KOMISJA
EUROPEJSKA

Bruksela, dnia 11.12.2025 r.
COM(2025) 752 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY

oceniające wpływ operacyjny wdrożenia zadań przewidzianych w rozporządzeniu (UE) 2022/991, w szczególności w art. 4 ust. 1 lit. t), art. 18 ust. 2 lit. e), art. 18 ust. 6a, a także art. 18a, art. 26, art. 26a i art. 26b w odniesieniu do celów Europolu, a także wpływ tych zadań na prawa podstawowe i wolności określone w Karcie zgodnie z art. 68 ust. 3 rozporządzenia (UE) 2016/794

{SWD(2025) 404 final}

1. Zakres oceny

Od czasu rozpoczęcia działalności w 1999 r. **Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol)** odgrywa **kluczową rolę w zwalczaniu poważnej przestępczości transgranicznej i terroryzmu** i stała się główną siłą napędową współpracy organów ścigania w Europie. W ciągu ostatnich 30 lat sytuacja w zakresie bezpieczeństwa zdecydowanie się zmieniła ze względu na zmianę DNA poważnej i zorganizowanej przestępczości[1]. Państwa członkowskie mają nowe potrzeby operacyjne związane ze skutecznym reagowaniem na pojawiające się zagrożenia, a ich **oczekiwania dotyczące wsparcia ze strony Europolu** również się **zmieniły**. W związku z tym kilkakrotnie zastępowano lub zmieniano zakres działania Europolu, aby utrzymać i zwiększyć znaczenie Agencji.

Zakres działania Europolu określony w rozporządzeniu (UE) 2016/794[2] („rozporządzenie w sprawie Europolu") został ostatnio zmieniony w 2022 r. rozporządzeniem (UE) 2022/991[3] w celu sprostania nowym zagrożeniom dla bezpieczeństwa. Rozporządzenie w sprawie Europolu nie było już adekwatne do zakładanych celów w nowej rzeczywistości, w której przestępcy wykorzystują korzyści wynikające z **transformacji cyfrowej**, **nowych technologii**, **globalizacji** i **mobilności**[4].

Cele szczegółowe rozporządzenia (UE) 2022/991[5] były następujące:

- umożliwienie skutecznej współpracy między **podmiotami prywatnymi** a organami ścigania w zakresie przeciwdziałania nadużywaniu usług transgranicznych przez przestępców;
- umożliwienie organom ścigania analizy **dużych i złożonych zbiorów danych** w celu wykrycia powiązań transgranicznych, z zachowaniem całkowitej zgodności z **prawami podstawowymi**;
- umożliwienie państwom członkowskim wykorzystywania **nowych technologii** do ścigania przestępstw.

Ponadto rozporządzeniem (UE) 2022/991 zmieniono przepisy o ochronie danych mające zastosowanie do Europolu, aby utrzymać **wysoki poziom ochrony danych**, zachowując równowagę między nowymi uprawnieniami Agencji w zakresie przetwarzania danych osobowych a prywatnością i ochroną danych osobowych osób fizycznych. W rozporządzeniu w dużej mierze dostosowano przepisy o ochronie danych mające zastosowanie do Europolu do przepisów mających zastosowanie do innych agencji i organów UE działających w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (WSiSW) na podstawie rozdziału IX rozporządzenia (UE) 2018/1725 („rozporządzenie (UE) 2018/1725") oraz do przepisów mających zastosowanie do organów ścigania państw członkowskich („właściwe organy") na mocy ich prawa krajowego transponującego dyrektywę (UE) 2016/680 („dyrektywa o ochronie danych w sprawach karnych")[6] w celu **ułatwienia przepływu informacji**.

---

1 Europol, Ocena zagrożenia poważną i zorganizowaną przestępczością w Unii Europejskiej (SOCTA) 2025: „The changing DNA of serious and organised crime" [Zmieniające się DNA poważnej i zorganizowanej przestępczości], dostępna na stronie https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf („EU SOCTA 2025"). Zob. również ocena zagrożeń celnych (CTA) z 2025 r., dostępna na stronie https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

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

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

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

5 *Tamże.*

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

Niniejsze sprawozdanie przyjęto zgodnie z obowiązkiem Komisji wynikającym z **art. 68 ust. 3 rozporządzenia w sprawie Europolu** dotyczącym oceny[7] wpływu operacyjnego zadań Europolu, jak określono w rozporządzeniu (UE) 2022/991, trzy lata po jego wejściu w życie. Zgodnie z upoważnieniem współprawodawców Komisja: po pierwsze, oceniła **wpływ operacyjny** niektórych nowych przepisów dotyczących przetwarzania danych osobowych w odniesieniu do celów Europolu, zgodnie z art. 3 rozporządzenia w sprawie Europolu (a mianowicie wspierania i wzmacniania działań właściwych organów państw członkowskich oraz ich wzajemnej współpracy w zakresie zapobiegania przestępstwom wchodzącym w zakres działań Europolu i ich zwalczania); po drugie, oceniła wpływ tych przepisów na **prawa podstawowe i wolności** („prawa podstawowe") zapisane w Karcie[8] i po trzecie, przeprowadziła **ocenę kosztów i korzyści** powiązanych zadań przetwarzania danych.

Aby przygotować przegląd, służby Komisji zebrały informacje i opinie z różnych źródeł oraz przeprowadziły konsultacje *ad hoc* z Europolem i państwami członkowskimi. Towarzyszący **dokument roboczy służb Komisji** zawiera szczegółowy opis ogólnego kontekstu i metodyki przeglądu, a także wyczerpujący opis źródeł dowodów i konsultacji potwierdzających główne ustalenia streszczone w niniejszym sprawozdaniu.

2. Kontekst ogólny

Zgodnie z art. 68 ust. 3 rozporządzenia w sprawie Europolu niniejsze sprawozdanie Komisji obejmuje wybrane przepisy rozporządzenia (UE) 2022/991 i koncentruje się na pięciu kluczowych aspektach pracy Europolu.

1) Wymiar zewnętrzny: art. 4 ust. 1 lit. t) rozporządzenia w sprawie Europolu odnoszący się proponowanych przez Europol wpisów informacyjnych do Systemu Informacyjnego Schengen (SIS) dotyczących obywateli państw trzecich

Biorąc pod uwagę **globalny charakter poważnej przestępczości i terroryzmu**, informacje będące w posiadaniu państw trzecich i organizacji międzynarodowych o sprawcach i osobach podejrzanych o takie przestępstwa mają coraz większe znaczenie dla bezpieczeństwa wewnętrznego UE. Zewnętrzny wymiar unijnej współpracy organów ścigania stał się zatem kluczowy dla państw członkowskich, podobnie jak **rola Europolu we wspieraniu państw członkowskich w ich partnerstwach z państwami trzecimi** lub podmiotami mającymi siedzibę w tych państwach. W **przyszłości zasadnicze znaczenie** będą miały dalsze wysiłki na rzecz poprawy bezpieczeństwa globalnego[9].

Rozporządzeniem (UE) 2022/991 wprowadzono już istotne zmiany do rozporządzenia w sprawie Europolu w celu wzmocnienia **zewnętrznego wymiaru działań Europolu**, w szczególności ułatwienia wymiany informacji z państwami trzecimi[10] i zobowiązania

---

[7] Niniejsza ocena przeprowadzona zgodnie z art. 68 ust. 3 rozporządzenia w sprawie Europolu nie jest oceną, którą należy przeprowadzić zgodnie z wytycznymi w sprawie lepszego stanowienia prawa w kontekście ewentualnego wniosku dotyczącego zmiany rozporządzenia w sprawie Europolu. Zob. także sekcja 4 poniżej.

[8] Karta praw podstawowych Unii Europejskiej, Dz.U. C 326 z 26.10.2012, s. 391, ELI: http://data.europa.eu/eli/treaty/char_2012/oj.

[9] Zob. ProtectEU: europejska strategia bezpieczeństwa wewnętrznego, COM(2025) 148 final z dnia 1 kwietnia 2025 r., https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52025DC0148.

[10] Zob. na przykład art. 25 ust. 4a rozporządzenia w sprawie Europolu zapewniający Europolowi możliwość przekazywania danych do państw trzecich po przeprowadzeniu przez Europol samooceny wszystkich okoliczności towarzyszących przekazaniu danych osobowych i stwierdzeniu, że istnieją odpowiednie zabezpieczenia w zakresie ochrony danych osobowych, a także art. 25 ust. 5 rozporządzenia w sprawie Europolu rozszerzający zakres wyjątkowych przypadków, w których Europol może przekazywać dane (kategorie danych) *ad hoc* w należycie uzasadnionych przypadkach do państw trzecich i organizacji międzynarodowych.

Europolu do włączenia strategii dotyczącej stosunków z państwami trzecimi i organizacjami międzynarodowymi do swojego programowania wieloletniego i rocznych programów prac[11].

W art. 4 ust. 1 lit. t) rozporządzenia w sprawie Europolu powierzono Europolowi nowe zadanie: wspieranie państw członkowskich w przetwarzaniu danych dotyczących osób zaangażowanych w działalność terrorystyczną lub poważną przestępczość, dostarczanych przez państwa trzecie lub organizacje międzynarodowe. Obejmuje to **proponowanie państwom członkowskim ewentualnego wprowadzenia do Systemu Informacyjnego Schengen (SIS) wpisów informacyjnych dotyczących obywateli państw trzecich w interesie Unii**. Tę nową kategorię wpisów informacyjnych wprowadzono w 2022 r.[12] w następstwie zmiany rozporządzenia (UE) 2018/1862 w sprawie użytkowania SIS w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych[13].

Niektóre informacje, zwłaszcza gdy dana osoba nie jest obywatelem UE i nie ma związku ze sprawą krajową, są przekazywane przez państwo trzecie wyłącznie Europolowi, który przetwarza dane i udostępnia wyniki swoich analiz wszystkim państwom członkowskim. Celem nowych przepisów była **maksymalizacja wykorzystania informacji** otrzymywanych przez Europol od państw trzecich przez zapewnienie większego dostępu do tych danych niż gdyby były one dostępne wyłącznie za pośrednictwem własnego systemu Europolu. Przepisy te uzupełniły inne środki, takie jak europejski portal wyszukiwania oraz ramy interoperacyjności[14] między systemami informacyjnymi UE w dziedzinie bezpieczeństwa oraz zarządzania granicami i migracją, eliminując niedociągnięcia strukturalne związane z tymi systemami, utrudniające pracę organów krajowych, w szczególności straży granicznej.

SIS jest postrzegany jako **kluczowy dodatkowy kanał rozpowszechniania informacji**: jest najpowszechniej wykorzystywaną bazą danych w Europie do celów ścigania przestępstw, kontroli granic i migracji. W 2024 r. w SIS przeprowadzono ponad 15 mld wyszukiwań w porównaniu z około 14 mln wyszukiwań w systemie informacyjnym Europolu i mniej niż 3 mld wyszukiwań (na całym świecie) w 19 bazach danych Interpolu, czyli w dwóch pozostałych wiodących systemach informacyjnych dla właściwych organów[15].

2) Innowacje: art. 18 ust. 2 lit. e) i art. 33a rozporządzenia w sprawie Europolu dotyczące przetwarzania danych osobowych przez Europol na potrzeby projektów w dziedzinie innowacji i badań naukowych

Rozwój technologiczny stwarza zarówno ogromne możliwości, jak i znaczne wyzwania dla bezpieczeństwa wewnętrznego UE[16] i ma tak głęboki wpływ na przestępczość, że zmienia nawet zasadniczy charakter – „DNA" – zagrożeń związanych z poważną i zorganizowaną

---

11 Art. 12 ust. 2 rozporządzenia w sprawie Europolu.

12 Rozporządzenie (UE) 2022/1190; Dz.U. L 185 z 12.7.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 Rozporządzenie (UE) 2018/1862; Dz.U. L 312 z 7.12.2018, s. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 Rozporządzenie (UE) 2019/818; Dz.U. L 135 z 22.5.2019, s. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

15 Sprawozdanie roczne eu-LISA za 2024 r. w sprawie SIS, dostępne pod adresem https://www.eulisa.europa.eu/sites/default/files/documents/sis-annual-report-2024.pdf, Europol, skonsolidowane roczne sprawozdanie z działalności za 2024 r., dostępne na stronie https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF, i https://www.interpol.int/How-we-work/Databases.

16 Europol, ocena zagrożenia zorganizowaną przestępczością internetową (IOCTA) 2024, dostępna na stronie Internet Organised Crime Threat Assessment (IOCTA) 2024 | Europol.

przestępczością[17]. Przestępcy szybko włączają nowe technologie do swojej działalności, tworząc nowe modele działania i udoskonalając taktyki. Jednocześnie postępy te oferują **organom ścigania bezprecedensowe możliwości zwiększenia zdolności**. W związku z tym badania naukowe i innowacje odgrywają kluczową rolę w bezpieczeństwie wewnętrznym, ponieważ przyczyniają się do opracowywania rozwiązań służących przeciwdziałaniu pojawiającym się zagrożeniom i nadążaniu za szybko zmieniającymi się formami i sposobami działania siatek przestępczych, w tym wynikającymi z niewłaściwego wykorzystania technologii. Unia poczyniła inwestycje i będzie nadal inwestować w rozwój innowacyjnych narzędzi w drodze finansowanych przez UE badań naukowych i innowacji w dziedzinie bezpieczeństwa, w ramach europejskiej strategii bezpieczeństwa wewnętrznego **ProtectEU**[18].

Utworzone pod koniec 2019 r. na polecenie ministrów ds. WSiSW państw członkowskich UE **Laboratorium Innowacji Europolu**[19] ma na celu zwiększenie zaangażowania Europolu na rzecz innowacji w dziedzinie ścigania przestępstw. Rozporządzeniem (UE) 2022/991 wprowadzono istotne zmiany do rozporządzenia w sprawie Europolu w celu zwiększenia zakresu działań Europolu w obszarze innowacji, tak aby wspierać potencjał Laboratorium Innowacji Europolu i promować synergię z innymi działaniami w dziedzinie badań naukowych i innowacji na szczeblu UE, w tym w szczególności działaniami Komisji, w ramach **unijnego centrum innowacji** na rzecz bezpieczeństwa wewnętrznego[20].

Aby umożliwić Europolowi **przetwarzanie operacyjnych danych osobowych** również **na potrzeby projektów w dziedzinie badań naukowych i innowacji**, zmieniono art. 18 ust. 2 rozporządzenia w sprawie Europolu dotyczący celów przetwarzania informacji. Dostępność wysokiej jakości zbiorów danych umożliwiających empiryczne testowanie ważności nowych narzędzi jest powszechnie uznawana za kluczowy warunek wstępny rozwoju technologii. Natomiast zawodne lub stronnicze zbiory danych do testowania mogą prowadzić do powstawania niepełnowartościowych technologii[21].

Dostosowane do potrzeb zabezpieczenia służące ochronie danych dotyczące takiego przetwarzania określono w art. 18 ust. 3 lit. a), art. 30 ust. 2 i 3 oraz **art. 33a rozporządzenia w sprawie Europolu**. Ten ostatni artykuł wymagał utworzenia **środowiska piaskownicy**, ponieważ przewidziano w nim, że wszelkie dane osobowe przetwarzane w kontekście projektu muszą być tymczasowo kopiowane do osobnego, wyizolowanego i chronionego środowiska przetwarzania danych w ramach Europolu wyłącznie w celu realizacji tego projektu.

3) **<u>Postępowania przygotowawcze</u>: art. 18 ust. 6a i art. 18a rozporządzenia w sprawie Europolu dotyczące warunków przetwarzania danych osobowych otrzymanych bez kategoryzacji osób, których dane dotyczą**

Europol, pełniąc rolę **unijnego centrum informacji kryminalnych**, nie tylko ułatwia gromadzenie i wymianę informacji, ale także pomaga **zwiększyć skuteczność postępowań przygotowawczych dzięki zaawansowanej analizie danych** oraz wykrywaniu transgranicznych powiązań między przestępstwami a sieciami przestępczymi, niewidocznych na szczeblu krajowym. Zdolności te stanowią wsparcie dla państw członkowskich, ponieważ wzbogacają informacje dostępne na potrzeby prowadzonych przez nie postępowań przygotowawczych.

---

17 Europol, EU SOCTA 2025, s. 19.

18 COM(2025) 148 final z dnia 1 kwietnia 2025 r., https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52025DC0148, s. 9.

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

20 Zob. w szczególności art. 4 ust. 1 lit. v) i w) rozporządzenia w sprawie Europolu.

21 SWD(2020) 543 final z dnia 9 grudnia 2020 r., s. 29.

Dzięki szerokiemu i intensywnemu wykorzystaniu technologii **duże i złożone zbiory danych stały się nową normą we wszystkich aspektach życia**, w tym w przestępczości[22]. W ramach postępowań przygotowawczych dotyczących przestępczości zorganizowanej lub terroryzmu zaczęto napotykać wyzwania związane z analizą dużych ilości danych przechowywanych w formie elektronicznej, często sięgających terabajtów, w tym danych audio, wideo i danych generowanych maszynowo skonfiskowanych podczas postępowań przygotowawczych. Na przykład we wspólnym dochodzeniu mającym na celu rozbicie sieci EncroChat[23] śledczy przeanalizowali miliony wiadomości, które przestępcy wymieniali między sobą w celu planowania poważnych przestępstw. W tym kontekście dostępność niezbędnych narzędzi technologii informacyjno-komunikacyjnych (ICT), wiedzy fachowej i zasobów do analizy dużych i złożonych zbiorów danych (znanych w żargonie technicznym jako „duże zbiory danych" (ang. „big data")[24]) ma kluczowe znaczenie dla organów ścigania i organów sądowych.

Chociaż w rozporządzeniu w sprawie Europolu przyjętym w 2016 r. nie nałożono ograniczeń jako takich na analizę dużych zbiorów danych, brakowało w nim ustrukturyzowanych przepisów określających warunki analizy tego rodzaju danych. **Najistotniejszym punktem** był **wymóg odnoszący się do kategoryzacji osób, których dane dotyczą**. Kategoryzacja osób, których dane dotyczą, odnosi się do potrzeby monitorowania zbiorów danych w celu wyodrębnienia danych osobowych według różnych kategorii, wyczerpująco wymienionych w załączniku II.A i załączniku II.B do rozporządzenia w sprawie Europolu, przed przystąpieniem do faktycznego przetwarzania danych do celów postępowań przygotowawczych, w tym przed sprawdzeniem krzyżowym danych w celu wykrycia powiązań lub przeprowadzeniem analiz o charakterze strategicznym lub tematycznym bądź analiz operacyjnych[25]. Odpowiednie kategorie są powiązane z różnymi rodzajami udziału w postępowaniach przygotowawczych i obejmują (i) podejrzanych, potencjalnych przyszłych sprawców; a także (ii) osoby kontaktowe, wspólników, ofiary, świadków i informatorów związanych z działalnością przestępczą. Zasadniczo Europol nie może przetwarzać ani nawet przechowywać danych osobowych osób, które nie należą do żadnej z tych kategorii.

Przed przekazaniem danych osobowych Europolowi[26] dostawcy danych, tacy jak **państwa członkowskie** lub **organy i agencje UE**, **zazwyczaj** przeprowadzają już kategoryzację osób, których dane dotyczą. Zgodnie z prawem Unii wszyscy dostawcy danych są zobowiązani do przeprowadzania kategoryzacji osób, których dane dotyczą, w przypadku przetwarzania i postępowań przygotowawczych przez nie przeprowadzanych, niezależnie od przekazania danych Europolowi, w oparciu o zasady równoważne, ale nie identyczne z zasadami

---

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 EIOD, opinia 7/2015, s. 7, dostępna na stronie https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf. „Ogólnie wspólnym mianownikiem różnych dostępnych definicji »**dużych zbiorów danych**« jest odniesienie do praktyki łączenia ogromnych ilości informacji pochodzących z różnych źródeł i ich analizowania z wykorzystaniem bardziej zaawansowanych algorytmów do podejmowania decyzji. Duże zbiory danych opierają się nie tylko na rosnącej zdolności technologii do wspierania gromadzenia i przechowywania dużych ilości danych, ale również na jej możliwościach w zakresie analizowania, rozumienia i wykorzystywania pełnej wartości danych (w szczególności z wykorzystaniem aplikacji analitycznych)".

25 Zob. art. 18 ust. 2 rozporządzenia w sprawie Europolu.

26 Państwa członkowskie przekazują dane Europolowi za pośrednictwem aplikacji sieci bezpiecznej wymiany informacji (SIENA), w której kategoryzacja osób, których dane dotyczą, stanowi pole obowiązkowe.

Europolu[27]. W przypadku dużych i złożonych zbiorów danych ręczne przetwarzanie wstępne jest jednak procesem zasobo- i czasochłonnym. Półautomatyczna analiza danych z jednego telefonu komórkowego może trwać do trzech dni, a w trakcie postępowania przygotowawczego można skonfiskować nawet setki telefonów komórkowych. Kategoryzacja osób, których dane dotyczą, **w przypadku dużych zbiorów danych nie zawsze jest możliwa**, z uwagi na samą ilość zbiorów danych, sposób, w jaki dane są (nie)ustrukturyzowane, brak zasobów lub **wymagany nadmierny nakład pracy ręcznej**. W praktyce jedyną możliwością jest przeprowadzenie najpierw bardziej dogłębnej analizy danych z operacyjnego punktu widzenia lub wykrywanie powiązań – również w sposób półautomatyczny – przez sprawdzanie krzyżowe dostępnych danych.

W rozporządzeniu (UE) 2022/991 doprecyzowano warunki odnoszące się do kategoryzacji osób, których dane dotyczą, w celu zagwarantowania **pewności prawa** w odniesieniu do przetwarzania dużych i złożonych zbiorów danych. Europol i Europejski Inspektor Ochrony Danych (EIOD) różnie interpretowali literę i ducha rozporządzenia w sprawie Europolu w odniesieniu do mającego zastosowanie okresu zatrzymywania danych. Według Europolu okres ten powinien wynosić trzy lata; według EIOD okres ten powinien wynosić sześć miesięcy[28]. Konieczne były również nowe przepisy, aby zapewnić **dodatkową elastyczność** i osiągnąć właściwą równowagę między ochroną danych a aspektami bezpieczeństwa.

W art. 18 ust. 5a rozporządzenia w sprawie Europolu, w związku z art. 73 rozporządzenia (UE) 2018/1725, najpierw doprecyzowano ogólną zasadę klasyfikacji osób, których dane dotyczą, na podstawie art. 18 ust. 2 i załącznika II. Europolowi wyznacza się, w stosownych przypadkach i w miarę możliwości, zadanie **wyraźnego przypisania danych osobowych do konkretnej kategorii osób, których dane dotyczą**. W praktyce, przed przetworzeniem danych osobowych Europol powinien co do zasady dokładnie określić rolę w działalności przestępczej (np. czy dana osoba to podejrzany, ofiara czy tylko świadek) w odniesieniu do każdej osoby, której dane osobowe będą przetwarzane, a nie na poziomie zagregowanym w odniesieniu do wszystkich osób w pliku danych, który ma być przetwarzany, lub jego części (na przykład przez zwykłe ustalenie, że wszystkie wymienione osoby są zaangażowane w działalność przestępczą wchodzącą w zakres działania Europolu, na podstawie analizy ogólnych okoliczności, które doprowadziły do wygenerowania pliku danych).

W art. 18 ust. 6a rozporządzenia w sprawie Europolu wyraźnie zezwala się na przetwarzanie danych osobowych otrzymanych bez kategoryzacji osób, których dane dotyczą, przez okres **do 18 miesięcy**, który w uzasadnionych przypadkach może zostać przedłużony do maksymalnie 36 miesięcy, wyłącznie w celu **zakończenia kategoryzacji osób, których dane dotyczą**. Art. 18 ust. 6a rozporządzenia w sprawie Europolu nie odnosi się wyraźnie do dużych i złożonych zbiorów danych, lecz – bardziej ogólnie – wymaga spełnienia kryterium „**absolutnej niezbędności**".

W art. 18a rozporządzenia w sprawie Europolu przewidziano odstępstwo polegające na umożliwieniu Europolowi przetwarzania danych osobowych otrzymanych od **właściwego organu**, Prokuratury Europejskiej (**EPPO**) lub **Eurojustu**, w razie potrzeby w celu wsparcia **toczącego się postępowania przygotowawczego**, bez konieczności wykonywania kategoryzacji osób, których dane dotyczą, jeżeli nie została ona jeszcze przeprowadzona, oraz

---

[27] Zob. na przykład art. 6 dyrektywy (UE) 2016/680 (dyrektywa o ochronie danych w sprawach karnych pośrednio w odniesieniu do właściwych organów); Dz.U. L 119 z 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj; art. 51 rozporządzenia Rady (UE) 2017/1939 (rozporządzenie w sprawie EPPO); Dz.U. L 283 z 31.10.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj; art. 27 ust. 3 rozporządzenia (UE) 2018/1727 („rozporządzenie w sprawie Eurojustu"); Dz.U. L 295 z 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.

wykraczających poza kategorie osób, których dane dotyczą, wymienione w rozporządzeniu w sprawie Europolu. Europol może przetwarzać dane w formie **analizy operacyjnej** lub, w wyjątkowych i należycie uzasadnionych przypadkach, w formie **sprawdzania krzyżowego** mającego na celu wskazanie powiązań lub innych odpowiednich związków. Odstępstwo to miało na celu wyeliminowanie różnic między przepisami odnoszącymi się do kategoryzacji osób, których dane dotyczą, mającymi zastosowanie do Europolu a przepisami mającymi zastosowanie do właściwych organów, Prokuratury Europejskiej i Eurojustu.

4) **Współpraca z osobami trzecimi: art. 26, 26a i 26b rozporządzenia w sprawie Europolu dotyczące wymiany danych osobowych między Europolem a podmiotami prywatnymi**

Przestępcy coraz częściej nadużywają (transgranicznych) usług świadczonych przez podmioty prywatne – internetowych, finansowych i klasycznych usług telekomunikacyjnych. W konsekwencji **podmioty prywatne posiadają dużą ilość danych osobowych istotnych dla postępowań przygotowawczych**. W szczególności internet stworzył przestrzeń publiczną, która faktycznie znajduje się w rękach prywatnych, co utrudnia egzekwowanie przepisów do celów ścigania przestępstw w internecie równie skutecznie jak poza internetem[29].

W tym kontekście **niezbędna** stała się **współpraca między organami ścigania a podmiotami prywatnymi.** Jak określono w europejskiej strategii bezpieczeństwa wewnętrznego **ProtectEU**, zasadnicze znaczenie będzie miało wzmocnienie partnerstw z sektorem prywatnym w celu ułatwienia wymiany informacji[30]. We wspólnej deklaracji w sprawie przyszłości Europolu szefowie policji wezwali również Europol[31], by pełnił rolę „**centralnego punktu dostępu umożliwiającego pozyskiwanie informacji od podmiotów prywatnych**". Charakter tej współpracy obejmuje różne formy: od wymiany informacji i dostarczania komercyjnych danych ze źródeł otwartych po angażowanie się w projekty w dziedzinie badań naukowych i innowacji oraz świadczenie usług wspierających funkcjonowanie przedsiębiorstw[32]. Na przykład w 2025 r. Europol z powodzeniem zakłócił działanie Lumma Stealer – największego na świecie zagrożenia związanego z infostealerami – dzięki współpracy z Microsoftem, który zidentyfikował ponad 394 000 komputerów z systemem Windows na całym świecie zainfekowanych złośliwym oprogramowaniem Lumma[33].

Rozporządzeniem (UE) 2022/991 wprowadzono **dodatkowe możliwości** wymiany danych osobowych przez Europol z podmiotami prywatnymi. Wcześniej Europol mógł otrzymywać dane osobowe od podmiotów prywatnych wyłącznie za pośrednictwem jednostki krajowej Europolu lub za pośrednictwem wcześniej określonych punktów kontaktowych lub organów państw trzecich bądź organizacji międzynarodowych. Cel przetwarzania przez Europol ograniczał się do zidentyfikowania odpowiedniej jednostki krajowej Europolu lub punktu kontaktowego lub organu państwa trzeciego i organizacji międzynarodowej, które mogłyby przejąć odpowiedzialność za daną sprawę.

---

29 SWD(2020) 543 final z dnia 9 grudnia 2020 r., s. 16.

30 Zob. ProtectEU: europejska strategia bezpieczeństwa wewnętrznego, 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" [Współpraca z podmiotami prywatnymi], 31 maja 2023 r., EDOC #1306090v13. Zob. również Milieu Consulting, „Study on the Practice of direct exchanges of personal data between Europol and Private Party" [Badanie dotyczące praktyki bezpośredniej wymiany danych osobowych między Europolem a podmiotami prywatnymi], sprawozdanie końcowe, wrzesień 2020 r.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Więcej przykładów przedstawiono w towarzyszącym dokumencie roboczym służb Komisji.

Zmieniony art. 26 rozporządzenia w sprawie Europolu rozszerzył zadanie Europolu, umożliwiając mu kompleksowe przetwarzanie informacji (w tym danych osobowych) pochodzących od podmiotów prywatnych. Głównym celem przetwarzania pozostało wskazanie odpowiedniej jednostki krajowej Europolu. Europol może jednak obecnie również uzupełniać informacje o własną analizę, aby ułatwić dalsze rozpatrywanie sprawy na szczeblu krajowym.

Oprócz przepisów horyzontalnych zawartych w art. 26 rozporządzenia w sprawie Europolu w art. 26a tego rozporządzenia wprowadzono przepisy dotyczące **sytuacji kryzysowych wywołanych publikacją w internecie**, a w art. 26b odniesiono się do **rozpowszechniania materiałów internetowych przedstawiających niegodziwe traktowanie dzieci w celach seksualnych**. W takich przypadkach Europol może pomagać państwom członkowskim przez przetwarzanie danych osobowych otrzymanych bezpośrednio od podmiotów prywatnych. Europol może również przekazywać dane osobowe podmiotom prywatnym w indywidualnych przypadkach.

Rozporządzeniem (UE) 2022/991 wprowadzono możliwość wykorzystywania infrastruktury Europolu do wymiany informacji między właściwymi organami a podmiotami prywatnymi, a także możliwość zwrócenia się przez Europol do państw członkowskich o uzyskanie przez nie, zgodnie z ich prawem krajowym, danych osobowych od podmiotów prywatnych.

Przepisy te przyjęto z uwzględnieniem innych inicjatyw, takich jak rozporządzenie w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym[34] i akt o usługach cyfrowych[35]. Przewiduje się dalsze środki zwiększające zaangażowanie podmiotów prywatnych w walkę z przestępczością i ułatwiające legalny dostęp do danych, aby zrealizować „ambitny cel zmiany kultury w dziedzinie bezpieczeństwa" (**podejście obejmujące całe społeczeństwo**) określony w europejskiej strategii bezpieczeństwa wewnętrznego **ProtectEU**[36].

5) Wewnętrzny i zewnętrzny nadzór nad przestrzeganiem przez Europol praw podstawowych

W rozporządzeniu (UE) 2022/991 podkreślono spoczywający na Europolu obowiązek poszanowania praw podstawowych, o którym mowa w przepisach określających zadania Europolu i zwiększone powiązane zabezpieczenia, w szczególności za pośrednictwem **wzmocnienia wewnętrznego i zewnętrznego nadzoru nad Agencją**.

W dziedzinie ochrony danych dostosowanie rozporządzenia w sprawie Europolu do zabezpieczeń ochrony danych przewidzianych w rozporządzeniu (UE) 2018/1725 oznaczało wprowadzenie nowych przepisów dotyczących nadzoru ze strony **inspektora ochrony danych** i **Europejskiego Inspektora Ochrony Danych** (EIOD). Na przykład stałym obowiązkiem w przypadku każdego nowego rodzaju przetwarzania stało się przedstawienie oceny skutków dla ochrony danych i uprzednie skonsultowanie się z EIOD. Rozporządzeniem (UE) 2022/991 wprowadzono również nowe kompetencje Europolu w odniesieniu do wniosków o przyznanie praw dostępu. Wcześniej, w przypadku gdy państwa członkowskie były dostawcami danych, za rozpatrywanie wniosków o przyznanie praw dostępu odpowiedzialne były właściwe organy krajowe.

---

[34] Rozporządzenie (UE) 2021/784; Dz.U. L 172 z 17.5.2021, s. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj.

[35] Rozporządzenie (UE) 2022/2065; Dz.U. L 277 z 27.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

[36] Zob. ProtectEU: europejska strategia bezpieczeństwa wewnętrznego, s. 2.

Rozporządzeniem (UE) 2022/991 utworzono również **nowe stanowisko inspektora ds. praw podstawowych** w Europolu, którego zadaniem jest między innymi informowanie dyrektora wykonawczego Europolu o ewentualnych naruszeniach praw podstawowych w trakcie działań Agencji.

Ponadto **wzmocniono nadzór demokratyczny i rozliczalność** dzięki politycznej kontroli działalności Europolu przez **Parlament Europejski i parlamenty narodowe**, zgodnie z art. 88 ust. 2 akapit drugi Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Rozporządzeniem (UE) 2022/991 wzmocniono monitorowanie prowadzone przez **grupę ds. wspólnej kontroli parlamentarnej** (GWKP)[37]. Przewidziano w nim na przykład obowiązkowe konsultacje z GWKP w sprawie projektu programowania wieloletniego i rocznego programu prac Europolu, możliwość kierowania przez GWKP konkretnych niewiążących zaleceń dla Europolu i przedkładania ich Parlamentowi Europejskiemu i parlamentom narodowym, a także ustanowienie forum konsultacyjnego, które, na wniosek, będzie wspierać GWKP w drodze niezależnego doradztwa w kwestiach związanych z prawami podstawowymi.

3. Główne ustalenia oceny

3.1. Aktualna sytuacja w dziedzinie wdrażania pod kątem operacyjnym nowych uprawnień i zadań Europolu w zakresie przetwarzania danych osobowych

Rozporządzenie (UE) 2022/991 **weszło w życie 28 czerwca 2022 r.** Jego wdrażanie pod kątem operacyjnym zależało jednak od różnych środków w zakresie zarządzania, środków technicznych i administracyjnych, a także wymogów operacyjnych, takich jak tworzenie nowych struktur ICT w niektórych przypadkach.

Trzy lata później **prawie wszystkie przepisy** wymienione w art. 68 ust. 3 rozporządzenia (UE) 2022/991 **zostały wdrożone**. Przepisy dotyczące analizy dużych i złożonych zbiorów danych (art. 18 ust. 6a i art. 18a rozporządzenia w sprawie Europolu) oraz współpracy z podmiotami prywatnymi (art. 26, 26a i 26b rozporządzenia w sprawie Europolu) zaczęły obowiązywać od 28 czerwca 2022 r. lub niedługo po tej dacie. Przetwarzanie danych osobowych na potrzeby projektów w dziedzinie badań naukowych i innowacji (art. 18 ust. 2 lit. e) rozporządzenia w sprawie Europolu) rozpoczęło się w 2023 r. po utworzeniu środowiska piaskownicy o nazwie ODIN w celu spełnienia szczególnych wymogów ochrony danych określonych w art. 33a rozporządzenia w sprawie Europolu. Do 29 czerwca 2025 r. nie uruchomiono jeszcze możliwości proponowania państwom członkowskim przez Europol wprowadzania **wpisów informacyjnych do SIS** zgodnie z art. 4 ust. 1 lit. t) rozporządzenia w sprawie Europolu, ponieważ nadal trwa techniczne wdrażanie nowego rodzaju wpisów. Oczekuje się, że wdrożenie nastąpi **w 2026 r.**

3.2. Ocena wpływu operacyjnego nowych uprawnień i zadań Europolu w zakresie przetwarzania danych osobowych na cele Agencji określone w art. 3 rozporządzenia w sprawie Europolu

Jeżeli chodzi o wpływ operacyjny nowych uprawnień i zadań Europolu w zakresie przetwarzania danych osobowych, konsultacje wykazały, że **państwa członkowskie ogólnie pozytywnie postrzegają** ich znaczenie, skuteczność i wartość dodaną oraz wsparcie Europolu dla właściwych organów państw członkowskich w powiązanych obszarach[38].

---

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

38 Zob. dowody przedstawione w sekcji 5 dokumentu roboczego służb Komisji towarzyszącego niniejszemu sprawozdaniu, w szczególności uwagi Europolu i odpowiedzi państw członkowskich na pytania 2, 4 i 5

Uprawnienia do prowadzenia postępowań przygotowawczych objęte niniejszą oceną nie są wykorzystywane w sposób ciągły ani systematyczny do przetwarzania danych do celów monitorowania; niektóre z nich mają nawet charakter wyjątkowy, podczas gdy inne wykorzystuje się w postępowaniach przygotowawczych w sposób bardziej regularny w zależności od potrzeb. **Operacyjne wykorzystanie nowych przepisów** w okresie odniesienia **różniło się znacznie** pod **względem ilościowym**, w zależności od różnych cech technicznych i warunków prawnych związanych z nowymi przepisami.

Europol otrzymał od państw członkowskich **istotną** liczbę **nowych zgłoszeń danych bez kategoryzacji osób, których dane dotyczą**, na podstawie art. 18 ust. 6a rozporządzenia w sprawie Europolu, wynoszącą 653 w 2023 r. i 597 w 2024 r. Nie odnotowano krótkoterminowego wzrostu zgłoszeń danych bez kategoryzacji osób, których dane dotyczą, a liczba przypadków, w których zastosowano art. 18 ust. 6a, utrzymywała się na **stałym** poziomie w porównaniu z równoważnymi przypadkami w okresie przed 28 czerwca 2022 r. Nowe przepisy nie miały też negatywnego wpływu na zaangażowanie państw członkowskich w przeprowadzanie kategoryzacji osób, których dane dotyczą[39]. W latach 2023–2024 udział zgłoszeń danych bez kategoryzacji osób, których dane dotyczą, stanowił **mniej niż 1 % wszystkich zgłoszeń danych** przyjętych przez Europol od państw członkowskich (0,85 % w 2023 r. i 0,71 % w 2024 r.). Od czerwca 2022 r. Europol konsekwentnie dokonywał kategoryzacji osób, których dane dotyczą, w ciągu 18 miesięcy, nie korzystając z przedłużonego okresu wynoszącego 36 miesięcy. Europol wraz z sześcioma państwami członkowskimi podkreślił, że pomimo większej pewności prawa **obciążenie administracyjne pozostaje znaczne** zarówno dla Europolu, jak i dla właściwych organów ze względu na wysiłek wymagany do zapewnienia zgodności z kategoryzacją danych osobowych według indywidualnego udziału w przestępstwie. Wymóg ten jest bardzo rygorystycznie stosowany przez Europol[40].

Europol poinformował, że wymiana informacji z **podmiotami prywatnymi** była nadal nieznaczna w 2023 r., ponieważ zarejestrowano jedynie 26 przypadków wdrożenia art. 26 rozporządzenia w sprawie Europolu (oprócz przypadków objętych aktem o usługach cyfrowych)[41]. W **2024 r.** statystyki wykazały jednak **gwałtowny wzrost do 284** przypadków (prawie +1 000 %) spraw dotyczących współpracy z podmiotami prywatnymi na podstawie art. 26 rozporządzenia w sprawie Europolu. Dotyczyło to w szczególności danych pochodzących od przedsiębiorstw prywatnych do celów prowadzenia postępowań przygotowawczych w sprawie **przestępstw finansowych i gospodarczych**. Europol w znacznym stopniu wykorzystał również art. 26b rozporządzenia w sprawie Europolu w walce z wykorzystywaniem seksualnym dzieci, w której to dziedzinie współpraca z podmiotami prywatnymi była już bardzo znacząca. W obu przypadkach dane obejmują również współpracę, która była możliwa na podstawie poprzednich ram prawnych. Dostępne dane nie ujawniają, w jakim stopniu te nowe przypadki wchodzą w zakres nowych przepisów lub też czy wynikają ze zwiększonego wykorzystania dotychczasowych możliwości.

zawarte w krótkim kwestionariuszu z 2 czerwca 2025 r. w załączniku III do dokumentu roboczego służb Komisji.

39 Jak podkreśliło jedno państwo członkowskie w trakcie konsultacji, „[państwa członkowskie] mogą wyraźnie wyodrębnić rodzaj danych, którymi się zajmują, co może być bardzo ważne w samym postępowaniu przygotowawczym”.

40 Zob. podsekcja 7.1.3 dokumentu roboczego służb Komisji towarzyszącego niniejszemu sprawozdaniu oraz odpowiedzi państw członkowskich na pytanie 9 zawarte w krótkim kwestionariuszu z 2 czerwca 2025 r. w załączniku III do dokumentu roboczego służb Komisji.

41 Europol, sprawozdanie z 2023 r. zgodnie z art. 16 ust. 11 rozporządzenia w sprawie Europolu.

W **2025 r.** Europol przyjął **nową strategię** mającą na celu dalsze zacieśnianie współpracy z podmiotami prywatnymi. Ponadto podjęto działania zmierzające do modernizacji infrastruktury ICT Europolu dostępnej dla właściwych organów na potrzeby wymiany informacji z podmiotami prywatnymi. W **2023 r**. Europol uruchomił platformę **PERCI** (*Plateforme Européenne de Retraits de Contenus illégaux sur Internet*), aby ułatwić wdrażanie rozporządzenia w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, a w przyszłości ewentualnie również art. 18 aktu o usługach cyfrowych, a także unijną platformę umożliwiającą zgłaszanie przypadków niegodziwego traktowania dzieci w celach seksualnych **(EU CARES)**. PERCI nie jest włączona do systemu informacyjnego Europolu[42].

Inne przepisy nie zostały w ogóle wykorzystane (art. 26a rozporządzenia w sprawie Europolu), mimo że zostały wdrożone, **lub** były stosowane **jedynie w wyjątkowych przypadkach** (jeden przypadek w 2024 r., w którym zastosowano art. 18a rozporządzenia w sprawie Europolu, oraz jeden projekt zrealizowany w 2025 r. obejmujący przetwarzanie danych osobowych na podstawie art. 18 ust. 1 lit. t) rozporządzenia w sprawie Europolu, a także trzy nowe projekty w trakcie przygotowań).

Ze względu na ograniczony okres wdrażania pod kątem operacyjnym przepisów wprowadzonych rozporządzeniem (UE) 2022/991 oraz długotrwały charakter postępowań przygotowawczych i sądowych państwa członkowskie nie były w stanie dostarczyć danych ilościowych na temat wpływu tych przepisów pod względem operacyjnym. Zamiast tego przedstawiły one przykłady udanych postępowań przygotowawczych, które pokazują **wymierne korzyści płynące z nowych możliwości dochodzeniowych w rzeczywistych sytuacjach** w odniesieniu do już stosowanych przepisów, a mianowicie przykłady EncroChat, Sky ECC, bałkańskich sieci przestępczych zajmujących się handlem kokainą czy Lumma Stealer.

Europol wraz z ośmioma państwami członkowskimi wskazał również kilka **obszarów wymagających poprawy**, aby zmaksymalizować skuteczne i spójne wykorzystanie nowych ram prawnych oraz zwiększyć rolę Europolu w przyszłości. Istnieją obawy, w szczególności ze strony Europolu, że nadmierna złożoność, fragmentacja i długość przepisów prawnych mogą zniechęcać praktyków lub podmioty prywatne do korzystania z nowych dostępnych instrumentów. Uwagi państw członkowskich dotyczą raczej sposobu, w jaki Europol restrykcyjnie wdraża zabezpieczenia służące ochronie danych pod nadzorem EIOD, co grozi osłabieniem skuteczności i wartości dodanej niektórych przepisów.

3.3. Ocena wpływu nowych uprawnień i zadań Europolu w zakresie przetwarzania danych osobowych na prawa podstawowe

Komisja **nie** znalazła **żadnych** dowodów na **negatywny wpływ na prawa podstawowe** wynikający z operacyjnego wykorzystania nowych uprawnień do przetwarzania danych osobowych w związku z dotychczasowym ograniczonym korzystaniem z nowych uprawnień do przetwarzania danych osobowych.

Poza wdrożeniem szczególnych wymogów w zakresie ochrony danych związanych z nowymi uprawnieniami do przetwarzania danych osobowych Europol stopniowo wprowadzał wszystkie niezbędne środki w celu wdrożenia nowych horyzontalnych mechanizmów nadzoru związanych z prawami podstawowymi.

[42] Rozporządzenie (UE) 2019/818; Dz.U. L 135 z 22.5.2019, s. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

W 2024 r. zarząd Europolu przyjął zmienione przepisy wykonawcze dotyczące inspektora ochrony danych jako jeden z ostatnich niezbędnych aktów wykonawczych związanych z nowym systemem ochrony danych. Zgromadzone dowody wskazują, że Europol i jego zarząd zapewnili również – we współpracy z inspektorem ochrony danych Europolu i EIOD – **rygorystyczne wdrożenie nowych zabezpieczeń ochrony danych** wprowadzonych w 2022 r. Podejście to na pierwszy rzut oka skutecznie zapobiegło wszelkiemu negatywnemu wpływowi lub ingerencjom wynikającym z początkowego wykorzystania nowych uprawnień do przetwarzania danych osobowych w odniesieniu do praw osób fizycznych do prywatności i ochrony danych osobowych. Według państw członkowskich Europol posiada obecnie **solidne ramy prawne ochrony danych**, które zapewniają wystarczające zabezpieczenia na potrzeby ewentualnego zwiększonego korzystania z nowych uprawnień. Siedem państw członkowskich podkreśliło również, że ramy te **ułatwiają przepływ informacji** dzięki zwiększeniu zaufania, chociaż nadal istnieje pole do poprawy. Tylko jedno państwo członkowskie wyraziło negatywną opinię[43].

Oprócz szczególnych **wyzwań** związanych z kategoryzacją osób, których dane dotyczą, Europol wraz z czterema państwami członkowskimi wymienił jako obszary wymagające poprawy koszty i czas związane z **oceną skutków dla ochrony danych** i **uprzednimi konsultacjami** z EIOD, które w praktyce są przeprowadzane domyślnie. Kolejnym wyzwaniem zgłoszonym przez sześć państw członkowskich jest rozpatrywanie przez Europol **wniosków o dostęp osób, których dane dotyczą**, w odniesieniu do których to wniosków Europol jest obecnie właściwy, nawet wtedy, gdy właścicielem danych jest państwo członkowskie.

Pierwszego inspektora ds. praw podstawowych mianowano w grudniu **2022 r.** W ciągu pierwszych dwóch lat kadencji **nie** otrzymał on żadnych skarg ani nie złożył **żadnych skarg** do dyrektora wykonawczego. GWKP nadal ściśle monitorowała działania Europolu i nie wydała żadnych zaleceń od czasu wejścia w życie nowych przepisów. W lutym **2024 r.** Parlament Europejski powołał **forum konsultacyjne ds. praw podstawowych GWKP**.

3.4. Ocena kosztów i korzyści wynikających z nowych uprawnień i zadań Europolu w zakresie przetwarzania danych osobowych

Biorąc pod uwagę wczesny etap wdrażania przepisów wprowadzonych rozporządzeniem (UE) 2022/991 oraz ograniczone doświadczenie z nimi związane, jest **zbyt wcześnie**, aby Komisja wyciągnęła znaczące wnioski na temat nowych przepisów na podstawie **oceny kosztów i korzyści**.

Służby Komisji zebrały od Europolu informacje dotyczące kosztów poniesionych do tej pory w związku z wdrażaniem pod kątem operacyjnym rozporządzenia (UE) 2022/991 w odniesieniu do analizowanych przepisów. Koszty te wyniosły w przybliżeniu **25 mln EUR** (około 5 % całkowitej alokacji dla Europolu[44]) w latach 2022–2025 i obejmowały głównie koszty jednorazowe. Państwa członkowskie nie poniosły do tej pory żadnych istotnych nowych kosztów związanych konkretnie z rozporządzeniem (UE) 2022/991.

Większość kosztów (prawie 17 mln EUR) była związana ze znacznymi inwestycjami w **rozwój nowych struktur ICT**, we wdrażanie przepisów dotyczących badań naukowych i innowacji (piaskownica ODIN) oraz w systemy informacyjne służące wymianie danych

---

[43] Zob. odpowiedzi państw członkowskich na pytanie 9 zawarte w krótkim kwestionariuszu z 2 czerwca 2025 r. w załączniku III do dokumentu roboczego służb Komisji.

[44] W tym samym okresie budżet przydzielony Europolowi wyniósł ogółem około **860 mln EUR** (stopniowo wzrastając z 192 mln EUR w 2022 r. do 241 mln EUR w 2025 r.). Szczegółowe informacje znajdują się w towarzyszącym dokumencie roboczym służb Komisji.

osobowych z podmiotami prywatnymi (PERCI i EU CARES). Koszty **zasobów ludzkich**, zarówno związane z ICT, jak i operacjami, stanowiły około jednej trzeciej całkowitych wydatków (około 8 mln EUR). **Główne koszty stałe w perspektywie długoterminowej** będą stanowić zasoby ludzkie.

Warto zauważyć, że kwota 8 mln EUR, o której mowa powyżej, nie obejmuje kosztów zasobów ludzkich dla Działu Zarządzania Informacjami ani zasobów związanych z (poprzednimi i nowymi) środkami nadzoru, które mają charakter horyzontalny i w przypadku których dezagregacja na poziomie wdrażania przepisów szczegółowych nie jest możliwa. Koszty takich zasobów nie są znikome. Na przykład w 2023 r. oszacowano, że **60 ekwiwalentów pełnego czasu pracy (EPC)** (prawie **5 %** pracowników Europolu) jest zaangażowanych w działania **organów poświadczających/nadzorczych oraz jednostek nadzorczych/doradczych**. Europol przydzielił 25 EPC na działania związane z nadzorem nad ochroną danych i odpowiednimi działaniami na rzecz zapewnienia ochrony danych. Obejmuje to działania następcze w związku z zaleceniami EIOD, a także prace przeprowadzone w kontekście uprzednich konsultacji dotyczących operacyjnego przetwarzania danych. Szesnaście z tych 25 EPC jest zaangażowanych konkretnie w działania związane z wymogami EIOD. Od czerwca 2025 r. Europol posiada w obszarze ochrony danych specjalny zespół składający się z ośmiu pracowników zatrudnionych w pełnym wymiarze czasu pracy, w tym inspektora ochrony danych.

Według Europolu i piętnastu państw członkowskich oczekuje się, że **korzyści** płynące z nowych uprawnień i zadań w zakresie przetwarzania danych osobowych, w szczególności analizowania dużych i złożonych zbiorów danych, a także współpracy z podmiotami prywatnymi, będą znaczące i **przewyższą związane z tym koszty**. Żadne państwo członkowskie nie było innego zdania. W perspektywie długoterminowej można zasadnie oczekiwać pewnego przyrostu wydajności dzięki korzyściom skali i malejącym kosztom krańcowym. Jedno z państw członkowskich podkreśliło, że „ważne jest, aby Europol zapewniał niezbędne zasoby ICT w celu dostarczania i dalszego rozwijania narzędzi służących wdrażaniu nowych możliwości przewidzianych w rozporządzeniu (UE) 2022/991”, co wsparły również dwa inne państwa członkowskie i inne zainteresowane strony[45].

Zdaniem Europolu i pięciu państw członkowskich należy również zająć się ewentualnymi **brakami efektywności** w zakresie wdrażania w **istniejących ramach zarządzania, administracji i ochrony danych**, aby uniknąć osłabienia wpływu operacyjnego nowych zadań związanych z przetwarzaniem danych osobowych przez opóźnienie lub ograniczenie ich wykorzystania. Pięć państw członkowskich zakwestionowało zbyt ostrożne wdrażanie przepisów o ochronie danych przez Europol i jego zarząd pod kierunkiem EIOD. Sugerują one, że elastyczność przyznana przez współprawodawców powinna być odpowiednio wykorzystywana, aby zmaksymalizować skuteczność i wydajność zadań Europolu oraz zapewnić ich adekwatność i długoterminową rentowność.

Ocena metod pracy Europolu i potencjalnych obszarów wymagających uproszczenia wykracza poza zakres sprawozdania, o którym mowa w art. 68 ust. 3 rozporządzenia w sprawie Europolu, i zostanie przeprowadzona w ramach oceny na podstawie art. 68 ust. 1 rozporządzenia w sprawie Europolu.

4. Wnioski i kierunki działań na przyszłość

[45] Zob. dowody przedstawione w sekcji 5 dokumentu roboczego służb Komisji towarzyszącego niniejszemu sprawozdaniu, w szczególności uwagi Europolu i odpowiedzi państw członkowskich na pytania 2, 4 i 5 zawarte w krótkim kwestionariuszu z 2 czerwca 2025 r. w załączniku III do dokumentu roboczego służb Komisji, a także wspólna deklaracja europejskich szefów policji w sprawie przyszłości Europolu.

Podsumowując, zgodnie ze wstępnymi głównymi ustaleniami Komisji państwa członkowskie nadal **popierają rolę odgrywaną przez Europol** w kluczowych obszarach, w których obecnie pomaga on państwom członkowskim w realizacji **nowych zadań związanych z przetwarzaniem danych osobowych**. Aby jednak **zmaksymalizować korzyści** płynące z nowych uprawnień do przetwarzania danych osobowych, zdaniem niektórych zainteresowanych stron konieczne jest **zaradzenie ewentualnym brakom efektywności**, zwłaszcza w istniejących ramach zarządzania, administracji i ochrony danych. Przydatne byłoby również ograniczenie **złożoności i fragmentacji** ram prawnych, które mogą zniechęcać praktyków do korzystania z nowych możliwości.

Ogólnie rzecz biorąc, Komisja nie znalazła dowodów na to, że nowe przepisy wywarły **negatywny wpływ na prawa podstawowe**, w szczególności dzięki solidnym zabezpieczeniom w zakresie ochrony danych, ułatwiającym również przepływ informacji dzięki zwiększeniu zaufania partnerów. Według niektórych państw członkowskich Europol preferował podejście konserwatywne, chociaż należy **odpowiednio wykorzystać elastyczność przyznaną przez współprawodawców** w odniesieniu do kategoryzacji osób, których dane dotyczą, oceny skutków dla ochrony danych, uprzednich konsultacji z inspektorem ochrony danych Europolu oraz rozpatrywania wniosków dotyczących praw dostępu.

Biorąc pod uwagę ogólnie krótki okres wdrażania nowych przepisów o ochronie danych osobowych przewidzianych w rozporządzeniu (UE) 2022/991, zgromadzone dowody nie są jednak rozstrzygające we wszystkich kwestiach.

W europejskiej strategii bezpieczeństwa wewnętrznego **ProtectEU**[46] Komisja zapowiedziała, że zaproponuje ambitny przegląd mandatu Europolu w celu sprostania rosnącym wyzwaniom w zakresie bezpieczeństwa. Zgodnie ze swoimi wytycznymi dotyczącymi lepszego stanowienia prawa[47] Komisja rozpoczęła przygotowania do oceny rozporządzenia w sprawie Europolu i metod pracy Europolu, torując drogę do przedstawienia przez Komisję **w 2026 r. wniosku mającego na celu zwiększenie operacyjności Europolu, jak określono w wytycznych politycznych**[48]. W lipcu 2025 r. Komisja opublikowała zaproszenie do zgłaszania uwag[49] i zleciła przeprowadzenie badania zewnętrznego, aby wesprzeć ocenę rozporządzenia w sprawie Europolu i ocenę skutków nowego wniosku. Ocena rozporządzenia w sprawie Europolu przeprowadzona na potrzeby przygotowania niniejszego sprawozdania ma stanowić wkład w tę ocenę.

---

46 ProtectEU: europejska strategia bezpieczeństwa wewnętrznego, s. 10.

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

48 Ursula von der Leyen, Wytyczne polityczne na następną kadencję Komisji Europejskiej 2024–2029, e6cd4328-673c-4e7a-8683-f63ffb2cf648_pl.

49 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Wspo%C5%82praca-organow-scigania-nowe-rozporzadzenie-w-sprawie-Europolu-wniosek-_pl.