zagotovi in izvaja učinkovit nadzor in da se zagotovijo potrebni varnostni ukrepi, bi bilo treba prednost nameniti izvajanju priporočil 1, 4, 14, 17 in 22.

(4) Ta sklep bi bilo treba poslati Evropskemu parlamentu in parlamentom držav članic. V skladu s členom 16(1) Uredbe (EU) št. 1053/2013 Portugalska v treh mesecih od sprejetja priporočila pripravi akcijski načrt za odpravo pomanjkljivosti, ugotovljenih v ocenjevalnem poročilu, ter ga predloži Komisiji in Svetu –

PRIPOROČA,

da bi morala Portugalska:

Nadzorni organ za varstvo podatkov

1. organu za varstvo podatkov (v nadaljnjem besedilu: DPA) dodeliti zadostne finančne in človeške vire, da lahko izpolni vse svoje naloge v okviru pravnega reda schengenskega informacijskega sistema II (v nadaljnjem besedilu: sistem SIS II) in vizumskega informacijskega sistema (v nadaljnjem besedilu: sistem VIS), tudi zaradi večje odgovornosti v prihodnosti;

2. za boljšo zagotovitev popolne neodvisnosti DPA omogočiti njegovo finančno samostojnost, s čimer lahko izvaja svoj letni proračun in samostojnost pri zaposlovanju osebja, pri minimalnem uravnavanju zadevnih pravil s tistimi, ki veljajo za druge samostojne organe na Portugalskem;

3. zagotoviti, da DPA nemudoma zaključi postopek glede sprejetja poročil po pregledu v zvezi z obdelavo osebnih podatkov v sistemu SIS II;

4. zagotoviti, da DPA nemudoma izvede revizijo sistema VIS;

Pravice posameznikov, na katere se nanašajo podatki

5. Pravice posameznikov, na katere se nanašajo osebni podatki zagotoviti, da so posamezniki, na katere se nanašajo osebni podatki, o svojih pravicah glede sistema SIS II obveščeni na spletnem mestu urada Serviço de Estrangeiros e Fronteiras (Urad za meje in priseljevanje, v nadaljnjem besedilu: SEF);

6. zagotoviti, da so posamezniki, na katere se nanašajo osebni podatki, po zahtevi za dostop do osebnih podatkov obveščeni o kategorijah podatkov, ki so dejansko obdelani v sistemu SIS II;

7. zagotoviti, da so posameznikom, na katere se nanašajo osebni podatki, zagotovljene jasne informacije glede identitete upravljavca podatkov, ki je odgovoren za obdelavo osebnih podatkov znotraj izdajanja schengenskih vizumov;

Vizumski informacijski sistem

8. pojasniti situacijo glede upravljanja obdelave osebnih podatkov v sistemu N.VIS (z zajemom aplikacij, ki se uporabljajo v Ministrstvu za zunanje zadeve (v nadaljnjem besedilu: MZZ) in SEF ter z njima povezanimi podatkovnimi centri), posebej s pojasnjevanjem vloge MZZ in pojasnjevanjem razporeditve odgovornosti, povezane z obdelavo osebnih podatkov med SEF in MZZ;

9. zagotoviti, da MZZ izvaja sistematične nadzorne dejavnosti, ki omogočajo smiselno oceno vidikov, v zvezi z obdelavo osebnih podatkov s strani zunanjega ponudnika storitev. V tem smislu je Portugalska spodbujena, da razširi vprašalnik, ki ga MZZ pošlje zunanjemu ponudniku storitev, z namenom bolje zajeti vidike varstva podatkov in izboljšati nadzorne dejavnosti MZZ, povezane z varstvom podatkov, ki jih izvaja zunanji ponudnik storitev ali podizvajalec, če je to potrebno;

10. zagotoviti postopek, ki omogoča preverjanje zadetkov sistema SIS II v okviru postopka izdaje vizuma;

11. zagotoviti, da so vsa uporabniška gesla sistema N.VIS šifrirana;

12. zagotoviti, da SEF in MZZ redno analizirata dnevniške datoteke, z namenom zagotoviti nadzorovanje varstva podatkov;

13. zagotoviti, da MZZ redno izvaja samonadzor obdelave osebnih podatkov v sistemu RPV in povezanih podatkovnih centrih;

14. zagotoviti, da MZZ nemudoma sprejme varnostni načrt za sistem RPV in povezane podatkovne centre;

15. v celoti izvajati Sklep Sveta 2008/633/PNZ z dne 23. junija 2008 o dostopu imenovanih organov držav članic in Europola do vizumskega informacijskega sistema (VIS) za iskanje podatkov za namene preprečevanja, odkrivanja in preiskovanja terorističnih dejanj in drugih hudih kaznivih dejanj ter zagotavljati, da dostop do podatkov N.VIS ustreza zahtevam in postopkom, določenim v njem;

16. zagotoviti, da zunanji ponudnik storitev izbriše osebne podatke vlagateljev, ki jih hrani v svojih sistemih, v skladu z roki Priloge X, dela A, točke (d) vizumskega zakonika, ki zahteva, da se takšni podatki izbrišejo nemudoma po njihovem prenosu konzulatu;

Schengenski informacijski sistem druge generacije

17. poskrbeti za celovit podporni center za sistem N.SIS II, ki zagotavlja popolno funkcionalnost, vključno s povezavo s komunikacijsko infrastrukturo s-Testa;

18. pojasniti odgovornosti med stranmi, ki so vključene v obdelavo podatkov sistema N.SIS II, kamor spadajo upravljavec podatkov in organi, ki dostopajo do sistema SIS.II (uporabniški organi), v smislu informacijske varnosti, nadzora in samonadzora, na primer s sklenitvijo sporazuma med upravljavcem podatkov in organi, ki dostopajo do sistema SIS II;

19. izvajati uporabniško upravljanje, ki omogoča učinkovit samonadzor na podlagi centralnih dnevnikov s strani upravljavca podatkov sistema N.SIS II, brez potrebe po posvetovanju z dnevniki pri uporabniških organih;

20. zagotoviti, da SEF redno analizira dnevniške datoteke, da zagotovi nadzorovanje varstva podatkov;

21. zagotoviti, da so informacijska okolja, ki jih uporabljajo uporabniki z daljnosežnim dostopom ali uredniškimi pravicami za sistem N.SIS II (kot so člani urada SIRENE), logično ali fizično ločena od internetnega dostopa;

22. zagotoviti, da upravljavec podatkov šifrira varnostne kopije na traku in trde diske sistema N.SIS;

23. zagotoviti, da so uporabniški profili z daljnosežnim dostopom ali pravicami urejanja podatkov N.SIS II (kot so člani urada SIRENE) zaščiteni z obvezno metodo dvostopenjske avtentikacije;

24. zagotoviti, da SEF okrepi svoje dejavnosti, povezane s samonadzorom obdelave osebnih podatkov sistema N.SIS, in ta samonadzor redno izvaja. Portugalska naj uradu SEF dodeli zadostne finančne in človeške vire, da zagotovi učinkovito in stalno samorevidiranje in informacijsko varnost, zlasti z zagotavljanjem, da je objava o informacijski varnosti za zaposlene v poslovni enoti SEF za informacijske tehnologije izpolnjena;

Ozaveščenost javnosti

25. zagotoviti, da spletno mesto SEF nudi ustrezne povezave na spletno mesto DPA.

V Bruslju,

Za Svet
Predsednik