Rada
Evropské unie

Brusel 24. září 2019
(OR. en)

12468/19

**Interinstitucionální spis:**
**2019/0168(NLE)**

**SCH-EVAL 157**
**DATAPROTECT 216**
**COMIX 427**

**VÝSLEDEK JEDNÁNÍ**

| | |
|---|---|
| Odesílatel: | Generální sekretariát Rady |
| Datum: | 20. září 2019 |
| Příjemce: | Delegace |
| Č. předchozího dokumentu: | 11904/19 |
| Předmět: | Prováděcí rozhodnutí Rady, kterým se stanoví doporučení týkající se řešení nedostatků zjištěných v roce 2018 při hodnocení toho, jak **Litva** 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 Litva 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 Litva 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 Litvě 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) 5700 přijata zpráva, která obsahuje tato zjištění a hodnocení a uvádí osvědčené postupy a nedostatky zjištěné během hodnocení.

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

(2) Za osvědčené postupy lze mimo jiné považovat: skutečnost, že úřad pro ochranu údajů poskytuje poradenství a pokyny jednotlivcům, kteří se na něj obrátí, místo aby žádosti pouze předával dál; vzorové dopisy pro uplatňování práv subjektů údajů v souvislosti se Schengenským informačním systémem II (SIS II) a Vízovým informačním systémem (VIS); obecně vysoká úroveň bezpečnostních opatření zavedených v prostorách oddělení pro informační technologie a komunikaci na ministerstvu vnitra (ITCD, jež provozuje N.VIS a N.SIS), která zajišťují bezpečné prostředí pro uchovávání údajů a prevenci případných incidentů; propracovaná odborná příprava pro koncové uživatele VIS, zejména pro konzulární pracovníky před vysláním na velvyslanectví nebo konzulát; odhodlání ke vzdělávání a rozvoji pracovníků – zde je třeba zmínit zejména propracovanou odbornou přípravu na téma ochrany údajů pro koncové uživatele N.SIS a zaměstnance centrály SIRENE; ucelené, užitečné a srozumitelné informace (dostupné v několika jazycích) týkající se SIS II a VIS poskytované na internetových stránkách úřadu pro ochranu údajů; informační brožury úřadu pro ochranu údajů „*Personal Data Protection in the Schengen Information System*“ (*Ochrana osobních údajů v Schengenském informačním systému*) a „*Personal Data Protection in the Visa Information System*“ (*Ochrana osobních údajů ve Vízovém informačním systému*), jež poskytují velmi dobré a dostupné informace o zpracování údajů v obou databázích a o souvisejících právech subjektů údajů, jakož aktivní účast úřadu pro ochranu údajů na mnoha konferencích, školeních a dalších akcích na zvyšování informovanosti, jež jsou mimo jiné určeny pracovníkům zabývajícím se zpracováním údajů v SIS II a VIS.

(3) Vzhledem k tomu, že je důležité dodržovat schengenské *acquis* v oblasti ochrany údajů, zejména pokud jde o plnou nezávislost úřadu pro ochranu údajů, mělo by být přednostně provedeno doporučení uvedené v bodě 1.

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

DOPORUČUJE:

aby Litva:

**Dozorový úřad pro ochranu údajů**

1. zrušila v zájmu lepšího zajištění plné nezávislosti Státního inspektorátu pro ochranu údajů (dále jen „úřad pro ochranu údajů“) požadavek, aby strategický akční plán úřadu pro ochranu údajů podléhal schválení ministrem spravedlnosti a aby byl tento akční plán s ministrem spravedlnosti konzultován, dříve než jej ředitel úřadu pro ochranu údajů může schválit; zrušení je důležité i pro zajištění toho, aby v rámci rozpočtového procesu neexistovalo žádné riziko narušení nezávislosti úřadu pro ochranu údajů;

2. pořádala v zájmu lepšího zajištění plné nezávislosti úřadu pro ochranu údajů pravidelná dvoustranná setkání ministra spravedlnosti a ředitele úřadu pro ochranu údajů tak, aby nemohlo vzniknout riziko přímého nebo nepřímého ovlivňování úřadu pro ochranu údajů ze strany vlády, jež by mohlo ohrozit nezávislost úřadu pro ochranu údajů;

3. odstranila všechny prvky odpovědnosti ředitele úřadu pro ochranu údajů vůči vládě a ministru spravedlnosti, které by mohly mít za následek riziko přímého nebo nepřímého ovlivňování ze strany vlády a ministra spravedlnosti a mohly by ohrozit nezávislost úřadu pro ochranu údajů;

4. zajistila, aby úřad pro ochranu údajů častěji sledoval zákonnost zpracování osobních údajů v SIS II;

5. zajistila, aby úřad pro ochranu údajů přinejmenším každé čtyři roky prováděl audity operací zpracování údajů v systému N.SIS;

6. zajistila, aby úřad pro ochranu údajů častěji sledoval zákonnost zpracování osobních údajů ve VIS. Úřad pro ochranu údajů by měl rovněž při inspekcích velvyslanectví provádět kontroly operací zpracování údajů a zabezpečení údajů u externích poskytovatelů služeb; tato možnost by měla být uvedena ve smlouvě mezi ministerstvem zahraničních věcí a externími poskytovateli služeb;

7. zajistila, aby úřad pro ochranu údajů přinejmenším každé čtyři roky prováděl audity operací zpracování údajů v systému N.VIS;

**Práva subjektů údajů**

8. zajistila, aby byla dodržována 60denní lhůta pro odpověď na žádosti subjektů údajů o přístup k údajům v SIS II stanovená v čl. 41 odst. 6 nařízení o SIS II a v čl. 58 odst. 6 rozhodnutí o SIS II, dokud nebude plně použitelné nové *acquis* v oblasti SIS[2] (nejpozději dne 28. prosince 2021), v němž se odkazuje na lhůtu pro odpověď na žádosti subjektů údajů stanovenou v obecném nařízení o ochraně osobních údajů[3] (30 dnů s možností prodloužení o další dva měsíce, je-li to nezbytné);

9. vyjasnila interní postupy týkající se odpovědnosti zúčastněných orgánů, pokud jde o práva subjektů údajů v souvislosti se SIS II; takto pak budou zaměstnanci moci vědět, komu příslušnou žádost postoupit;

---

[2] Nařízení Evropského parlamentu a Rady (EU) 2018/1862 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně a o zrušení rozhodnutí Rady 2007/533/SVV a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 a rozhodnutí Komise 2010/261/EU (Úř. věst. L 312, 7.12.2018, s. 56; viz zejména články 66–71). Nařízení Evropského parlamentu a Rady (EU) 2018/1861 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol, o změně Úmluvy k provedení Schengenské dohody a o změně a zrušení nařízení (ES) č. 1987/2006 (Úř. věst. L 312, 7.12.2018, s. 14; viz zejména články 51–57).

[3] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

10. zajistila konzistentnost konečných odpovědí ministerstva vnitra jednotlivcům, kteří chtějí v souvislosti se SIS II uplatnit práva subjektů údajů, tak aby jim byly poskytnuty informace o jejich právu odvolat se k úřadu pro ochranu údajů a o právu domáhat se nápravy u soudu;

11. vyjasnila interní postupy týkající se odpovědnosti zúčastněných orgánů, pokud jde o nakládání s právy subjektů údajů v souvislosti s VIS; takto pak budou zaměstnanci moci vědět, komu příslušnou žádost postoupit;

12. zajistila konzistentnost konečných odpovědí ministerstva vnitra jednotlivcům, kteří chtějí v souvislosti s VIS uplatnit práva subjektů údajů, tak aby jim byly poskytnuty informace o jejich právu odvolat se k úřadu pro ochranu údajů a o právu domáhat se nápravy u soudu;

**Vízový informační systém**

13. podnikla nezbytné kroky k zajištění toho, aby smlouvy mezi ministerstvem zahraničních věcí a externími poskytovateli služeb upravovaly způsob, jakým se může litevský úřad pro ochranu údajů podílet na kontrolách prováděných velvyslanectvími, konzuláty a ministerstvem zahraničních věcí;

14. zlepšila interní monitoring prostřednictvím pravidelné proaktivní kontroly protokolů s cílem sledovat zákonnost zpracování osobních údajů ve VIS. Ministerstvo vnitra by mělo dále rozvíjet systém SIEM tak, aby prováděl automatickou kontrolu protokolů;

15. zajistila, aby byl pověřenec pro ochranu údajů výrazněji zapojen do přípravy a poskytování školení v oblasti ochrany údajů pro zaměstnance ministerstva zahraničních věcí včetně pracovníků vyslaných na velvyslanectví nebo konzuláty;

**Schengenský informační systém II**

16. zrušila možnost pro koncového uživatele přihlásit se prostřednictvím prohlížeče POLIS Browser do N.SIS na několika zařízeních současně;

17. zajistila, aby v zájmu zvýšení úrovně bezpečnosti byly na policii zavedeny čipové karty pro přístup k pracovním stanicím uživatelů N.SIS;

18. zajistila, aby byla plně uplatňována a pravidelně kontrolována technická opatření zavedená s cílem zabránit používání USB klíčů na pracovních stanicích v centrále SIRENE;

19. zlepšila interní monitoring prostřednictvím pravidelné proaktivní kontroly protokolů koncových uživatelů SIS II ve všech dotčených orgánech s cílem sledovat zákonnost zpracování osobních údajů v SIS II; ministerstvo vnitra by mělo dále rozvíjet systém SIEM tak, aby prováděl automatickou kontrolu protokolů;

20. zajistila větší informovanost příslušných pracovníků o ochraně údajů v souvislosti se zpracováváním údajů v SIS II a ve VIS prostřednictvím pravidelných opakovacích školení;

21. zajistila, aby oblast školení a zvyšování informovanosti pracovníků, kteří mají přístup do N.SIS, byla pod vedením skupiny pověřenců pro ochranu údajů na ministerstvu vnitra. Tímto způsobem by mohla být zajištěna stálá struktura a plánování rozvoje zaměstnanců.

**Informovanost veřejnosti**

22. zajistila, aby odkazy na internetových stránkách úřadu pro ochranu údajů ohledně SIS II a VIS byly pravidelně aktualizovány;

23. zajistila, aby internetové stránky organizací, které mají kontakty se státními příslušníky jiných zemí, jako je ministerstvo vnitra, policie, státní pohraniční stráž, ministerstvo zahraničních věcí a konzulární úřady, poskytovaly přístupné a jasné informace o SIS II a VIS a o souvisejících právech subjektů údajů také v angličtině;

24. zajistila, aby v případě, že internetové stránky poskytují informace o SIS II a VIS a o souvisejících právech subjektů údajů v angličtině, bylo snazší tyto informace nalézt;

25. zajistila jednotnost informací o uplatňování práv subjektů údajů v souvislosti s N.SIS II a VIS uvedených na internetových stránkách institucí, které s těmito systémy pracují;

26. přidala informace o zpracování údajů a právech subjektů údajů v souvislosti s VIS na portál EPM, na kterém jednotlivci poskytují údaje v žádostech o vízum.

V Bruselu dne

*Za Radu*
*předseda* nebo *předsedkyně*