Rada
Evropské unie

Brusel 24. září 2019
(OR. en)

12469/19

Interinstitucionální spis:
2019/0169(NLE)

SCH-EVAL 158
DATAPROTECT 217
COMIX 428

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	20. září 2019
Příjemce:	Delegace
Č. předchozího dokumentu:	11906/1/19 REV 1
Předmět:	Prováděcí rozhodnutí Rady, kterým se stanoví doporučení týkající se řešení nedostatků zjištěných v roce 2018 při hodnocení toho, jak **Lotyšsko** uplatňuje schengenské acquis v oblasti **ochrany údajů**

Delegace naleznou v příloze prováděcí rozhodnutí Rady, kterým se stanoví doporučení týkající se řešení nedostatků zjištěných v roce 2018 při hodnocení toho, jak Lotyšsko uplatňuje schengenské *acquis* v oblasti ochrany údajů, které Rada přijala na zasedání konaném dne 20. září 2019.

V souladu s čl. 15 odst. 3 nařízení Rady (EU) č. 1053/2013 ze dne 7. října 2013 bude toto doporučení předáno Evropskému parlamentu a vnitrostátním parlamentům.

Prováděcí rozhodnutí Rady, kterým se stanoví

DOPORUČENÍ

týkající se řešení nedostatků zjištěných v roce 2018 při hodnocení toho, jak Lotyšsko uplatňuje schengenské *acquis* v oblasti ochrany údajů

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Rady (EU) č. 1053/2013 ze dne 7. října 2013 o vytvoření hodnotícího a monitorovacího mechanismu k ověření uplatňování schengenského *acquis* a o zrušení rozhodnutí výkonného výboru ze dne 16. září 1998, kterým se zřizuje Stálý výbor pro hodnocení a provádění Schengenu[1], a zejména na článek 15 uvedeného nařízení,

s ohledem na návrh Evropské komise,

vzhledem k těmto důvodům:

(1) Účelem tohoto rozhodnutí je doporučit Lotyšsku nápravná opatření k řešení nedostatků zjištěných při schengenském hodnocení v oblasti ochrany údajů, které proběhlo v roce 2018. V návaznosti na hodnocení byla prováděcím rozhodnutím Komise C(2019) 5720 přijata zpráva, která obsahuje tato zjištění a hodnocení a uvádí osvědčené postupy a nedostatky zjištěné během hodnocení.

(2) Za osvědčené postupy lze mimo jiné považovat úspěšné využití financování Evropské komise ke zlepšení informovanosti veřejnosti a skutečnost, že odpovědi centrály SIRENE jsou k dispozici v různých jazycích a že jsou obvykle poskytovány v krátké době.

[1] Úř. věst. L 295, 6.11.2013, s. 27.

(3) Vzhledem k tomu, že je důležité dodržovat schengenské *acquis* v oblasti ochrany údajů v souvislosti se Schengenským informačním systémem II (SIS II), měla by být přednostně provedena doporučení uvedená v bodech 15 až 18.

(4) Vzhledem k tomu, že je důležité dodržovat schengenské *acquis* v oblasti ochrany údajů v souvislosti s Vízovým informačním systémem (VIS), měla by být přednostně provedena doporučení uvedená v bodech 9 a 11.

(5) Toto rozhodnutí by mělo být předloženo Evropskému parlamentu a parlamentům členských států. Do tří měsíců od jeho přijetí by Lotyšsko podle čl. 16 odst. 1 nařízení (EU) č. 1053/2013 mělo vypracovat akční plán s výčtem všech doporučení k odstranění veškerých nedostatků zjištěných v hodnotící zprávě a předloží jej Komisi a Radě,

DOPORUČUJE:

Lotyšsko by mělo:

Dozorový úřad pro ochranu údajů

1. zajistit úplnou nezávislost úřadu pro ochranu údajů a přijmout v tomto ohledu vnitrostátní právní předpisy, které budou v souladu s kapitolou VI obecného nařízení o ochraně osobních údajů, zejména pokud jde o postup pro odvolání ředitele;

2. zajistit, aby měl úřad pro ochranu údajů k dispozici dostatečné financování a přiměřený počet zaměstnanců, aby mohl plnit všechny úkoly, které mu byly svěřeny v rámci *acquis* v oblasti Schengenského informačního systému II (dále jen „SIS II“) a Vízového informačního systému (dále jen „VIS“);

3. zajistit, aby byl včas proveden audit činností zpracování údajů v N.SIS, jak požaduje čl. 44 odst. 2 nařízení o SIS II a čl. 60 odst. 2 rozhodnutí Rady o SIS II;

4. zajistit, aby byl včas proveden audit činností zpracování údajů v N-VIS, jak požaduje čl. 41 odst. 2 nařízení o VIS a čl. 8 odst. 6 rozhodnutí Rady o VIS;

5. zajistit, aby budoucí audity SIS II a VIS byly komplexní a byly vedeny podle mezinárodních auditorských standardů, jak požaduje *acquis* SIS II a VIS, a zajistit, aby byli pro tyto audity zajištěni potřební odborníci na informatiku;

6. zajistit, aby součástí dozorové činnosti úřadu pro ochranu údajů v souvislosti se SIS II byly pravidelné kontroly záznamů v SIS II;

7. zajistit, aby součástí dozorové činnosti úřadu pro ochranu údajů v souvislosti s VIS byly pravidelné kontroly konzulárních úřadů;

8. zajistit, aby víceletý plán kontrol prováděných úřadem pro ochranu údajů zahrnoval i jiné kontrolní činnosti, než jsou povinné audity SIS II a VIS;

Vízový informační systém

9. zajistit pravidelnou analýzu souborů protokolů za účelem kontroly zákonnosti činností zpracování údajů v souladu s čl. 34 odst. 1 a 2 nařízení o VIS;

10. vyjasnit úlohu ministerstva zahraničních věcí (zpracovatel údajů nebo společný správce) ve vztahu k úřadu pro občanství a migraci;

11. zajistit, aby úřad pro občanství a migraci častěji prováděl interní audity činností zpracování údajů v rámci VIS;

12. revidovat smlouvy s externími poskytovateli služeb tak, aby byly v souladu s požadavky stanovenými v obecném nařízení o ochraně osobních údajů;

13. jasně vymezit úkoly a pravomoci pověřenců pro ochranu údajů na úřadu pro občanství a migraci a ministerstvu zahraničních věcí;

14. zajistit, aby online formuláře používané v souvislosti s žádostmi o vízum obsahovaly oznámení o ochraně osobních údajů informující subjekty údajů o činnostech v oblasti zpracování údajů a použitelných individuálních právech;

Schengenský informační systém

15. zajistit, aby policie pravidelně prováděla interní audity, zejména interní kontroly protokolů;

16. generovat vnitrostátní protokoly SIS II na centrální úrovni a zajistit, aby na základě těchto protokolů bylo možné stanovit oprávněnost vyhledávání;

17. zajistit pravidelné přezkoumávání souborů protokolů za účelem kontroly zákonnosti zpracovávání údajů v souladu s čl. 12 odst. 2 nařízení o SIS II a rozhodnutí Rady o SIS II;

18. minimalizovat bezpečnostní riziko spojené s mobilní aplikací, jež umožňuje přístup k SIS II, například povolením přístupu pouze prostřednictvím služby VPN;

19. zavést dvoufaktorový autentizační systém;

20. zajistit, aby produkční údaje nebyly používány pro zkušební účely a aby vyhledávání v systému N.SIS mohly provádět pouze oprávněné osoby;

21. jasně vymezit úkoly a pravomoci pověřence pro ochranu osobních údajů u policie, včetně jeho účasti na vnitřních monitorovacích činnostech, jako je monitorování účinnosti bezpečnostních opatření;

Práva subjektů údajů a zvyšování informovanosti

22. pravidelně poskytovat úřadu pro ochranu údajů statistiky ohledně výkonu práv subjektů údajů týkajících se SIS II a VIS;

23. zvýšit dostupnost informačních materiálů, jako je brožurka *Personal Data in the Schengen Information System* (Osobní údaje v Schengenském informačním systému), na letišti a dalších veřejných místech.

V Bruselu dne

Za Radu
předseda nebo *předsedkyně*