Rada
Európskej únie

V Bruseli 24. septembra 2019
(OR. en)

12469/19

Medziinštitucionálny spis:
2019/0169(NLE)

SCH-EVAL 158
DATAPROTECT 217
COMIX 428

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	20. septembra 2019
Komu:	Delegácie
Č. predch. dok.:	11906/1/19 REV 1
Predmet:	Vykonávacie rozhodnutie Rady, ktorým sa stanovuje odporúčanie týkajúce sa riešenia nedostatkov zistených v roku 2018 pri hodnotení **Lotyšska,** pokiaľ ide o uplatňovanie schengenského *acquis* v oblasti **ochrany údajov**

Delegáciám v prílohe zasielame vykonávacie rozhodnutie Rady, ktorým sa stanovuje odporúčanie týkajúce sa riešenia nedostatkov zistených v roku 2018 pri hodnotení Lotyšska, pokiaľ ide o uplatňovanie schengenského *acquis* v oblasti ochrany údajov, ktoré Rada prijala na zasadnutí 20. septembra 2019.

Toto odporúčanie sa v súlade s článkom 15 ods. 3 nariadenia Rady (EÚ) č. 1053/2013 zo 7. októbra 2013 zašle Európskemu parlamentu a národným parlamentom.

Vykonávacie rozhodnutie Rady, ktorým sa stanovuje

ODPORÚČANIE

týkajúce sa riešenia nedostatkov zistených v roku 2018 pri hodnotení Lotyšska, pokiaľ ide o uplatňovanie schengenského *acquis* v oblasti ochrany údajov

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Rady (EÚ) č. 1053/2013 zo 7. októbra 2013, ktorým sa vytvára hodnotiaci a monitorovací mechanizmus na overenie uplatňovania schengenského *acquis* a ktorým sa zrušuje rozhodnutie výkonného výboru zo 16. septembra 1998, ktorým bol zriadený Stály výbor pre hodnotenie a vykonávanie Schengenu[1], a najmä na jeho článok 15,

so zreteľom na návrh Európskej komisie,

keďže:

(1) Účelom tohto rozhodnutia je odporučiť Lotyšsku nápravné opatrenia na riešenie nedostatkov zistených počas schengenského hodnotenia v roku 2018 v oblasti ochrany údajov. V nadväznosti na toto hodnotenie bola vykonávacím rozhodnutím Komisie C(2019) 5720 prijatá správa o zisteniach a hodnoteniach, v ktorej sa uvádzajú aj najlepšie postupy a nedostatky zistené počas hodnotenia.

(2) Za osvedčený postup sa okrem iného považuje úspešné využívanie finančných prostriedkov Európskej komisie na zvýšenie informovanosti verejnosti a skutočnosť, že odpovede útvaru SIRENE sa zvyčajne poskytujú v krátkom čase a v rôznych jazykoch.

[1] Ú. v. EÚ L 295, 6.11.2013, s. 27.

(3) Vzhľadom na dôležitosť dodržiavania schengenského *acquis* v oblasti ochrany údajov v súvislosti so Schengenským informačným systémom II (SIS II) by sa prednostne mali vykonať odporúčania 15 až 18.

(4) Vzhľadom na dôležitosť dodržiavania schengenského *acquis* v oblasti ochrany údajov v súvislosti s vízovým informačným systémom (VIS) by sa prednostne mali vykonať odporúčania 9 a 11.

(5) Toto rozhodnutie by sa malo zaslať Európskemu parlamentu a parlamentom členských štátov. Do troch mesiacov od jeho prijatia by Lotyšsko malo v súlade s článkom 16 ods. 1 nariadenia (EÚ) č. 1053/2013 vypracovať akčný plán so zoznamom všetkých odporúčaní na nápravu všetkých nedostatkov uvedených v hodnotiacej správe a predložiť ho Komisii a Rade,

ODPORÚČA:

že Lotyšsko by malo:

Dozorný orgán pre ochranu údajov

1. zabezpečiť úplnú nezávislosť orgánu pre ochranu údajov (ďalej len „OOÚ“) prijatím vnútroštátnych právnych predpisov, ktoré sú v súlade s kapitolou VI všeobecného nariadenia o ochrane údajov, najmä pokiaľ ide o postup odvolania riaditeľa;

2. zabezpečiť, aby sa OOÚ poskytli dostatočné finančné prostriedky a primeraný počet zamestnancov, aby mohol plniť všetky úlohy, ktorými bol poverený na základe *acquis* týkajúceho sa Schengenského informačného systému II (ďalej len „SIS II“) a vízového informačného systému (ďalej len „VIS“);

3. zabezpečiť, aby bol včas vykonaný audit operácií spracúvania údajov v N.SIS, ako sa požaduje v článku 44 ods. 2 nariadenia o SIS II a v článku 60 ods. 2 rozhodnutia Rady o SIS II;

4. zabezpečiť, aby bol včas vykonaný audit operácií spracúvania údajov v NVIS, ako sa požaduje v článku 41 ods. 2 nariadenia o VIS a v článku 8 ods. 6 rozhodnutia Rady o VIS;

5. zabezpečiť, aby budúce audity SIS II a VIS boli komplexné a aby boli vykonávané v súlade s medzinárodnými audítorskými štandardmi, ako to vyžaduje *acquis* týkajúce sa SIS II a VIS, a zabezpečiť, aby boli pre uvedené audity zaistené potrebné odborné znalosti v oblasti IT;

6. zabezpečiť, aby činnosti dohľadu OOÚ v súvislosti so SIS II zahŕňali pravidelné kontroly zápisov do SIS II;

7. zabezpečiť, aby činnosti dohľadu OOÚ v súvislosti s VIS zahŕňali pravidelné kontroly konzulárnych úradov;

8. zabezpečiť, aby viacročný plán kontrol OOÚ zahŕňal aj iné kontrolné činnosti, ako sú povinné audity systémov SIS II a VIS;

Vízový informačný systém

9. zabezpečiť, aby sa logy pravidelne analyzovali na účely monitorovania zákonnosti činností spracúvania údajov v súlade s článkom 34 ods. 1 a 2 nariadenia o VIS;

10. objasniť úlohu (sprostredkovateľ údajov alebo spoločný prevádzkovateľ) ministerstva zahraničných vecí – vo vzťahu k Úradu pre občianstvo a migráciu;

11. zabezpečiť, aby Úrad pre občianstvo a migráciu častejšie vykonával vlastný audit činností v oblasti spracúvania údajov v rámci VIS;

12. revidovať a upraviť zmluvy s externými poskytovateľmi služieb tak, aby bol zabezpečený súlad s požiadavkami stanovenými vo všeobecnom nariadení o ochrane údajov;

13. jasne vymedziť úlohy a právomoci zodpovedných osôb v rámci Úradu pre občianstvo a migráciu a ministerstva zahraničných vecí;

14. zabezpečiť, aby online formuláre používané v súvislosti so žiadosťami o vízum obsahovali oznámenie o ochrane údajov informujúce dotknuté osoby o činnostiach spracovania údajov a o uplatniteľných individuálnych právach;

Schengenský informačný systém

15. zabezpečiť, aby polícia vykonávala pravidelné vlastné audity, najmä vlastné monitorovanie logov;

16. generovať vnútroštátne logy SIS II na centrálnej úrovni a zabezpečiť, aby bolo vyhľadávanie odôvodnené na základe príslušného logu;

17. zabezpečiť, aby sa logy pravidelne preskúmavali s cieľom kontrolovať zákonnosť spracúvania údajov v súlade s článkom 12 ods. 2 nariadenia o SIS II a s rozhodnutím Rady o SIS II.

18. minimalizovať bezpečnostné riziko, ktoré predstavuje mobilná aplikácia umožňujúca prístup k SIS II, napríklad poskytnutím prístupu iba prostredníctvom služby virtuálnej privátnej siete (VPN);

19. zaviesť dvojúrovňový autentifikačný systém;

20. zabezpečiť, aby sa produkčné údaje nepožívali na skúšobné účely a aby vyhľadávanie v systéme N.SIS mohli vykonávať iba náležite oprávnení používatelia;

21. jasne vymedziť úlohy a právomoci zodpovednej osoby v rámci polície, vrátane jej účasti na interných monitorovacích činnostiach, ako je monitorovanie účinnosti bezpečnostných opatrení;

Práva dotknutých osôb a zvyšovanie informovanosti

22. pravidelne poskytovať OOÚ štatistické údaje o uplatňovaní práv dotknutých osôb v súvislosti so SIS II a VIS;

23. zabezpečiť, aby informačné materiály, ako napríklad brožúra „Personal Data in the Schengen Information System“ (Osobné údaje v Schengenskom informačnom systéme) boli na letisku a na iných verejných miestach lepšie dostupné.

V Bruseli

Za Radu
predseda