



Brusel 22. února 2022  
(OR. en)

6426/22

---

---

Interinstitucionální spis:  
2021/0392(NLE)

---

---

SCH-EVAL 21  
DATAPROTECT 42  
COMIX 87

### VÝSLEDEK JEDNÁNÍ

---

Odesílatel: Generální sekretariát Rady

Datum: 21. února 2022

Příjemce: Delegace

---

Č. předchozího  
dokumentu:

5893/22

---

Předmět: Prováděcí rozhodnutí Rady, kterým se stanoví doporučení týkající se řešení nedostatků zjištěných v roce 2019 při hodnocení toho, jak **Polsko** 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 2019 při hodnocení toho, jak Polsko uplatňuje schengenské *acquis* v oblasti ochrany údajů, které přijala Rada na zasedání konaném dne 21. února 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 2019 při hodnocení toho, jak Polsko 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<sup>1</sup>, a zejména na článek 15 uvedeného nařízení,

s ohledem na návrh Evropské komise,

vzhledem k těmto důvodům:

- (1) V souladu s nařízením (EU) č. 1053/2013 bylo v Polsku v roce 2019 provedeno hodnocení k ověření uplatňování schengenského *acquis* v oblasti ochrany osobních údajů. V návaznosti na hodnocení byla prováděcím rozhodnutím Komise C(2021) 9100 přijata zpráva, která zahrnuje zjištění a hodnocení a uvádí osvědčené postupy a nedostatky zjištěné během hodnocení.
- (2) S ohledem na výsledky hodnocení je namístě doporučit Polsku určitá nápravná opatření k řešení zjištěných nedostatků.

---

<sup>1</sup> Úř. věst. L 295, 6.11.2013, s. 27.

- (3) Jako osvědčené postupy jsou vnímány zejména: vnitrostátní právní rámec, který umožňuje předsedovi polského úřadu pro ochranu osobních údajů nezávisle jmenovat svého zástupce a členy poradního sboru; požadavek, aby uchazeči na pozici předsedy úřadu pro ochranu osobních údajů absolvovali veřejné slyšení v parlamentu, které je rovněž prostřednictvím oficiálního parlamentního kanálu vysíláno na internetu; časté kontroly externích poskytovatelů služeb, na nichž se podílí pověřenec pro ochranu osobních údajů, a časté kontroly konzulátů; závazek týkající se odborné přípravy a rozvoje pracovníků, a to i v oblasti ochrany údajů, v případě koncových uživatelů vnitrostátního schengenského informačního systému (N.SIS) a pracovníků centrály SIRENE; bezpečnostní opatření uplatňovaná v prostorách datových center poskytujících hosting systému N.SIS a vnitrostátního vízového informačního systému (N.VIS).
- (4) Vzhledem k důležitosti dodržování schengenského *acquis* v oblasti ochrany osobních údajů, pokud jde o vízový informační systém (VIS) a schengenský informační systém (SIS), by měla být přednostně provedena doporučení č. 11, 12, 13, 20, 21 a 22 uvedená v tomto rozhodnutí.
- (5) V souladu s nařízením (EU) č. 1053/2013 by toto rozhodnutí mělo být předloženo Evropskému parlamentu a vnitrostátním parlamentům členských států a Polsko by mělo do tří měsíců od jeho přijetí vypracovat akční plán s výčtem všech doporučení popisujících, jak napraví nedostatky zjištěné v hodnotící zprávě, a předložit jej Komisi a Radě,

DOPORUČUJE:

Polsko by mělo:

## **Právní předpisy**

1. výslovně objasnit, jak se 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, GDPR) použije v relevantních případech na zpracování osobních údajů v systémech N.VIS a N.SIS;

## **Úřad pro ochranu osobních údajů**

2. zajistit, aby článek 174 zákona o ochraně údajů z roku 2018 a článek 106 zákona o ochraně údajů z roku 2018, který stanoví maximální výši výdajů za určitý rok, nestanovily rozpočet polského úřadu pro ochranu osobních údajů na nižší úroveň, než jsou částky přidělené ve státním rozpočtu pro daný rok;
3. zajistit, aby úřad pro ochranu osobních údajů lépe plánoval a organizoval své četné kontroly systému N.SIS II tak, aby se vztahovaly na všechny operace zpracování údajů v systému N.SIS II a na všechny relevantní subjekty a aby tyto kontroly vyústily v komplexní audit N.SIS II, jak stanoví čl. 44 odst. 2 nařízení (ES) č. 1987/2006;
4. zajistit, aby úřad pro ochranu osobních údajů provedl komplexní inspekci systému N.VIS, a zcela tak splnil své úkoly v souladu s čl. 41 odst. 2 nařízení (ES) č. 767/2008;

## **Práva subjektů údajů**

5. zajistit, aby statistiky úřadu pro ochranu osobních údajů související s výkonem práv subjektů údajů doznaly zlepšení a aby rozlišovaly stížnosti od žádostí, dotčený systém (SIS nebo VIS), předmět a druh žádosti (oprava, smazání, přístup);
6. zajistit, aby správce údajů zaujímal proaktivnější přístup k poskytování informací o právech subjektů údajů v souvislosti s údaji VIS;

7. zajistit, aby správce údajů SIS a VIS (polská státní policie – ústřední technický orgán pro vnitrostátní informační systém) zveřejnil standardní formuláře pro žádosti o uplatnění práv subjektů údajů;

### **Vízový informační systém**

8. zajistit, aby záznamy o přístupu do systému VIS obsahovaly také informace o odůvodnění tohoto přístupu;
9. přezkoumat seznam orgánů s přístupem do VIS a jejich práva pro přístup k údajům VIS s ohledem na jejich pravomoci a využití takových údajů v praxi;
10. s ohledem na velký počet správců údajů VIS ustanovených vnitrostátními předpisy a smluvními ustanoveními a na značný počet zapojených subjektů vyjasnit vztah mezi orgány zapojenými do postupu vydávání víz a orgány provádějícími zpracování údajů VIS, jakož i odpovědnost těchto orgánů za zpracování údajů;
11. zajistit, aby protokolové soubory VIS byly pravidelně analyzovány pro účely monitorování ochrany údajů v zájmu plného využívání uchovávaných protokolových souborů;
12. přijmout bezpečnostní plán pro VIS pokrývající fyzickou bezpečnost druhého střediska pro zpracování údajů i další bezpečnostní aspekty vnitrostátního informačního systému včetně systému N.VIS;
13. uvést do souladu dobu uchovávání protokolů u žádostí týkajících se VIS (zejména žádostí „Pobyt“ a „ZSE 6“) se lhůtami podle čl. 34 odst. 2 nařízení (ES) č. 767/2008 a článku 16 rozhodnutí Rady 2008/633/SVV;

### **Schengenský Informační Systém II**

14. zajistit, aby správce údajů N.SIS II zavedl ústřední systém správy uživatelů umožňující účinnou vlastní kontrolu bez potřeby konzultovat protokoly u institucí, které jsou koncovými uživateli systému N.SIS II;

15. zajistit, aby protokolové soubory SIS byly pravidelně analyzovány pro účely monitorování ochrany údajů v zájmu plného využívání uchovávaných protokolových souborů;
16. zajistit automatizované oznamování událostí v oblasti bezpečnosti IT a činností vlastní kontroly ze strany správce údajů v zájmu dalšího zlepšení bezpečnosti;
17. zajistit, aby technická opatření zahrnovala také znemožnění používání zařízení nebo klíčů USB pomocí blokace veškerých portů USB u pracovních stanic SIS;
18. zvážit možnost proaktivního a pravidelného zapojení pověřence pro ochranu osobních údajů působícího v rámci ministerstva vnitra do kontroly zpracování údajů SIS a VIS prostřednictvím kontroly protokolů auditu;
19. zajistit, aby správce údajů SIS poskytoval úřadu pro ochranu osobních údajů profily pracovníků všech orgánů s přístupem do systému SIS;
20. uvést do souladu dobu uchovávání protokolů u žádostí o přístup k údajům SIS s požadavky čl. 12 odst. 4 nařízení (ES) č. 1987/2006 a čl. 12 odst. 4 rozhodnutí Rady 2007/533/SVV;
21. zajistit, aby správce údajů SIS přijal v souladu s článkem 10 nařízení (ES) č. 1987/2006 a článkem 10 rozhodnutí Rady 2007/533/SVV bezpečnostní plán pro SIS;
22. zajistit, aby bylo opětovně posouzeno široké spektrum institucí s přístupem k údajům SIS II s cílem ujistit se, že k údajům mohou mít přístup pouze instituce, které jej potřebují s ohledem na své pravomoci a praktické potřeby;

## **Povědomí veřejnosti**

23. zajistit, aby internetové stránky úřadu pro ochranu osobních údajů a policie poskytovaly informace o právech subjektů údajů v případě údajů VIS.

V Bruselu dne

*Za Radu*

*předseda / předsedkyně*

---