EVROPSKÁ
KOMISE

V Bruselu dne 11.12.2025
COM(2025) 752 final

ZPRÁVA KOMISE EVROPSKÉMU PARLAMENTU A RADĚ,

o vyhodnocení a posouzení provozního dopadu provádění úkolů stanovených v nařízení (EU) 2022/991, zejména v čl. 4 odst. 1 písm. t), čl. 18 odst. 2 písm. e), čl. 18 odst. 6a a článcích 18a, 26, 26a a 26b, pokud jde o cíle Europolu, jakož i dopadu těchto úkolů na základní práva a svobody stanovené v Listině, v souladu čl. 68 odst. 3 nařízení (EU) 2016/794

{SWD(2025) 404 final}

1. Rozsah hodnocení

Od zahájení své činnosti v roce 1999 hraje **Agentura Evropské unie pro spolupráci v oblasti prosazování práva (Europol) ústřední roli v boji proti závažné přeshraniční trestné činnosti a terorismu** a stala se klíčovou hnací silou spolupráce v oblasti prosazování práva v Evropě. Bezpečnostní prostředí prošlo za posledních 30 let drastickými změnami, kterým odpovídala i změna DNA závažné a organizované trestné činnosti[1]. Členské státy mají nové operační potřeby, pokud jde o účinné řešení vznikajících hrozeb, a jejich **očekávání ohledně podpory ze strany Europolu** se rovněž **vyvíjejí**. Mandát Europolu byl proto několikrát nahrazen nebo pozměněn, aby se zachoval a zvýšil význam této agentury.

Mandát Europolu, jak je stanoven v nařízení (EU) 2016/794[2] (dále jen „nařízení o Europolu“), byl naposledy změněn v roce 2022 nařízením (EU) 2022/991[3] s cílem řešit nové bezpečnostní hrozby. Nařízení o Europolu již nesplňovalo svůj účel v nové realitě, v níž pachatelé trestné činnosti využívají výhod **digitální transformace**, **nových technologií**, **globalizace** a **mobility**[4].

Specifickými cíli nařízení (EU) 2022/991[5] bylo:

- umožnit účinnou spolupráci mezi **soukromými subjekty** a orgány pro vymáhání práva v boji proti zneužívání přeshraničních služeb pachateli trestné činnosti,
- umožnit orgánům pro vymáhání práva analyzovat **rozsáhlé a složité soubory údajů** za účelem odhalení přeshraničních souvislostí, a to v plném souladu se **základními právy**,
- umožnit členským státům využívat **nové technologie** k prosazování práva.

Nařízením (EU) 2022/991 byla navíc změněna pravidla pro ochranu údajů platná pro Europol s cílem zachovat **vysokou úroveň ochrany údajů** a dosáhnout rovnováhy mezi novými pravomocemi agentury zpracovávat osobní údaje a ochranou soukromí a osobních údajů jednotlivců. **S cílem usnadnit tok informací** byla do značné míry sjednocena pravidla ochrany údajů platná pro Europol s pravidly platnými pro ostatní agentury a orgány EU v oblasti spravedlnosti a vnitřních věcí (SVV) podle kapitoly IX nařízení (EU) 2018/1875 (dále jen „nařízení EU o ochraně údajů“) a s pravidly platnými pro orgány členských států pro vymáhání práva (dále jen „příslušné orgány“) podle jejich vnitrostátních právních předpisů, kterými byla provedena směrnice (EU) 2016/680 (dále jen „směrnice o prosazování práva“)[6].

Tato zpráva byla přijata v souladu s povinností Komise podle **čl. 68 odst. 3 nařízení o Europolu**, kterou je vyhodnotit[7] a posoudit provozní dopad úkolů Europolu stanovených v nařízení (EU) 2022/991 tři roky po jeho vstupu v platnost. V souladu s pověřením spolunormotvůrců Komise: zaprvé vyhodnotila a posoudila **provozní dopad** některých nových

---

1 Europol, 2025 EU Serious and Organised Crime Threat Assessment (SOCTA) – The changing DNA of serious and organized crime („Posouzení hrozeb závažné a organizované trestné činnosti v EU z roku 2025 – Měnící se DNA závažné a organizované trestné činnosti“), k dispozici online na adrese https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf (dále jen „EU SOCTA 2025“). Viz také posouzení hrozeb v celní oblasti (CTA) za rok 2025, které je k dispozici online na adrese https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

2 Úř. věst. L 135, 24.5.2016, s. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj.

3 Úř. věst. L 169, 27.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/991/oj.

4 SWD(2020) 543 final ze dne 9. prosince 2020, s. 37, https://eur-lex.europa.eu/resource.html?uri=cellar:1a4d9f40-3b02-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

5 *Tamtéž.*

6 Úř. věst. L 119, 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

7 Toto hodnocení provedené v souladu s čl. 68 odst. 3 nařízení o Europolu není hodnocením, které má být provedeno podle pokynů pro zlepšování právní úpravy s ohledem na případný návrh revize nařízení o Europolu. Viz rovněž oddíl 4 níže.

pravidel pro zpracování osobních údajů ve vztahu k cílům Europolu podle článku 3 nařízení o Europolu (konkrétně: podpora a posílení činností příslušných orgánů členských států a jejich vzájemná spolupráce při předcházení trestným činům spadajícím pod mandát Europolu a při boji proti nim); zadruhé posoudila dopad těchto pravidel na **základní práva a svobody** (dále jen „základní práva“) zakotvené v Listině[8] a zatřetí provedla **analýzu nákladů a přínosů** souvisejících úkolů zpracování údajů.

Při přípravě přezkumu shromáždily útvary Komise informace a zpětnou vazbu z různých zdrojů a vedly ad hoc konzultace s Europolem a členskými státy. Doprovodný **pracovní dokument útvarů** Komise obsahuje podrobný popis obecného kontextu a metodiky přezkumu, jakož i komplexní popis zdrojů důkazů a konzultací, které potvrzují hlavní zjištění shrnutá v této zprávě.

2. Obecné souvislosti

V souladu s čl. 68 odst. 3 nařízení o Europolu se tato zpráva Komise zabývá vybranými ustanoveními nařízení (EU) 2022/991 a zaměřuje se na pět klíčových aspektů činnosti Europolu.

(1) Vnější rozměr: ustanovení čl. 4 odst. 1 písm. t) nařízení o Europolu o informačních záznamech v Schengenském informačním systému (SIS) o státních příslušnících třetích zemí na návrh Europolu

Vzhledem ke **globální povaze závažné trestné činnosti a terorismu** mají informace o pachatelích a osobách podezřelých z těchto trestných činů, které mají k dispozici třetí země a mezinárodní organizace, stále větší význam pro vnitřní bezpečnost EU. Vnější rozměr spolupráce EU v oblasti prosazování práva se proto stal pro členské státy klíčovým, stejně jako **úloha Europolu při podpoře členských států v jejich partnerství se třetími zeměmi** nebo subjekty, které se v těchto zemích nacházejí. V zájmu posílení globální bezpečnosti bude **v budoucnu nezbytné** vyvinout další úsilí[9].

Nařízení (EU) 2022/991 již zavedlo podstatné změny nařízení o Europolu s cílem posílit **vnější rozměr činnosti Europolu**, zejména usnadnit výměnu informací se třetími zeměmi[10] a požadovat, aby Europol do svých víceletých programů a ročních pracovních programů zahrnul strategii pro vztahy se třetími zeměmi a mezinárodními organizacemi[11].

Ustanovení čl. 4 odst. 1 písm. t) nařízení o Europolu pověřilo Europol novým úkolem: podporovat členské státy při zpracovávání údajů o osobách zapojených do terorismu nebo závažné trestné činnosti, které poskytly třetí země nebo mezinárodní organizace. To zahrnuje **návrh členským státům na možné vkládání informačních záznamů o státních příslušnících třetích zemí v zájmu Unie do Schengenského informačního systému (SIS)**. Tato nová kategorie informačních záznamů byla zavedena v roce 2022[12], a to na základě změny

---

8 Listina základních práv Evropské unie (Úř. věst. C 326, 26.10.2012, s. 391, ELI: http://data.europa.eu/eli/treaty/char_2012/oj.

9 Viz ProtectEU: Evropská strategie vnitřní bezpečnosti, COM(2025) 148 final ze dne 1. dubna 2025, https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52025DC0148.

10 Viz například čl. 25 odst. 4a nařízení o Europolu, který Europolu umožňuje předávat údaje třetím zemím na základě vlastního posouzení všech okolností daného předání osobních údajů, pokud dospěl k závěru, že ve vztahu k ochraně osobních údajů existují vhodné záruky, a čl. 25 odst. 5 nařízení o Europolu, který rozšiřuje rozsah výjimečných případů, kdy Europol může ad hoc předávat v řádně odůvodněných případech údaje nebo kategorie údajů třetím zemím a mezinárodním organizacím.

11 Ustanovení čl. 12 odst. 2 nařízení o Europolu.

12 Nařízení (EU) 2022/1190, Úř. věst. L 185, 12.7.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj

nařízení (EU) 2018/1862 o využívání SIS v oblasti policejní a justiční spolupráce v trestních věcech[13].

Některé informace, zejména pokud dotyčná osoba není občanem EU a nemá žádnou souvislost s vnitrostátním případem, sdílí třetí země informace pouze s Europolem, který údaje zpracovává a výsledky analýzy sdílí se všemi členskými státy. Cílem nových ustanovení bylo **maximalizovat využití informací**, které Europol získává od třetích zemí, tím, že budou přístupnější, než kdyby byly dostupné pouze prostřednictvím vlastního systému Europolu. Byla tak doplněna další opatření, jako je Evropský vyhledávací portál (ESP) a rámec interoperability[14] mezi informačními systémy EU pro řízení bezpečnosti, správu hranic a řízení migrace, s cílem řešit strukturální nedostatky související s těmito systémy, které brání práci vnitrostátních orgánů a zejména pohraniční stráže.

Systém SIS je považován za **další klíčový kanál pro šíření informací**. Je nejpoužívanější databází v Evropě pro vymáhání práva, ochranu hranic a migraci. V roce 2024 bylo v SIS provedeno více než 15 miliard vyhledávání ve srovnání s přibližně 14 miliony vyhledávání v informačním systému Europolu a méně než 3 miliardami vyhledávání (celosvětově) v 19 databázích Interpolu, což jsou dva další hlavní informační systémy pro příslušné orgány[15].

(2) Inovace: ustanovení čl. 18 odst. 2 písm. e) a článek 33a nařízení o Europolu o zpracování osobních údajů Europolem pro inovační a výzkumné projekty

Technologický vývoj představuje pro vnitřní bezpečnost EU jak obrovské příležitosti, tak i značné výzvy[16], a má tak zásadní dopad na kriminalitu, že mění i hlubokou podstatu, „DNA“, hrozeb závažné a organizované trestné činnosti[17]. Pachatelé trestné činnosti do svých operací rychle začleňují nové technologie, vytvářejí nové obchodní modely a zdokonalují své taktiky. Zároveň tento pokrok nabízí **nebývalé možnosti pro posílení kapacit orgánů pro vymáhání práva**. Výzkum a inovace proto hrají zásadní roli v oblasti vnitřní bezpečnosti, neboť vyvíjejí řešení k tomu, abychom mohli bojovat proti novým hrozbám a držet krok s rychle se vyvíjejícími formami a způsoby fungování zločineckých sítí, včetně těch, které vyplývají ze zneužívání technologií. Unie investovala a bude i nadále investovat do vývoje inovativních nástrojů prostřednictvím výzkumu a inovací v oblasti bezpečnosti financovaných EU v rámci Evropské strategie vnitřní bezpečnosti, **ProtectEU**[18].

Inovační laboratoř Europolu[19], založená koncem roku 2019 na základě pověření ministrů spravedlnosti a vnitřních věcí členských států EU, má za cíl podpořit závazek Europolu týkající se inovací v oblasti prosazování práva. Nařízení (EU) 2022/991 zavedlo podstatné změny nařízení o Europolu s cílem posílit mandát Europolu v oblasti inovací a podpořit potenciál inovační laboratoře Europolu a součinnost s dalšími výzkumnými a inovačními činnostmi na úrovni EU, včetně zejména Komise, v rámci **inovačního centra EU** pro vnitřní bezpečnost[20].

---

13 Nařízení (EU) 2018/1862, Úř. věst. L 312, 7.12.2018, s. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj

14 Nařízení (EU) 2019/818, Úř. věst. L 135, 22.5.2019, s. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj

15 Výroční zpráva agentury eu-LISA o SIS z roku 2024, která je k dispozici online na stránce https://www.eulisa.europa.eu/sites/default/ files/documents/sis-annual-report-2024.pdf, Europol, souhrnná výroční zpráva o činnosti z roku 2024, dostupná online na stránce https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF a https://www.interpol.int/How-we-work/Databases.

16 Europol, posouzení hrozeb organizované trestné činnosti na internetu (IOCTA) z roku 2024, k dispozici online na stránce Posouzení hrozeb organizované trestné činnosti na internetu (IOCTA) 2024 | Europol.

17 Europol, EU SOCTA 2025, s. 19.

18 COM(2025) 148 final ze dne 1. dubna 2025, https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52025DC0148, s. 9.

19 https://www.europol.europa.eu/how-we-work/innovation-lab.

20 Viz zejména čl. 4 odst. 1 písm. v) a w) nařízení o Europolu.

Ustanovení čl. 18 odst. 2 nařízení o Europolu o účelech zpracování informací bylo změněno tak, aby Europol mohl **zpracovávat operativní osobní údaje** také **pro výzkumné a inovační projekty**. Dostupnost vysoce kvalitních souborů dat, které umožňují empirické testování platnosti nových nástrojů, je obecně považována za klíčový předpoklad pro vývoj technologií. Naopak nespolehlivé nebo neobjektivní soubory dat pro testování mohou vést k vývoji špatných technologií.[21]

Přizpůsobené záruky ochrany údajů pro takové zpracování byly stanoveny v čl. 18 odst. 3a, čl. 30 odst. 2 a 3 a článku **33a nařízení o Europolu**. Poslední z uvedených článků vyžadoval zřídit **prostředí „pískoviště"** tím, že stanovil, že veškeré osobní údaje zpracovávané v souvislosti s projektem musí být dočasně zkopírovány do samostatného, izolovaného a chráněného prostředí pro zpracování údajů v rámci Europolu, které bude použito výhradně pro tento projekt.

(3) <u>Trestní vyšetřování</u>: ustanovení čl. 18 odst. 6a a článku 18a nařízení o Europolu o podmínkách zpracování osobních údajů získaných bez kategorizace subjektů údajů

Europol jako **centrála EU pro informace o trestné činnosti** nejen usnadňuje shromažďování a výměnu informací, ale také pomáhá **zvyšovat účinnost vyšetřování prostřednictvím pokročilé analýzy údajů** a odhalováním přeshraničních vazeb mezi trestnými činy a zločineckými sítěmi, které nejsou na vnitrostátní úrovni viditelné. Tyto schopnosti podporují členské státy tím, že obohacují informace dostupné pro jejich vyšetřování trestných činů.

Díky rozsáhlému a intenzivnímu používání technologií **se rozsáhlé a složité soubory údajů staly novou normou ve všech oblastech života**, včetně trestné činnosti.[22] Vyšetřování organizovaného zločinu nebo terorismu se začalo potýkat s výzvou analyzovat velké objemy elektronicky uložených dat, které často dosahují terabytů, včetně zvukových a obrazových záznamů a strojově generovaných dat zabavených během vyšetřování. Například při společném vyšetřování, jehož cílem bylo rozbít síť EncroChat[23], vyšetřovatelé analyzovali miliony zpráv, které si zločinci vyměňovali při plánování závažných trestných činů. V této souvislosti je pro donucovací a justiční orgány klíčová dostupnost nezbytných nástrojů informačních a komunikačních technologií (IKT), odborných znalostí a zdrojů pro analýzu rozsáhlých a složitých souborů údajů (v odborném žargonu označovaných jako „data velkého objemu"[24]).

Nařízení o Europolu přijaté v roce 2016 sice samo o sobě neukládá omezení na analýzu dat velkého objemu, ale chybí v něm strukturovaná ustanovení, která by stanovila podmínky pro analýzu tohoto typu dat. **Nejkritičtějším bodem** byl **požadavek na kategorizaci subjektů údajů**. Kategorizace subjektů údajů odkazuje na potřebu prověřit soubory údajů a roztřídit osobní údaje podle různých kategorií, které jsou taxativně uvedeny v příloze II.A a II.B nařízení o Europolu, předtím, než se přistoupí k vlastnímu zpracování údajů pro účely vyšetřování, a to také před křížovou kontrolou údajů za účelem zjištění souvislostí nebo provádění analýz

---

21 SWD(2020) 543 final ze dne 9. prosince 2020, s. 29.

22 Europol, EU SOCTA 2025, *passim*.

23 https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochatcommunications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized.

24 Evropský inspektor ochrany údajů, stanovisko č. 7/2015, s. 7, k dispozici na adrese https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf. „Obecně platí, že jako společný jmenovatel různých dostupných definic se „**daty velkého objemu**" rozumí praxe kombinování obrovských objemů informací z různých zdrojů a jejich analýza s využitím sofistikovanějších algoritmů pro rozhodování. Data velkého objemu se opírají nejen o rostoucí schopnost technologie podporovat shromažďování a ukládání velkého množství dat, ale také o její schopnost analyzovat, pochopit a využít plnou hodnotu dat (zejména pomocí analytických aplikací)."

strategické či tematické povahy nebo operativních analýz[25]. Příslušné kategorie jsou spojeny s různými typy zapojení do vyšetřování trestných činů, včetně i) podezřelých osob, potenciálních budoucích pachatelů a také ii) kontaktů, společníků, obětí, svědků a informátorů spojených s trestnou činností. Obecně platí, že Europol nemůže zpracovávat ani uchovávat osobní údaje osob, které nespadají do žádné z těchto kategorií.

Poskytovatelé údajů, jako jsou **členské státy** nebo **orgány a agentury EU**, **obvykle** provádějí kategorizaci subjektů údajů již před předáním osobních údajů Europolu[26]. Podle právních předpisů EU jsou povinni provádět kategorizaci subjektů údajů pro své vlastní zpracování a vyšetřování, bez ohledu na předávání údajů Europolu, a to na základě rovnocenných, nikoli však totožných pravidel, jako jsou pravidla Europolu[27]. U rozsáhlých a složitých souborů údajů je však ruční předběžné zpracování náročné na zdroje a čas. Analýza dat z jednoho mobilního telefonu poloautomatizovaným způsobem může trvat až tři dny a během vyšetřování mohou být zabaveny i stovky mobilních telefonů. Kategorizace subjektů údajů u **dat velkého objemu není vždy možná** vzhledem k obrovskému objemu datových souborů, způsobu, jakým jsou data (ne)strukturována, nedostatku zdrojů nebo nadměrnému **potřebnému manuálnímu úsilí**. V praxi je jedinou možností nejprve hlouběji analyzovat data z operačního hlediska nebo zjistit souvislosti, a to i poloautomatizovaným způsobem, křížovou kontrolou dostupných údajů.

Nařízení (EU) 2022/991 vyjasnilo podmínky pro kategorizaci subjektů údajů s cílem zajistit **právní jistotu** ohledně zpracování rozsáhlých a složitých souborů údajů. Europol a evropský inspektor ochrany údajů (EIOÚ) si rozdílně vykládali literu a ducha nařízení o Europolu, pokud jde o použitelnou dobu pro uchovávání údajů. Podle Europolu by tato doba měla být tři roky a podle evropského inspektora ochrany údajů by to mělo být šest měsíců[28]. Nová ustanovení byla rovněž nutná k zajištění **větší flexibility** a dosažení správné rovnováhy mezi ochranou údajů a bezpečnostními aspekty.

Ustanovení čl. 18 odst. 5a nařízení o Europolu ve spojení s článkem 73 nařízení EU o ochraně údajů nejprve dále objasnilo obecnou zásadu kategorizace subjektů údajů podle čl. 18 odst. 2 a přílohy II. Úkolem Europolu je v příslušných případech a v co nejvyšší možné míře **jednoznačně přiřazovat osobní údaje ke konkrétní kategorii subjektů údajů**. V praxi by měl Europol zpravidla určovat přesnou roli v trestné činnosti (například zda je osoba podezřelá, oběť nebo pouze svědek) pro každou osobu, jejíž osobní údaje budou zpracovávány, a nikoliv na souhrnné úrovni pro všechny osoby v souboru údajů, který má být zpracováván, nebo jeho části (například prostým stanovením, že všechny uvedené osoby jsou zapojeny do trestné činnosti spadající do jeho mandátu na základě posouzení obecných okolností, které vedly ke vzniku souboru údajů) předtím, než mohou být osobní údaje zpracovány.

Ustanovení čl. 18 odst. 6a nařízení o Europolu výslovně povoluje zpracování osobních údajů získaných bez kategorizace subjektů údajů po dobu **až 18 měsíců**, kterou lze v odůvodněných případech prodloužit až na 36 měsíců, a to výhradně za **účelem dokončení kategorizace subjektů údajů**. Ustanovení čl. 18 odst. 6a nařízení o Europolu se výslovně nevztahuje na rozsáhlé a složité soubory údajů, ale obecněji vyžaduje test „**striktně nezbytné povahy**“.

---

25 Viz čl. 18 odst. 2 nařízení o Europolu.

26 Členské státy předávají údaje Europolu prostřednictvím jeho aplikace sítě pro bezpečnou výměnu informací (SIENA), kde je kategorizace subjektů údajů zavedena jako povinné pole.

27 Viz například článek 6 směrnice (EU) 2016/680 (dále jen „směrnice o prosazování práva“, pokud jde o nepřímo příslušné orgány), Úř. věst. L 119, 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj; článek 51 nařízení Rady (EU) 2017/1939 (dále jen „nařízení o úřadu EPPO“), Úř. věst. L 283, 31.10.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj; ustanovení čl. 27 odst. 3 nařízení (EU) 2018/1727 (dále jen „nařízení o Eurojustu“), Úř. věst. L 295, 21.11.2018, s. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

28 https://www.edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf.

Článek 18a nařízení o Europolu stanoví výjimku, která Europolu umožňuje zpracovávat osobní údaje získané od **příslušného orgánu**, Úřadu evropského veřejného žalobce (**EPPO**) nebo **Eurojustu**, pokud je to nezbytné pro podporu **probíhajícího trestního vyšetřování**, aniž by bylo nutné provést kategorizaci subjektů údajů, pokud již nebyla provedena, a mimo kategorie subjektů údajů uvedené v nařízení o Europolu. Europol může údaje zpracovávat prostřednictvím **operativní analýzy** nebo ve výjimečných a řádně odůvodněných případech **křížovou kontrolou** s cílem zjistit souvislosti nebo jiné relevantní vazby. Tato výjimka byla navržena tak, aby řešila rozdíly mezi pravidly pro kategorizaci subjektů údajů platnými pro Europol a pravidly platnými pro příslušné orgány, úřad EPPO a Eurojust.

(4) Spolupráce se třetími stranami: články 26, 26a a 26b nařízení o Europolu o výměně osobních údajů mezi Europolem a soukromými subjekty

Pachatelé trestné činnosti stále častěji zneužívají (přeshraniční) služby soukromých subjektů – internetové, finanční a klasické telekomunikační služby. **Soukromé subjekty proto disponují velkým množstvím osobních údajů důležitých pro vyšetřování trestných činů**. Zejména internet vytvořil veřejný prostor, který je ve skutečnosti v soukromých rukou, což ztěžuje prosazování pravidel na internetu pro účely vymáhání práva stejně účinně jako mimo něj.[29]

V této souvislosti se **spolupráce mezi orgány pro vymáhání práva a soukromými subjekty** stala **nezbytnou.** Jak je uvedeno v Evropské strategii vnitřní bezpečnosti, **ProtectEU**, bude v zájmu snazší výměny informací nezbytné posílit partnerství se soukromým sektorem[30]. Policejní ředitelé ve svém společném prohlášení o budoucnosti Europolu[31] rovněž vyzvali, aby Europol sloužil jako „**důležitá brána pro získávání informací od soukromých subjektů**“. Povaha této spolupráce sahá od sdílení informací a poskytování komerčních dat s otevřeným zdrojovým kódem až po zapojení do výzkumných a inovačních projektů a poskytování služeb na podporu fungování podniků.[32] Například v roce 2025 se Europolu podařilo ve spolupráci se společností Microsoft, která celosvětově identifikovala více než 394 000 počítačů se systémem Windows infikovaných malwarem Lumma, úspěšně narušit nejvýznamnější infostealerovou hrozbu na světě, Lumma Stealer[33].

Nařízení (EU) 2022/991 zavedlo pro Europol **další možnosti** výměny osobních údajů se soukromými subjekty. Dříve mohl Europol získávat osobní údaje od soukromých subjektů pouze prostřednictvím národní jednotky Europolu (NJE) nebo prostřednictvím předem určených kontaktních míst či orgánů třetích zemí nebo mezinárodních organizací. Účel zpracování Europolem byl omezen na určení příslušné národní jednotky nebo kontaktního místa či orgánu třetí země a mezinárodní organizace, který by mohl převzít odpovědnost za daný případ.

Pozměněný článek 26 nařízení o Europolu rozšířil úkoly Europolu a umožnil mu komplexně zpracovávat informace (včetně osobních údajů) od soukromých subjektů. Hlavním účelem zpracování zůstává určení dotčené národní jednotky Europolu (NJE). Europol však

---

29 SWD(2020) 543 final ze dne 9. prosince 2020, s. 16.

30 Viz ProtectEU: Evropská strategie vnitřní bezpečnosti, s. 6.

31 https://prezydencja.policja.pl/ppl/aktualnosci/260402,Wspolna-Deklaracja-Europejskich-Szefow-Policji-w-sprawie-przyszlosci-Europolu-Jo.html.

32 Europol, Cooperation with Private Parties („Spolupráce se soukromými subjekty“), 31. května 2023, EDOC #1306090v13. Viz také Milieu Consulting, Study on the Practice of direct exchanges of personal data between Europol and Private Parties („Studie o praxi přímé výměny osobních údajů mezi Europolem a soukromými subjekty“), závěrečná zpráva, září 2020.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Další příklady jsou k dispozici v doprovodném pracovním dokumentu útvarů Komise.

nyní může informace doplnit o vlastní analýzu, aby usnadnil další zpracování případu na vnitrostátní úrovni.

Kromě horizontálních ustanovení článku 26 nařízení o Europolu zavedl článek 26a nařízení o Europolu pravidla pro **online krizové situace** a článek 26b se zabýval **šířením materiálů o pohlavním zneužívání dětí online**. V těchto případech může Europol pomáhat členským státům tím, že bude zpracovávat osobní údaje získané přímo od soukromých subjektů. V jednotlivých případech může Europol soukromým subjektům osobní údaje také předávat.

Nařízení (EU) 2022/991 zavedlo možnost využívat infrastrukturu Europolu pro výměnu informací mezi příslušnými orgány a soukromými subjekty a také možnost Europolu požádat členské státy, aby v souladu se svými vnitrostátními právními předpisy získávaly osobní údaje od soukromých subjektů.

Tato ustanovení byla přijata v souladu s dalšími iniciativami, jako je nařízení o teroristickém obsahu online[34] a nařízení o digitálních službách[35]. V rámci Evropské strategie vnitřní bezpečnosti, **ProtectEU**[36], se počítá s dalšími opatřeními, která zvýší zapojení soukromých subjektů do boje proti trestné činnosti a usnadní zákonný přístup k údajům, aby se uskutečnila „ambice změnit kulturu v oblasti bezpečnosti“ (**celospolečenský přístup**).

(5) Interní a externí dohled nad dodržováním základních práv ze strany Europolu

Nařízení (EU) 2022/991 zdůrazňuje povinnost Europolu dodržovat základní práva podle ustanovení vymezujících úkoly Europolu a posílilo související záruky, zejména **posílením interního a externího dohledu nad agenturou**.

V oblasti ochrany údajů znamenalo sladění nařízení o Europolu se zárukami ochrany údajů podle nařízení EU o ochraně údajů zavedení nových pravidel pro dohled ze strany **pověřence pro ochranu osobních údajů** a **evropského inspektora ochrany údajů** (EIOÚ). Například povinnost provést posouzení vlivu na ochranu osobních údajů a předchozí konzultace s evropským inspektorem ochrany údajů se staly systematickými pro každý nový typ zpracování. Nařízení (EU) 2022/991 rovněž zavedlo novou pravomoc Europolu v oblasti žádostí o přístupová práva. Dříve byly za vyřizování žádostí o přístupová práva odpovědné příslušné vnitrostátní orgány, pokud byly poskytovateli údajů členské státy.

Nařízením (EU) 2022/991 byla rovněž zřízena **nová pozice úředníka pro otázky základních práv** v Europolu, který je mimo jiné pověřen informováním výkonného ředitele Europolu o možném porušování základních práv v průběhu činností agentury.

Kromě toho byly **posíleny demokratický dohled a odpovědnost** prostřednictvím politického monitorování činností Europolu **Evropským parlamentem a vnitrostátními parlamenty**, jak je stanoveno v čl. 88 odst. 2 druhém pododstavci Smlouvy o fungování Evropské unie (SFEU). Nařízení (EU) 2022/991 posílilo monitorování prováděné **skupinou pro společnou parlamentní kontrolu**[37]. Stanovilo například povinnou konzultaci této skupiny k návrhu víceletého programování a ročních pracovních programů Europolu, možnost skupiny adresovat Europolu nezávazná konkrétní doporučení a předkládat je Evropskému parlamentu a vnitrostátním parlamentům a zřízení poradního fóra, které by skupině pro společnou parlamentní kontrolu na požádání poskytovalo nezávislé poradenství v otázkách základních práv.

---

34 Nařízení (EU) 2021/784, Úř. věst. L 172, 17.5.2021, s. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj.

35 Nařízení (EU) 2022/2065, Úř. věst. L 277, 27.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

36 Viz ProtectEU: Evropská strategie vnitřní bezpečnosti, s. 2.

37 Viz https://www.europarl.europa.eu/relnatparl/en/eu-agencies-oversight/jpsg-on-europol.

3. Hlavní zjištění hodnocení

3.1. Aktuální stav operativního provádění nových pravomocí a úkolů Europolu v oblasti zpracování osobních údajů

Nařízení (EU) 2022/991 vstoupilo **v platnost dne 28. června 2022**. Jeho operativní provádění však záviselo na různých řídicích, technických a administrativních opatřeních a také na provozních požadavcích, jako je v některých případech zřízení nových struktur IKT.

O tři roky později **byla do provozu uvedena téměř všechna ustanovení** uvedená v čl. 68 odst. 3 nařízení (EU) 2022/991. Ustanovení týkající se analýzy rozsáhlých a složitých souborů údajů (čl. 18 odst. 6a a článek 18a nařízení o Europolu) a spolupráce se soukromými subjekty (články 26, 26a a 26b nařízení o Europolu) se začala uplatňovat od 28. června 2022 nebo krátce poté. Zpracování osobních údajů pro výzkumné a inovační projekty (čl. 18 odst. 2 písm. e) nařízení o Europolu) bylo zahájeno v roce 2023 poté, co bylo zřízeno prostředí pískoviště s názvem ODIN, které splňuje zvláštní požadavky na ochranu údajů podle článku 33a nařízení o Europolu. Do 29. června 2025 ještě nezačala fungovat možnost Europolu navrhovat členským státům **informační záznamy do SIS** podle čl. 4 odst. 1 písm. t) nařízení o Europolu, protože technická implementace nového typu záznamů stále probíhá. Uvedení do provozu se **očekává v roce 2026**.

3.2. Vyhodnocení provozního dopadu nových pravomocí a úkolů Europolu v oblasti zpracování osobních údajů na cíle agentury podle článku 3 nařízení o Europolu

Pokud jde o provozní dopad nových pravomocí a úkolů Europolu v oblasti zpracování osobních údajů, z konzultace vyplynulo, že **členské státy celkově kladně hodnotí** jejich význam, účinnost a přidanou hodnotu a podporu Europolu jejich příslušným orgánům v souvisejících oblastech[38].

Vyšetřovací pravomoci, jichž se týká toto hodnocení, se nevyužívají průběžně ani systematicky ke zpracování údajů pro účely monitorování; některé z nich jsou dokonce výjimečné povahy, zatímco jiné se při vyšetřování používají pravidelněji podle potřeby. **Provozní využití nových ustanovení** v referenčním období se **z kvantitativního hlediska značně lišilo** v závislosti na různých technických vlastnostech a právních podmínkách spojených s novými ustanoveními.

Europol od členských států obdržel **nezanedbatelný** počet **nových příspěvků bez kategorizace subjektů údajů** podle čl. 18 odst. 6a nařízení o Europolu, a to 653 v roce 2023 a 597 v roce 2024. Nedošlo ke krátkodobému nárůstu příspěvků bez kategorizace subjektů údajů a počet případů, kdy byl uplatněn čl. 18 odst. 6a, zůstal ve srovnání s obdobnými případy v období před 28. červnem 2022 **stabilní**. Nová ustanovení neměla žádný negativní dopad ani na zapojení členských států do provádění kategorizace subjektů údajů[39]. V letech 2023 až 2024 tvořil podíl příspěvků bez kategorizace subjektů údajů **méně než 1 % všech příspěvků** přijatých Europolem od členských států (0,85 % v roce 2023 a 0,71 % v roce 2024). Od června 2022 Europol důsledně dokončoval kategorizaci subjektů údajů do 18 měsíců, aniž by využil prodlouženou 36měsíční lhůtu. Europol a šest členských států zdůraznilo, že navzdory lepší právní jistotě **zůstává administrativní zátěž** pro Europol i příslušné orgány **značná**, a to kvůli

[38] Viz důkazy předložené v oddíle 5 pracovního dokumentu útvarů Komise přiloženého k této zprávě, a zejména podání Europolu a odpovědi členských států na otázky 2, 4 a 5 krátkého dotazníku ze dne 2. června 2025 v příloze III pracovního dokumentu útvarů Komise.

[39] Jak zdůraznil jeden členský stát během konzultace, „[členské státy] mohou jasně rozlišit, s jakým druhem údajů mají co do činění, což může být velmi důležité při samotném vyšetřování“.

úsilí, které je třeba vynaložit k dosažení souladu s kategorizací osobních údajů podle účasti jednotlivých osob na trestném činu. Europol tento požadavek uplatňuje velmi přísně[40].

Europol uvedl, že výměna informací se **soukromými subjekty** byla v roce 2023 stále zanedbatelná, neboť bylo zaznamenáno pouze 26 případů provádění článku 26 nařízení o Europolu (kromě případů spadajících do působnosti nařízení o digitálních službách)[41]. V roce **2024** však statistiky ukázaly **prudký nárůst na 284** (o téměř 1 000 % více) případů spolupráce se soukromými subjekty podle článku 26 nařízení o Europolu. To se týkalo zejména údajů od soukromých společností za účelem vyšetřování **finančních a hospodářských trestných činů**. Europol rovněž významně využil článek 26b nařízení o Europolu v boji proti pohlavnímu vykořisťování dětí, kde byla spolupráce se soukromými subjekty velmi významná již dříve. V obou případech údaje zahrnují i spolupráci, která byla možná podle předchozího právního rámce. Dostupné údaje neuvádějí, do jaké míry tyto nové případy spadají do působnosti nových ustanovení nebo zda se stávající možnosti využívají více.

V roce **2025** přijal Europol **novou strategii** pro další posílení spolupráce se soukromými subjekty. Kromě toho byla přijata opatření na modernizaci infrastruktury informačních a komunikačních technologií Europolu, kterou mají příslušné orgány k dispozici pro výměnu informací se soukromými subjekty. V roce **2023** Europol spustil platformu *Plateforme Européenne de Retraits de Contenus Illégaux sur Internet* (**(PERCI**), která má usnadnit provádění nařízení o teroristickém obsahu online a v budoucnu případně i článku 18 nařízení o digitálních službách, jakož i *službu EU pro postupování případů zneužívání dětí* **(EU CARES)**. Platforma PERCI není součástí informačního systému Europolu[42].

Ostatní ustanovení se nepoužila vůbec (článek 26a nařízení o Europolu), přestože byla platná, **nebo** byla použita **pouze výjimečně** (jeden případ, kdy byl článek 18a nařízení o Europolu využit v roce 2024, a jeden projekt realizovaný se zpracováním osobních údajů podle čl. 18 odst. 1 písm. t) nařízení o Europolu v roce 2025, přičemž tři nové projekty se již připravují).

Vzhledem k omezenému období operativního provádění ustanovení zavedených nařízením (EU) 2022/991 a zdlouhavé povaze vyšetřování trestných činů a soudních řízení nebyly členské státy schopny poskytnout kvantitativní údaje o dopadu těchto ustanovení z operativního hlediska. Namísto toho nabídly několik příkladů úspěšných vyšetřování, které ukazují **hmatatelný přínos nových vyšetřovacích možností v reálných situacích** pro již používaná ustanovení, jako jsou například EncroChat, Sky ECC, balkánské zločinecké sítě zapojené do obchodu s kokainem nebo Lumma Stealer.

Europol a osm členských států rovněž označilo několik **oblastí, které je třeba zlepšit**, aby se maximalizovalo účinné a soudržné využívání nového právního rámce a posílila role Europolu v budoucnosti. Existují obavy, zejména ze strany Europolu, že nadměrná složitost, roztříštěnost a délka právních ustanovení může odborníky z praxe nebo soukromé subjekty odradit od využívání nových dostupných nástrojů. Připomínky členských států se týkají spíše způsobu, jakým Europol restriktivně provádí záruky ochrany údajů pod dohledem evropského inspektora ochrany údajů, což může ohrozit účinnost a přidanou hodnotu některých ustanovení.

3.3. Posouzení dopadu nových pravomocí a úkolů Europolu v oblasti zpracování osobních údajů na základní práva

---

40 Viz pododdíl 7.1.3. pracovního dokumentu útvarů Komise přiloženého k této zprávě a odpovědi členských států na otázku 9 krátkého dotazníku ze dne 2. června 2025 v příloze III pracovního dokumentu útvarů Komise.

41 Europol, zpráva za rok 2023 podle čl. 16 odst. 11 nařízení o Europolu.

42 Nařízení (EU) 2019/818, Úř. věst. L 135, 22.5.2019, s. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

Z dosud omezeného využívání nových pravomocí v oblasti zpracování osobních údajů Komise **nezjistila žádné** důkazy o **negativním dopadu na základní práva** v důsledku operativního využívání nových pravomocí v oblasti zpracování osobních údajů.

Kromě provádění zvláštních požadavků na ochranu údajů souvisejících s novými pravomocemi v oblasti zpracování osobních údajů Europol postupně přijal veškerá nezbytná opatření k zavedení nových horizontálních mechanismů dohledu souvisejících se základními právy.

V roce 2024 přijala správní rada Europolu revidovaná prováděcí pravidla pověřence pro ochranu osobních údajů jako jeden z posledních nezbytných prováděcích aktů souvisejících s novým režimem ochrany údajů. Ze shromážděných důkazů vyplývá, že Europol a jeho správní rada ve spolupráci s pověřencem Europolu pro ochranu osobních údajů a evropským inspektorem ochrany údajů rovněž zajistili **důsledné provádění nových záruk ochrany údajů** zavedených v roce 2022. Tento přístup na první pohled účinně zabránil jakémukoli negativnímu dopadu nebo zásahu počátečního využívání nových pravomocí v oblasti zpracování osobních údajů do práv fyzických osob na soukromí a ochranu osobních údajů. Podle členských států má Europol v současné době k dispozici **spolehlivý právní rámec pro ochranu údajů**, který zajišťuje dostatečné záruky pro případné větší využívání jeho nových pravomocí. Sedm členských států rovněž zdůraznilo, že tento rámec **usnadňuje tok informací**, protože zvyšuje důvěru, ačkoli stále existuje prostor pro zlepšení. Pouze jeden členský stát se vyjádřil negativně[43].

Kromě konkrétních **problémů** souvisejících s kategorizací subjektů údajů Europol a čtyři členské státy uvedly jako oblasti pro zlepšení náklady a čas spojený s **posouzením vlivu na ochranu údajů** a **předběžnou konzultací** s evropským inspektorem ochrany údajů, které se v praxi provádějí standardně. Dalším problémem, který zmínilo šest členských států, je vyřizování **žádostí subjektů údajů o přístup** ze strany Europolu, který je nyní příslušný i v případě, že je vlastníkem údajů členský stát.

První úředník pro otázky základních práv byl jmenován v prosinci **2022**. Za první dva roky svého mandátu **neobdržel ani nepředložil** výkonnému řediteli **žádnou stížnost**. Skupina pro společnou parlamentní kontrolu nadále pečlivě sleduje činnosti Europolu a od doby, kdy nová ustanovení vstoupila v platnost, nevydala žádná doporučení. Evropský parlament zřídil v únoru **2024 poradní fórum skupiny pro společnou parlamentní kontrolu pro základní práva**.

3.4. Analýza nákladů a přínosů nových pravomocí a úkolů Europolu v oblasti zpracování osobních údajů

Vzhledem k rané fázi provádění ustanovení zavedených nařízením (EU) 2022/991 a omezeným zkušenostem s nimi je **předčasné**, aby Komise vyvozovala smysluplné závěry o nových ustanoveních na základě **analýzy nákladů a přínosů**.

Útvary Komise shromáždily od Europolu informace o nákladech, které dosud vznikly v souvislosti s operativním prováděním nařízení (EU) 2022/991, pokud jde o přezkoumávaná ustanovení. Tyto náklady činily v letech 2022 až 2025 celkem přibližně **25 milionů EUR** (přibližně 5 % celkového přídělu pro Europol[44]) a zahrnovaly především jednorázové náklady. Členským státům doposud nevznikly žádné nové relevantní náklady, které by byly konkrétně spojeny s nařízením (EU) 2022/991.

---

43 Viz odpovědi členských států na otázku 9 krátkého dotazníku ze dne 2. června 2025 v příloze III doprovodného pracovního dokumentu útvarů Komise.

44 Ve stejném období činil rozpočet přidělený Europolu celkem přibližně **860 milionů EUR** (postupně se zvyšoval ze 192 milionů EUR v roce 2022 na 241 milionů EUR v roce 2025). Podrobnosti naleznete v doprovodném pracovním dokumentu útvarů Komise.

Většinu nákladů (téměř 17 milionů EUR) tvořily významné investice do **vývoje nových struktur IKT**, provádění ustanovení o výzkumu a inovacích (pískoviště ODIN) a do informačních systémů pro výměnu osobních údajů se soukromými subjekty (PERCI a EU CARES). Náklady na **lidské zdroje (HR)**, a to jak v souvislosti s IKT, tak s provozem, tvořily přibližně jednu třetinu celkových výdajů (přibližně 8 milionů EUR). Lidské zdroje budou **v dlouhodobém horizontu představovat hlavní opakující se náklady**.

Je třeba poznamenat, že výše uvedených 8 milionů EUR nezahrnuje náklady na lidské zdroje pro jednotku odpovědnou za správu informací ani zdroje spojené s (dřívějšími a novými) opatřeními v oblasti dohledu, která mají horizontální charakter a u nichž není možné rozdělení na úrovni provádění konkrétních ustanovení. Náklady na tyto zdroje nejsou zanedbatelné. Odhaduje se například, že v roce 2023 bude **60 ekvivalentů plného pracovního úvazku** (téměř **5 %** zaměstnanců Europolu) zapojeno do činností v **orgánech zabývajících se zajišťováním kvality a dozorem a v subjektech v oblasti dohledu a poradenství**. Europol přidělil 25 ekvivalentů plného pracovního úvazku na činnosti související s dohledem nad ochranou údajů a odpovídajícími opatřeními v oblasti zajištění. To zahrnuje následné kroky v návaznosti na doporučení evropského inspektora ochrany údajů a činnost vytvořenou v rámci předchozích konzultací pro operativní zpracování údajů. Šestnáct z těchto 25 ekvivalentů plného pracovního úvazku se konkrétně zabývá činnostmi souvisejícími s požadavky evropského inspektora ochrany údajů. Od června 2025 má Europol specializovaný tým osmi zaměstnanců na plný úvazek v oblasti ochrany údajů, včetně pověřence pro ochranu osobních údajů.

Podle Europolu a patnácti členských států se očekává, že **přínosy** nových pravomocí a úkolů v oblasti zpracování osobních údajů, zejména analýzy rozsáhlých a složitých souborů údajů a spolupráce se soukromými subjekty, budou značné a **převáží nad souvisejícími náklady**. Žádný členský stát nebyl jiného názoru. V dlouhodobém horizontu lze důvodně očekávat určité zvýšení efektivity, a to díky účinkům úspor z rozsahu a klesajícím marginálním nákladům. Jeden z členských států zdůraznil, že „je důležité, aby Europol poskytl nezbytné zdroje v oblasti informačních a komunikačních technologií k zajištění a dalšímu rozvoji nástrojů pro provádění nových možností nařízení (EU) 2022/991“, což podpořily i dva další členské státy a další zúčastněné strany[45].

Podle názoru Europolu a pěti členských států je třeba **v rámci stávajícího rámce řízení, správy a ochrany údajů** řešit také možné **nedostatky** při provádění, aby nedošlo k oslabení provozního dopadu nových úkolů v oblasti zpracování osobních údajů tím, že by se zpozdilo nebo omezilo jejich používání. Pět členských států zpochybnilo příliš opatrné provádění pravidel ochrany údajů ze strany Europolu a jeho správní rady pod vedením evropského inspektora ochrany údajů. Navrhují, aby flexibilita, kterou spolunormotvůrci poskytují, byla náležitě využita k maximalizaci účinnosti a efektivity úkolů Europolu a k zajištění jejich relevance a dlouhodobé ziskovosti.

Hodnocení pracovních metod Europolu a potenciálních oblastí pro zjednodušení nespadá do oblasti působnosti zprávy podle čl. 68 odst. 3 nařízení o Europolu a bude provedeno v rámci hodnocení podle čl. 68 odst. 1 nařízení o Europolu.

4. Závěry a další postup

[45] Viz důkazy předložené v oddíle 5 pracovního dokumentu útvarů Komise přiloženého k této zprávě, a zejména podání Europolu a odpovědi členských států na otázky 2, 4 a 5 krátkého dotazníku ze dne 2. června 2025 v příloze III pracovního dokumentu útvarů Komise a společné prohlášení evropských policejních ředitelů o budoucnosti Europolu.

Celkově lze říci, že podle předběžných hlavních zjištění Komise členské státy nadále **podporují úlohu Europolu** v klíčových oblastech, v nichž v současné době pomáhá členským státům s **novými úkoly v oblasti zpracování osobních údajů**. Podle názoru některých zúčastněných stran je však v zájmu **maximalizace přínosů** nových pravomocí v oblasti zpracování osobních údajů třeba **řešit možné nedostatky**, zejména v rámci stávajícího rámce řízení, správy a ochrany údajů, které mohou zpozdit a omezit jejich využívání. Bylo by také užitečné zmírnit **složitost a roztříštěnost** právního rámce, které mohou odborníky z praxe odrazovat od využívání nových možností.

Obecně Komise nenašla důkazy o tom, že by nová pravidla měla **negativní dopad na základní práva**, a to zejména díky spolehlivým zárukám ochrany údajů, které rovněž usnadňují tok informací tím, že zvyšují důvěru partnerů. U některých členských států agentura upřednostňuje konzervativní přístup, přičemž **by měla být přiměřeně využita flexibilita, kterou spolunormotvůrci poskytují**, pokud jde o kategorizaci subjektů údajů, posouzení vlivu na ochranu údajů, předchozí konzultace s inspektorem Europolu pro ochranu údajů a vyřizování žádostí o přístupová práva.

Vzhledem k obecně krátkému období provádění nových pravidel ochrany osobních údajů stanovených nařízením (EU) 2022/991 však shromážděné důkazy nejsou ve všech otázkách přesvědčivé.

V Evropské strategii vnitřní bezpečnosti, **ProtectEU**[46], Komise oznámila, že navrhne ambiciózní revizi mandátu Europolu, aby mohl řešit stupňující se bezpečnostní výzvy. V souladu se svými pokyny pro zlepšování právní úpravy[47] zahájila Komise přípravy na hodnocení nařízení o Europolu a pracovních metod Europolu, čímž připravuje půdu pro svůj **návrh v roce 2026 zaměřený na zvýšení operativnosti agentury, jak je uvedeno v politických směrech**[48]. V červenci 2025 Komise zveřejnila výzvu k předložení faktických podkladů[49] a zadala externí studii, která má podpořit hodnocení nařízení o Europolu a posouzení dopadů nového návrhu. Hodnocení nařízení o Europolu provedené pro účely přípravy této zprávy má k tomuto hodnocení přispět.

46 ProtectEU: Evropská strategie vnitřní bezpečnosti, s. 10.

47 Viz https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en.

48 Ursula von der Leyenová, Politické směry pro příští Evropskou komisi 2024–2029, e6cd4328-673c-4e7a-8683-f63ffb2cf648_en.

49 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Spoluprace-v-oblasti-prosazovani-prava-nove-narizeni-o-Europolu-navrh-_cs.