Svet
Evropske unije

Bruselj, 25. januar 2021
(OR. en)

5534/21

Medinstitucionalna zadeva:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

IZID POSVETOVANJA

Pošiljatelj:	generalni sekretariat Sveta
Prejemnik:	delegacije
Št. predh. dok.:	14250/20
Zadeva:	Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih leta 2019 med ocenjevanjem uporabe schengenskega pravnega reda pri **varstvu podatkov** na **Slovaškem**

V prilogi vam pošiljamo Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih leta 2019 med ocenjevanjem uporabe schengenskega pravnega reda pri varstvu podatkov na Slovaškem, ki je bil sprejet 21. januarja 2021 po pisnem postopku.

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 2019 med ocenjevanjem uporabe schengenskega pravnega reda pri varstvu podatkov na Slovaškem

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 Slovaški priporočiti ukrepe za odpravo pomanjkljivosti, ugotovljenih v letu 2019 med ocenjevanjem uporabe schengenskega pravnega reda na področju varstva podatkov. Po ocenjevanju je bilo z Izvedbenim sklepom Komisije C(2020) 8160 sprejeto poročilo, ki vključuje ugotovitve in ocene ter navaja dobre prakse in pomanjkljivosti, ugotovljene med ocenjevanjem. Med dobre prakse se na primer šteje naslednje:

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

(2) da je organ za varstvo podatkov od zadnjega ocenjevanja uporabe schengenskega pravnega reda leta 2012 redno izvajal nadzorne dejavnosti SIS II v skladu z letnim načrtovanjem in da je bila oblikovana zasnova za preglede SIS II za naslednja štiri leta; da je organ za varstvo podatkov izvedel veliko število pregledov VIS na konzulatih; prizadevanja organa za varstvo podatkov in ministrstva za notranje zadeve za zagotavljanje informacij posameznikom, na katere se nanašajo osebni podatki, v elektronski in tiskani obliki; večjezikovne različice informacij o temah, povezanih s schengenskim pravnim redom, na spletišču organa za varstvo podatkov in v zloženkah; da je organ za varstvo podatkov pripravil predloge za zahtevke za posameznike, na katere se nanašajo osebni podatki v SIS in VIS; da urad SIRENE odgovorov na zahtevke ne pošilja le v slovaškem jeziku, temveč tudi v angleščini; da slovaški organi posameznike, na katere se nanašajo osebni podatki, obvestijo, če v SIS II niso shranjeni podatki o njih; zelo dejaven nadzor evidenc VIS in SIS II s strani oddelka za preglede službe za preglede ministrstva za notranje zadeve; zelo dejavna vloga dveh uslužbencev na oddelku za varnost ministrstva za zunanje in evropske zadeve, ki se ukvarja z vprašanji varstva podatkov; da ministrstvo za zunanje in evropske zadeve svojemu osebju zagotavlja usposabljanje o varstvu podatkov, zlasti pred začasno napotitvijo na opravljanje konzularnih nalog, in da to usposabljanje zagotavlja oddelek za varnost (v vlogi urada pooblaščene osebe za varstvo podatkov); da sta varnost postopkov in fizična varnost, vzpostavljeni za varstvo podatkov iz SIS II, na visoki ravni; zelo dejavna vloga pooblaščene osebe za varstvo podatkov v enoti za varstvo podatkov oddelka za preglede službe za preglede ministrstva za notranje zadeve pri upravljanju in nadzoru evidenc v zvezi s SIS II; da ministrstvo za notranje zadeve zagotavlja usposabljanje o varstvu podatkov vsem končnim uporabnikom N.SIS II.

(3) Glede na pomen spoštovanja schengenskega pravnega reda o varstvu podatkov v zvezi z VIS bi bilo treba prednost nameniti izvajanju priporočil 7 in 24.

(4) Ta sklep bi bilo treba poslati Evropskemu parlamentu in parlamentom držav članic. Slovaška 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:

Slovaška bi morala:

Organ za varstvo podatkov

1. zagotoviti, da bo za večjo uspešnost in učinkovitost organa za varstvo podatkov nadalje okrepila proračun in osebje organa za varstvo podatkov;

2. zagotoviti, da bo del celotnega državnega proračuna, ki je predviden za organ za varstvo podatkov, jasno prikazan, s čimer se bo zagotovil ločen javni letni proračun za organ za varstvo podatkov;

3. zagotoviti, da bo državni svet v proračunskem postopku seznanjen s stališčem organa za varstvo podatkov glede njegovih proračunskih potreb ter razpravami med organom za varstvo podatkov in ministrstvom za finance glede proračuna;

4. sprejeti ukrepe, da ministrstvo za finance ne bo moglo vzpostavljati korelacije med proračunom in številom denarnih kazni, ki jih pobira organ za varstvo podatkov, saj bi to lahko vplivalo na naravo in prednostno razvrščanje dela organa za varstvo podatkov ter s tem na njegovo neodvisnost. Zagotoviti bi bilo treba, da proračuna organa za varstvo podatkov med koledarskim letom ni mogoče zmanjšati, kadar organ za varstvo podatkov ne pobere v celoti ocenjenih denarnih kazni;

5. zagotoviti, da bodo organu za varstvo podatkov dodeljene vse naloge in pooblastila za organe za varstvo podatkov iz členov 57 in 58 splošne uredbe o varstvu podatkov;

6. zagotoviti, da bo poleg običajnih nadzornih dejavnosti, ki se izvajajo na uradih N.SIS in SIRENE, organ za varstvo podatkov nadzoroval več organov za končne uporabnike, ki imajo dostop do SIS II;

7. zagotoviti, da bodo nadzorne dejavnosti organa za varstvo podatkov v zvezi z VIS vključevale inšpekcijski pregled osrednjega organa, pristojnega za izdajo vizumov, pri postopkih obdelave osebnih podatkov v N.VIS. Rok za prvo revizijo nacionalnega vizumskega sistema je bil oktobra 2015 in organ za varstvo podatkov bi moral čim prej izvesti ta še vedno manjkajoči del revizije;

8. zagotoviti, da bo organ za varstvo podatkov redno preverjal tudi zunanje ponudnike storitev;

Pravice posameznikov, na katere se nanašajo podatki

9. poiskati ustrezen način, kako bi organ za varstvo podatkov, ministrstvo za notranje zadeve ter ministrstvo za zunanje in evropske zadeve obveščali posameznike, na katere se nanašajo osebni podatki, o morebitnih tveganjih pri predložitvi kopij osebnih izkaznic in občutljivih informacij prek odprtega interneta. Ministrstvo za notranje zadeve ter ministrstvo za zunanje in evropske zadeve sta pozvana k razmisleku o tem, da bi za posameznike, na katere se nanašajo osebni podatki, zagotovila varen kanal za elektronsko predložitev takih dokumentov;

10. zagotoviti, da se 60-dnevni rok za odgovor na zahtevke posameznikov, na katere se nanašajo osebni podatki v SIS II, iz člena 41(6) uredbe SIS II in člena 58(6) sklepa SIS II spoštuje, dokler se v celoti ne začne uporabljati novi pravni red SIS[1] (najpozneje do 28. decembra 2021), ki se sklicuje na rok, ki je za odgovor na zahtevke posameznikov, na katere se nanašajo osebni podatki, določen v splošni uredbi o varstvu podatkov (30 dni z možnostjo podaljšanja za dva dodatna meseca, če je potrebno);

11. proučiti možnosti za zagotavljanje tiskanega gradiva (zloženk, plakatov ipd.) posameznikom, na katere se nanašajo osebni podatki, na policijskih postajah, ki bo vidno in zlahka dostopno;

12. proučiti možnosti, na primer za zagotavljanje neuradne angleške različice odločb organa za varstvo podatkov v zvezi s pritožbami glede zahtevkov posameznikov, na katere se nanašajo osebni podatki, za SIS II; tako bi posamezniki, na katere se nanašajo osebni podatki, bolje razumeli odločbe, kar bi okrepilo pravice posameznikov, na katere se nanašajo osebni podatki;

13. zagotoviti lažje iskanje informacij o pravicah posameznikov, na katere se nanašajo osebni podatki v VIS, na spletišču ministrstva za zunanje in evropske zadeve; na spletišču bi morale biti na voljo tudi predloge za uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki v VIS;

---

[1] Uredba (EU) 2018/1862 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, o spremembi in razveljavitvi Sklepa Sveta 2007/533/PNZ ter o razveljavitvi Uredbe (ES) št. 1986/2006 Evropskega parlamenta in Sveta in Sklepa Komisije 2010/261/EU (UL L 312, 7.12.2018, str. 56; glej zlasti člene 66–71); Uredba (EU) 2018/1861 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju mejnih kontrol, o spremembi Konvencije o izvajanju Schengenskega sporazuma ter o spremembi in razveljavitvi Uredbe (ES) št. 1987/2006 (UL L 312, 7.12.2018, str. 14; glej zlasti člene 51–57).

14. zagotoviti, da vloga za izdajo vizuma vsebuje jasne informacije o različnih organih, ki obdelujejo osebne podatke v nacionalnem vizumskem sistemu. Zlasti bi morala biti navedena informacija, da je upravljavec podatkov ministrstvo za zunanje in evropske zadeve;

15. zagotoviti tiskane informacije (letake, plakate ipd.) posameznikom, na katere se nanašajo osebni podatki v VIS, na letališčih in drugih mejnih kontrolnih točkah, na viden in zlahka dostopen način;

16. zagotoviti, da odgovori posameznikom, na katere se nanašajo osebni podatki, za VIS vključujejo informacijo o možnosti pritožbe zoper odgovor pri organu za varstvo podatkov in pristojnem sodišču;

17. sprejeti ustrezne ukrepe, da se jasno opredeli odgovornost ministrstva za zunanje in evropske zadeve ter ministrstva za notranje zadeve za obravnavanje zahtevkov posameznikov, na katere se nanašajo osebni podatki v VIS, ter zagotovijo notranje ali metodološke smernice za oba organa; te informacije bi morale biti na voljo posameznikom, na katere se nanašajo osebni podatki;

Vizumski informacijski sistem

18. sprejeti potrebne ukrepe za višjo raven varnosti pri dostopu do vladnega okolja in zlasti nacionalnih vlog za izdajo vizumov pri ministrstvu za zunanje in evropske zadeve ter ministrstvu za notranje zadeve, predvsem z dostopom do nacionalnih vizumskih podatkovnih zbirk prek večfaktorske tehnologije;

19. sprejeti potrebne ukrepe za izboljšanje fizične in organizacijske varnosti v podatkovnem centru za N.VIS ministrstva za zunanje in evropske zadeve, zlasti glede naslednjih vidikov:

   – vodenje evidence obiskovalcev pri vhodu v podatkovni center za osebje IKT, obiskovalce ali dobavitelje, katerih dostop bi moral biti omejen;

   – namestitev sistema za gašenje požarov s plinom (aragonit);

   – namestitev sistema za odkrivanje iztekanja vode;

   – čiščenje prahu s tal in skrb za njihovo urejenost;

   – zaklepanje zaščitne ograde za strežnike EU;

20. pospešiti postopek za vzpostavitev novega podatkovnega centra za N.VIS na drugi lokaciji in preselitev sedanjega podatkovnega centra;

21. proučiti možnosti za spremembo lokalnega obdobja hrambe evidenc N.VIS na diplomatskih in konzularnih predstavništvih z določitvijo časovnega obdobja namesto količine MB;

22. proučiti možnosti za uporabo sistemov za avtomatski nadzor evidenc na ministrstvu za zunanje in evropske zadeve;

23. sprejeti potrebne ukrepe, da bodo diplomatska predstavništva ali ministrstvo za zunanje in evropske zadeve redno izvajala inšpekcijske preglede zunanjih ponudnikov storitev;

24. sprejeti potrebne ukrepe za bolj sistematično in enotno zagotavljanje usposabljanj o varstvu podatkov lokalnemu konzularnemu osebju;

25. zagotoviti, da so v elektronski vlogi za izdajo vizuma zahtevani enaki podatki kot v vlogi za izdajo vizuma v papirni obliki (kot je določeno v Prilogi I k vizumskemu zakoniku EU[1]);

Schengenski informacijski sistem II

26. sprejeti potrebne ukrepe za višjo raven varnosti pri dostopu do N.SIS II, zlasti z uporabo večfaktorske avtentikacije in zgolj z uporabo povezav https pri dostopu do N.SIS II;

27. zagotoviti, da ministrstvo za notranje zadeve obvesti organ za varstvo podatkov o vsaki kršitvi varstva podatkov, ki bi lahko ogrozila pravice in svoboščine fizičnih oseb. Ministrstvo za notranje zadeve bi moralo poleg tega vzpostaviti register kršitev varstva osebnih podatkov;

[1] Uredba (ES) št. 810/2009 Evropskega parlamenta in Sveta z dne 13. julija 2009 o vizumskem zakoniku Skupnosti (Vizumski zakonik). UL L 243/1, 15.9.2009.

Ozaveščanje javnosti

28. proučiti, kako bi lahko posameznikom, na katere se nanašajo osebni podatki, dali na voljo zloženke organa za varstvo podatkov na dostopnejših mestih, kot so policijske postaje, območja nadzora meje in konzulati;

29. proučiti, ali bi lahko predstavitve, seminarje in dogodke odprtih vrat organa za varstvo podatkov omogočili tudi širši javnosti, zlasti posameznikom, na katere se nanašajo podatki, saj informacije o SIS II in VIS zadevajo tudi njih.

V Bruslju,

Za Svet
Predsednik