

Brusel 14. května 2025
(OR. en)

8833/25

Interinstitucionální spis:
2024/0126(NLE)

SCH-EVAL 29
DATAPROTECT 88
COMIX 140
NO
CH
IS
LI

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Příjemce:	Delegace
Č. předchozího dokumentu:	8093/25
Předmět:	Prováděcí rozhodnutí Rady, kterým se stanoví doporučení týkající se řešení nedostatků zjištěných v roce 2021 při hodnocení toho, jak Itálie uplatňuje schengenské <i>acquis</i> v oblasti ochrany údajů

Delegace naleznou v příloze prováděcí rozhodnutí Rady, kterým se stanoví doporučení k řešení nedostatků zjištěných v roce 2021 při hodnocení toho, jak Itálie uplatňuje schengenské *acquis* v oblasti ochrany údajů, které Rada přijala na zasedání konaném dne 12. května 2025.

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 2021 při hodnocení toho, jak Itálie 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 Schengenu¹, a zejména na čl. 15 odst. 3 uvedeného nařízení,

s ohledem na návrh Evropské komise,

vzhledem k těmto důvodům:

- (1) V září 2021 bylo u Itálie provedeno schengenské hodnocení v oblasti ochrany osobních údajů. V návaznosti na hodnocení byla dne 30. května 2024 prováděcím rozhodnutím Komise C(2024) 1910 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) Za osvědčené se považují zejména tyto postupy: rozsáhlá bezpečnostní opatření týkající se fyzické bezpečnosti serveru vnitrostátního Schengenského informačního systému (N.SIS); komplexní odborná příprava poskytovaná zaměstnancům a koncovým uživatelům N.SIS a centrály SIRENE, zejména pokud jde o odbornou přípravu a úsilí o zvyšování povědomí ze strany úřadu pověřence pro ochranu osobních údajů; značné úsilí úřadu pověřence pro ochranu osobních údajů o posílení ochrany údajů a zabezpečení údajů, a to i v případě N.SIS; pravidelné kontroly prováděné Ministerstvem zahraničních věcí a mezinárodní spolupráce na velvyslanectvích a konzulátech, jakož i kontroly u externích poskytovatelů služeb prováděné velvyslanectvími a konzuláty na základě pokynů Ministerstva zahraničních věcí a mezinárodní spolupráce; vývěsky na letišti a na policejní stanici, které poskytují snadný přístup k informacím o SIS v několika jazycích prostřednictvím kódů QR; užitečné a přístupné informace o právech subjektů údajů ve vztahu k Schengenském informačním systému (SIS) uvedené na internetových stránkách *Polizia di Stato* a úřadu pro ochranu osobních údajů; skutečnost, že internetové stránky Ministerstva vnitra obsahují odkazy na domovskou stránku *Polizia di Stato*, která subjektům údajů poskytuje snadný a rychlý způsob výkonu jejich práv; skutečnost, že *Polizia di Stato* informuje subjekty údajů, pokud jejich údaje nejsou uvedeny v SIS; užitečné a přístupné informace o právech subjektů údajů ve vztahu k Vízovému informačním systému (VIS) uvedené na internetových stránkách úřadu pro ochranu osobních údajů.
- (3) Měla by být učiněna doporučení ohledně nápravných opatření, která má Itálie přijmout k řešení nedostatků zjištěných v rámci hodnocení. Vzhledem k tomu, že je důležité dodržovat schengenské *acquis* v oblasti ochrany osobních údajů, a zejména pokud jde o dohled ze strany úřadu pro ochranu osobních údajů a odbornou přípravu v oblasti SIS a VIS, měla by být přednostně provedena doporučení 4 a 6 stanovená v tomto rozhodnutí.
- (4) V souladu s čl. 15 odst. 3 nařízení (EU) č. 1053/2013 by Rada měla toto rozhodnutí předložit Evropskému parlamentu a vnitrostátním parlamentům členských států.
- (5) Ode dne 1. října 2022 se používá nařízení Rady (EU) 2022/922². V souladu s čl. 31 odst. 3 uvedeného nařízení by činnosti navazující na hodnotící zprávy a doporučení a sledování těchto hodnotících zpráv a doporučení, počínaje předložením akčních plánů, měly být prováděny v souladu s uvedeným nařízením.
- (6) Do dvou měsíců od přijetí tohoto rozhodnutí by měla Itálie podle čl. 21 odst. 1 nařízení (EU) 2022/922 vypracovat akční plán pro provedení všech doporučení a nápravu nedostatků zjištěných v hodnotící zprávě. Itálie by měla tento akční plán předložit Komisi a Radě,

² Nařízení Rady (EU) 2022/922 ze dne 9. června 2022 o vytvoření a fungování hodnotícího a monitorovacího mechanismu k ověření uplatňování schengenského *acquis* a o zrušení nařízení (EU) č. 1053/2013 (Úř. věst. L 160, 15.6.2022, s. 1).

DOPORUČUJE,

že by Itálie měla, pokud jde o:

Úřad pro ochranu osobních údajů

1. zajistit, aby byl úřad pro ochranu osobních údajů formálně zapojen do rozpočtového procesu, zejména aby měl formální vliv na návrh svého rozpočtu předtím, než je návrh souhrnného rozpočtu předložen parlamentu k projednání a přijetí;
2. zajistit, aby byl úřadu pro ochranu osobních údajů přidělen dostatečný počet zaměstnanců k výkonu včasného a účinného dohledu nad SIS a VIS;
3. provádět pravidelnou kontrolu u některých orgánů, které jsou koncovými uživateli SIS, jako jsou operativní policejní orgány, včetně pravidelných kontrol a analýz souborů protokolů, aby mohl úřad pro ochranu osobních údajů plnit své úkoly související s komplexním monitorováním zpracování osobních údajů v rámci SIS;
4. dokončit probíhající audit operací zpracování údajů v N.SIS, jakmile to situace způsobená pandemií COVID-19 dovolí, a zajistit, aby byly následující audity prováděny ve stanoveném čtyřletém cyklu;
5. zajistit také pravidelnou kontrolu u většího počtu orgánů, které jsou koncovými uživateli VIS, jako je policie, pohraniční stráž a imigrační orgány, aby mohl úřad pro ochranu osobních údajů plnit své úkoly související s komplexním monitorováním zpracování osobních údajů v rámci VIS;
6. zajistit, aby byly audity národního vízového informačního systému prováděny ve stanoveném čtyřletém cyklu;
7. zajistit, aby audity VIS kromě auditních opatření Ministerstva zahraničních věcí a mezinárodní spolupráce zahrnovaly i opatření Ministerstva vnitra coby dalšího správce VIS;

Schengenský informační systém

8. zajistit, aby bylo zprovozněno zvláštní centrum pro obnovu po selhání systému v Bari;
9. zajistit, aby záložní kopie souborů protokolů N.SIS byly uchovávány mimo centrum na místě s jinou zeměpisnou polohou než v Římě, a to nejen systematicky, ale i v příslušně krátkém časovém úseku pro pořízení kopie;

10. zajistit, aby operační systémy na některých pracovištích, jako je centrála SIRENE, a na místní policejní stanici *Commissariato Trevi-Campo Marzio* byly co nejdříve aktualizovány;
11. zajistit, aby pro monitorování souborů protokolů SIS byly přijaty pokyny s kritérii platnými pro všechny pracovníky provádějící monitoring a aby byl zaveden softwarový modul pro analýzu souborů protokolů SIS s automatickým výstražným systémem pro případy neobvyklého vyhledávání za účelem zjištění případného zneužití;
12. zajistit vyšší bezpečnostní standard, pokud jde o přístup do databází, jako je aplikace SIS, zavedením dvoufaktorového autentizačního systému;
13. zajistit, aby úřad pro ochranu osobních údajů a Ministerstvo vnitra vypracovaly obecnou shodu nebo protokol týkající se kritérií nebo prahových hodnot pro oznamování případů porušení zabezpečení osobních údajů v N.SIS úřadu pro ochranu osobních údajů;
14. přehodnotit a zavést pravidla skupinové politiky pro automatické uzamčení počítačových systémů v případě nečinnosti na všech pracovištích s přístupem k SIS;
15. zavést bezpečnostní politiku a politiku ochrany údajů a sledovat praxi týkající se uchovávání osobních údajů o registraci ubytování v policejní databázi s cílem zajistit, aby poté, co jsou všechny osobní údaje uchovávány pro nezbytné kontroly v počátečním období, pravidelný přezkum zaručil, že osobní údaje zůstanou v rámci maximální doby uchovávání údajů v policejní databázi uchovány pouze po dobu, která je nezbytná a přiměřená pro účely sledované článkem 45 Schengenské úmluvy³;

Vízový informační systém

16. stanovit přiměřený limit pro neúspěšné pokusy o přihlášení s ohledem na chyby typu překlep, zapomenuté heslo atd., po jehož překročení by měl být uživatel systémem při přístupu do národního vízového informačního systému (N-VIS) zablokován;
17. zavést dodatečná opatření k monitorování povolení přístupu do N-VIS (kromě toho, že povolení přístupu uživatelů N-VIS jsou přísně a pravidelně revidována subjektem, ke kterému tito uživatelé přísluší) s cílem zajistit účinnost a účelnost revize, například automatické pozastavení povolení přístupu po dlouhé a atypické době bez jakékoli činnosti v systému VIS;
18. zajistit vyšší stupeň zabezpečení tak, že se při přikládání identifikační karty u dvou čtecích zařízení RFID instalovaných u vstupu do prostor datového centra Ministerstva zahraničních věcí a mezinárodní spolupráce a v serverové místnosti Visa zároveň vloží osobní kód PIN;

³ Úmluva k provedení Schengenské dohody ze dne 14. června 1985 mezi vládami států Hospodářské unie Beneluxu, Spolkové republiky Německo a Francouzské republiky o postupném odstraňování kontrol na společných hranicích (Úř. věst. L 239, 22.9.2000, s. 19).

19. uplatňovat na zařízení uložená v uzamčených skříňkách stejné postupy, které již byly přijaty u ostatních zařízení v serverové místnosti N.VIS;
20. zavést náležitý bezpečnostní systém schopný poskytovat ověření přístupu do místnosti a audit akcí a dovybavit serverové místnosti se záložním systémem VIS stejným hasicím systémem pro elektrická zařízení, jako je systém instalovaný v serverové místnosti VIS;
21. zavést infrastrukturu pro obnovu po selhání systému na místě s jinou zeměpisnou polohou než v *Palazzo della Farnesina*;
22. přezkoumat procesy zálohování uplatňované na velvyslanectvích a konzulátech, vyhýbat se používání flash disků, nebo při jejich používání uchovávané informace šifrovat;
23. zavést automatickou kontrolu protokolů u protokolů I-VIS;
24. doplnit modul ochrany osobních údajů do interního školení, jež je poskytováno zaměstnancům, kteří se zabývají vyřizováním víz, před jejich vysláním;
25. zajistit, aby Ministerstvo zahraničních věcí a mezinárodní spolupráce posoudilo kritická místa místních seznamů varování, na která upozornil úřad pro ochranu osobních údajů, a to nejen na vnitrostátní úrovni, ale také prostřednictvím spolupráce s ostatními dotčenými konzuláty, a včas informovalo úřad pro ochranu osobních údajů o opatřeních, která mohou být přijata s cílem zajistit plný soulad s požadavky na ochranu osobních údajů;
26. posílit úřad pověřence pro ochranu osobních údajů při Ministerstvu zahraničních věcí a mezinárodní spolupráce;

Informovanost veřejnosti a práva subjektů údajů

27. zajistit, aby informace o SIS na internetových stránkách Ministerstva vnitra byly srozumitelné i osobám, které nemluví italsky;
28. zajistit, aby byly na internetových stránkách úřadu pro ochranu osobních údajů uvedeny vzorové dopisy týkající se SIS a aby bylo na příslušných internetových stránkách zviditelněno tlačítko „Nový mechanismus pro výkon práv na ochranu údajů“;
29. změnit standardní odpověď, že „subjekt údajů nemá zákaz vstupu na schengenské území“ (č. 6), která je považována za zavádějící v případech, kdy subjektu údajů nejsou poskytnuty žádné informace o záznamu, například z důvodu ohrožení veřejné nebo národní bezpečnosti;

30. zajistit, aby internetové stránky Ministerstva zahraničních věcí a mezinárodní spolupráce a Ministerstva vnitra obsahovaly zvláštní šablonu pro žádost o přístup k osobním údajům ve VIS v souvislosti s osobními údaji zpracovávány v rámci VIS;
31. zvážit poskytování informací o VIS a právech subjektů údajů v souvislosti se zpracováním osobních údajů v rámci VIS na hraničních přechodech, jako jsou letiště, stejným způsobem, jako je tomu již v případě SIS, například prostřednictvím vývěsek, kódů QR s odkazem na více informací atd.

V Bruselu dne

*Za Radu
předseda/předsedkyně*
