Svet
Evropske unije

Bruselj, 22. februar 2022
(OR. en)

6426/22

Medinstitucionalna zadeva:
2021/0392(NLE)

SCH-EVAL 21
DATAPROTECT 42
COMIX 87

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Datum:	21. februar 2022
Prejemnik:	delegacije
Št. predh. dok.:	5893/22
Zadeva:	Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih leta 2019 med ocenjevanjem uporabe schengenskega pravnega reda na področju **varstva podatkov** na **Poljskem**

V prilogi vam pošiljamo Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih leta 2019 med ocenjevanjem uporabe schengenskega pravnega reda na področju varstva podatkov na Poljskem, ki ga je Svet sprejel na seji 21. februarja 2022.

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 na področju varstva podatkov na Poljskem

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) V skladu z Uredbo (EU) št. 1053/2013 je bilo leta 2019 izvedeno ocenjevanje za preverjanje uporabe schengenskega pravnega reda na področju varstva osebnih podatkov na Poljskem. Po ocenjevanju je bilo z Izvedbenim sklepom Komisije C(2021) 9100 sprejeto poročilo z ugotovitvami in ocenami, v katerem so navedene dobre prakse in pomanjkljivosti, ugotovljene med ocenjevanjem.

(2) Glede na rezultate ocenjevanja je primerno Poljski priporočiti nekatere ukrepe za odpravo ugotovljenih pomanjkljivosti.

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

(3) Za dobro prakso se štejejo zlasti: nacionalni pravni okvir, ki predsedniku poljskega organa za varstvo podatkov omogoča, da neodvisno imenuje svoje namestnike in člane svetovalnega sveta; obveznost, da morajo kandidati za položaj predsednika organa za varstvo podatkov v parlamentu prestati javno zaslišanje, ki se prenaša tudi prek uradnega kanala parlamenta na internetu; pogoste kontrolne dejavnosti v zvezi z zunanjimi ponudniki storitev, pri katerih sodeluje pooblaščena oseba za varstvo podatkov, in pogoste kontrole konzulatov; zavezanost usposabljanju in razvoju – tudi v zvezi z varstvom podatkov – osebja, ki je končni uporabnik nacionalnega Schengenskega informacijskega sistema (N. SIS), in osebja urada SIRENE; varnostne ukrepe, ki se izvajajo v prostorih podatkovnih centrov, ki gostijo N. SIS in nacionalni Vizumski informacijski sistem (N. VIS).

(4) Glede na pomen spoštovanja schengenskega pravnega reda o varstvu osebnih podatkov v zvezi z Vizumskim informacijskim sistemom (VIS) in Schengenskim informacijskim sistemom (SIS) bi bilo treba prednost dati izvajanju priporočil 11, 12, 13, 20, 21 in 22 iz tega sklepa.

(5) V skladu z Uredbo (EU) št. 1053/2013 bi bilo treba ta sklep poslati Evropskemu parlamentu in parlamentom držav članic, Poljska pa bi morala 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:

Poljska bi morala:

Zakonodaja

1. izrecno razjasniti uporabo Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) za obdelavo osebnih podatkov v N. VIS oziroma N. SIS;

Organ za varstvo podatkov

2. poskrbeti, da člen 174 zakona o varstvu podatkov iz leta 2018 in člen 106 zakona o varstvu podatkov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj iz leta 2018, ki določa zgornjo mejo letnih stroškov, ne omejujeta proračuna poljskega organa za varstvo podatkov niže, kot je zanj predvideno v državnem proračunu;

3. poskrbeti, da organ za varstvo podatkov bolje načrtuje in organizira številne preglede N. SIS II, za zagotovitev, da so zajeti vsi postopki obdelave N. SIS II in vsi zadevni subjekti ter se na podlagi pregledov opravi celovita revizija N. SIS II, kot je določeno v členu 44(2) Uredbe (ES) št. 1987/2006;

4. poskrbeti, da organ za varstvo podatkov opravi celovit pregled N. VIS, da v celoti izpolni svoje naloge iz člena 41(2) Uredbe (ES) št. 767/2008;

Pravice posameznikov, na katere se nanašajo osebni podatki

5. poskrbeti za izboljšanje statistike organa za varstvo podatkov v zvezi z uveljavljanjem pravic posameznikov, na katere se nanašajo osebni podatki, ter razlikovati med pritožbami in zahtevami, sistemoma, na katera se nanašajo (SIS ali VIS), vsebinami ter vrstami zahtev (popravek, izbris, dostop);

6. poskrbeti, da postane upravljavec podatkov bolj proaktiven pri nudenju informacij posameznikom, na katere se nanašajo osebni podatki, o njihovih pravicah v zvezi s podatki VIS;

7. poskrbeti, da upravljavec podatkov SIS in VIS (poljska nacionalna policija – osrednji tehnični organ za nacionalni informacijski sistem) objavi standardne obrazce za zahtevke za uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki;

Vizumski informacijski sistem

8. poskrbeti, da evidence o dostopu do VIS vsebujejo tudi informacije o utemeljitvi tega dostopa;

9. ponovno oceniti seznam organov z dostopom do VIS in njihove pravice dostopa do podatkov VIS glede na njihove pristojnosti in uporabo teh podatkov v praksi;

10. glede na številne upravljavce podatkov VIS, imenovane z nacionalnimi zakoni in pogodbenimi določbami, in glede na število vpletenih akterjev pojasniti razmerje med organi, vključenimi v postopek izdaje vizumov, in organi, ki obdelujejo podatke VIS, ter odgovornosti teh organov za obdelavo podatkov;

11. za popoln izkoristek dnevniških datotek, ki se hranijo, poskrbeti, da se dnevniške datoteke VIS redno analizirajo za spremljanje varstva podatkov;

12. sprejeti varnostni načrt VIS, ki naj zajema fizično varnost druge lokacije podatkov in druge vidike informacijske varnosti nacionalnega informacijskega sistema, vključno z N. VIS;

13. uskladiti obdobje hrambe dnevnikov v aplikacijah, povezanih z VIS (zlasti v aplikacijah „Pobyt“ in „ZSE 6“), z roki iz člena 34(2) Uredbe (ES) št. 767/2008 in člena 16 Sklepa Sveta 2008/633/PNZ;

Schengenski informacijski sistem II

14. poskrbeti, da upravljavec N. SIS II vzpostavi centralni sistem za upravljanje uporabnikov, ki omogoča učinkovit notranji nadzor brez preverjanja dnevnikov v institucijah, ki so končni uporabniki N. SIS II;

15. za popoln izkoristek dnevniških datotek, ki se hranijo, poskrbeti, da se dnevniške datoteke SIS redno analizirajo za spremljanje varstva podatkov;

16. poskrbeti za samodejno obveščanje o dogodkih v zvezi z informacijsko varnostjo in dejavnostih notranjega spremljanja upravljavca podatkov, da se varnost dodatno izboljša;

17. poskrbeti, da tehnični ukrepi vključujejo tudi blokiranje uporabe naprav USB in ključkov USB z blokiranjem vseh vrat USB na delovnih postajah SIS;

18. razmisliti o tem, da bi pooblaščena oseba za varstvo podatkov na ministrstvu za notranje zadeve s spremljanjem revizijskih dnevnikov proaktivno in redno sodelovala pri spremljanju obdelave podatkov SIS in VIS;

19. poskrbeti, da upravljavec podatkov SIS organu za varstvo podatkov posreduje profile osebja vseh organov, ki imajo dostop do SIS;

20. obdobje hrambe dnevnikov v aplikacijah z dostopom do podatkov SIS uskladiti s členom 12(4) Uredbe (ES) št. 1987/2006 in členom 12(4) Sklepa Sveta 2007/533/PNZ;

21. poskrbeti, da upravljavec podatkov SIS v skladu s členom 10 Uredbe (ES) št. 1987/2006 in členom 10 Sklepa Sveta 2007/533/PNZ sprejme varnostni načrt SIS;

22. poskrbeti za pregled širokega spektra institucij z dostopom do podatkov SIS II, da se zagotovi, da imajo dostop do podatkov le institucije, ki glede na svoje pristojnosti in praktične potrebe dostop morajo imeti;

Ozaveščanje javnosti

23. poskrbeti, da spletni mesti organa za varstvo podatkov in policije vsebujeta informacije o pravicah posameznikov, na katere se nanašajo osebni podatki, v zvezi s podatki VIS.

V Bruslju,

Za Svet
predsednik