Rada
Evropské unie

Brusel 17. června 2022
(OR. en)

10396/22

Interinstitucionální spis:
2021/0224(NLE)

SCH-EVAL 83
DATAPROTECT 197
COMIX 324

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	17. června 2022
Příjemce:	Delegace
Č. předchozího dokumentu:	7788/22
Předmět:	Prováděcí rozhodnutí Rady, kterým se stanoví doporučení týkající se řešení nedostatků zjištěných v roce 2020 při hodnocení toho, jak **Rakousko** 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 2020 při hodnocení toho, jak Rakousko uplatňuje schengenské *acquis* v oblasti ochrany údajů, které přijala Rada na zasedání konaném dne 17. června 2022.

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 2020 při hodnocení toho, jak Rakousko 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) V listopadu 2020 bylo v Rakousku provedeno schengenské hodnocení v oblasti ochrany údajů. V návaznosti na toto hodnocení byla prováděcím rozhodnutím Komise C(2021) 9200 přijata zpráva, která obsahuje zjištění a hodnocení a uvádí osvědčené postupy a nedostatky zjištěné během hodnocení.

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

(2) Jako osvědčené postupy jsou vnímány zejména: skutečnost, že od posledního hodnocení byl zvýšen a dále bude zvyšován počet zaměstnanců rakouského úřadu pro ochranu osobních údajů a došlo k navýšení rozpočtu; dohody se správci a zpracovateli v oblasti údajů VIS, které umožňují vysokou úroveň ochrany údajů a zajišťují, že všechny strany zapojené do zpracování údajů VIS mají zavedeny příslušné záruky ochrany údajů; školení pracovníků v otázkách ochrany údajů v souvislosti s VIS, které provádí ministerstvo vnitra a ministerstvo pro evropské a mezinárodní záležitosti; mnohostranný přístup ministerstva pro evropské a mezinárodní záležitosti k auditům postupu udělování víz; velmi podrobné a snadno přístupné informace o systémech SIS II a VIS poskytované úřadem pro ochranu osobních údajů; zpřístupnění dokumentace o systémech SIS a VIS na internetových stránkách ministerstva vnitra a rychlá reakce ministerstva na žádosti o přístup týkající se systémů SIS II a VIS.

(3) Měla by být vydána doporučení ohledně nápravných opatření, která má Rakousko přijmout za účelem řešení nedostatků zjištěných během hodnocení. Vzhledem k důležitosti dodržování schengenského *acquis* v oblasti ochrany osobních údajů by měla být přednostně provedena doporučení č. 1, 6, 7 a 13 uvedená v tomto rozhodnutí.

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

DOPORUČUJE:

Rakousko by mělo:

Právní předpisy

1. uplatňovat článek 79 obecného nařízení o ochraně osobních údajů (GDPR)[1] a provést ve svém vnitrostátním právu článek 54 směrnice (EU) 2016/680[2] s cílem zaručit právo na účinnou soudní ochranu vůči rozhodnutí správce nebo zpracovatele, který je orgánem veřejné moci;

Úřad pro ochranu osobních údajů

2. stanovit v právních předpisech důvody pro odvolání vedoucího rakouského úřadu pro ochranu osobních údajů a jeho zástupce, aby se zabránilo riziku předčasného ukončení jejich funkčního období z jiných důvodů, než je závažné pochybení nebo skutečnost, že již nesplňují podmínky požadované pro výkon jejich povinností;

3. zajistit, aby odborník v oblasti informačních technologií (IT), kterého úřad pro ochranu osobních údajů nově přijme, a jakýkoli další odborník v této oblasti měli nebo získali ucelené znalosti o Schengenském informačním systému druhé generace (SIS II) a o Vízovém informačním systému (VIS) a o řízení bezpečnosti informací, aby byli rovněž schopni aktivně se podílet na činnostech v oblasti dohledu nad systémy SIS a VIS. Úřad pro ochranu osobních údajů by měl nadále do kontrol zapojovat externí IT odborníky až do doby, kdy bude schopen zajistit plnění veškerých úkolů spojených s kontrolami v oblasti IT vlastními pracovníky;

---

[1] 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).

[2] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, s. 89).

4. zajistit, aby úřad pro ochranu osobních údajů prováděl kontrolní návštěvy v centrále SIRENE, kontroly některých koncových uživatelů systému, např. policie, a rovněž pravidelné kontroly a analýzy protokolových souborů s cílem plnit své úkoly související s komplexním monitorováním zpracování osobních údajů SIS II;

5. zajistit, aby se činnosti úřadu pro ochranu osobních údajů v oblasti dohledu v rámci VIS týkaly také bezpečnostních aspektů včetně protokolů, a to prostřednictvím pravidelných kontrol na základě analýzy protokolových souborů, a aby úřad prováděl důkladné kontroly serverových místností a některých koncových uživatelů systému VIS, například policie;

6. zajistit, aby úřad pro ochranu osobních údajů dokončil druhý audit systému N.VIS, jakmile to situace spojená s COVID-19 umožní;

7. zajistit, aby úřad pro ochranu osobních údajů prováděl audit operací zpracování údajů v systému N.VIS alespoň jednou za čtyři roky;

Schengenský informační systém

8. zajistit, aby veškerá zařízení umožňující přístup k údajům SIS II používala dvoufaktorové ověřování;

9. zajistit, aby všechny dokumenty týkající se systémů řízení bezpečnosti informací zavedených pro obě datová centra podléhaly častější revizi a aby byly používané normy stále aktuální;

10. zajistit, aby byl bezpečnostní plán pro SIS II pravidelně revidován a v případě potřeby aktualizován a aby byla zavedena bezpečnostní opatření k zajištění trvalé odolnosti, spolu s důvěrností, integritou a přístupností. Toho lze dosáhnout zejména tak, že správce údajů přihlíží k technickému vývoji s cílem zajistit, že přijatá bezpečností opatření i nadále plní uvedené cíle;

11. objasnit, zda je clearingové středisko nedílnou součástí ministerstva vnitra nebo externím zpracovatelem údajů;

12. zajistit, aby při vyřizování případů zneužití totožnosti došlo ke zlepšením, pokud jde o informace poskytované subjektu údajů a používané formuláře souhlasu, a aby formuláře určené pro subjekt údajů obsahovaly informace o právech subjektů údajů, kontaktní údaje pověřence pro ochranu osobních údajů, právní základ pro zpracování údajů a informace o době, po kterou budou osobní údaje uchovávány;

Vízový informační systém

13. zajistit, aby protokoly veškerých operací zpracování údajů v systému VIS byly uchovávány na vnitrostátní úrovni v souladu s článkem 34 nařízení (ES) č. 767/2008 (nařízení o VIS), a to po dobu jednoho roku po uplynutí doby uchování uvedené v čl. 23 odst. 1 nařízení o VIS;

Povědomí veřejnosti a práva subjektů údajů

14. zajistit, aby ministerstvo vnitra na svých internetových stránkách poskytovalo informace také v jiných jazycích než v němčině, např. v angličtině, pokud jde o zpracování údajů SIS II a VIS a související práva subjektů údajů, a aby tyto informace o právech subjektů údajů v souvislosti s údaji SIS II a VIS byly na jeho stránkách snadněji přístupné;

15. zajistit, aby ministerstvo vnitra na svých internetových stránkách poskytovalo formuláře pro uplatnění práva na přístup, opravu a vymazání v němčině i v jiných jazycích, např. v angličtině;

16. vytvořit tištěné verze informačních brožur o SIS, které budou dostupné u orgánů veřejné správy;

17. zajistit, aby ministerstvo vnitra poskytovalo neoficiální překlad (např. do angličtiny) odpovědí určených subjektům údajů v zájmu posílení práv těchto subjektů;

18. zajistit, aby internetové stránky zemských policejních ředitelství poskytovaly informace o systémech SIS II a VIS, včetně informací o zpracování osobních údajů, a obsahovaly odkazy na internetové stránky úřadu pro ochranu osobních údajů;

19. zajistit, aby byly informace o zpracování osobních údajů v systému VIS snadno přístupné na internetových stránkách ministerstva pro evropské a mezinárodní záležitosti, konzulátů a velvyslanectví a aby tyto stránky obsahovaly odkazy na internetové stránky úřadu pro ochranu osobních údajů;

20. zajistit, aby úřad pro ochranu osobních údajů poskytoval na svých internetových stránkách (v němčině a angličtině) i ve formulářích žádostí subjektů údajů o přístup tytéž informace, pokud jde o povinnost subjektu údajů prokázat svou totožnost;

21. zajistit, aby úřad pro ochranu osobních údajů poskytoval na svých internetových stránkách (v němčině a angličtině) specifické standardní formuláře žádostí o opravu a vymazání v souvislosti s údaji SIS a VIS;

22. zajistit, aby úřad pro ochranu osobních údajů na svých internetových stránkách v angličtině uváděl informace o lhůtě pro podání stížnosti, jak je stanovena v čl. 24 odst. 4 zákona o ochraně údajů.

V Bruselu dne

Za Radu
předseda/předsedkyně