ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 11.12.2025 г.
COM(2025) 752 final

# ДОКЛАД НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

**за оценка на оперативното въздействие от изпълнението на задачите, предвидени в Регламент (ЕС) 2022/991, по-специално в член 4, параграф 1, буква у), член 18, параграф 2, буква д), член 18, параграф 6а и членове 18а, 26, 26а и 26б, по отношение на целите на Европол, както и въздействието на тези задачи върху основните права и свободи, предвидени в Хартата, съгласно член 68, параграф 3 от Регламент (ЕС) 2016/794**

{SWD(2025) 404 final}

## 1. Обхват на оценката

От момента, в който започна да функционира, през 1999 г., **Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол)** играе **централна роля в борбата с тежката трансгранична престъпност и тероризма**, като се превърна в основна движеща сила на сътрудничеството в областта на правоприлагането в Европа. Драстичните промени в областта на сигурността през последните 30 години доведоха до съответни промени в „ДНК-то“ на тежката и организираната престъпност[1]. Държавите членки имат нови оперативни потребности, за да се справят ефективно с възникващите заплахи, като **очакванията им за подкрепа от Европол** също **се промениха**. Поради това мандатът на Европол беше заменян или изменян неколкократно с цел запазване и подобряване на релевантността на Агенцията.

Мандатът на Европол, определен в Регламент (ЕС) 2016/794[2] („Регламентът за Европол“ или „РЕ“), беше изменен последно през 2022 г. с Регламент (ЕС) 2022/991[3] с цел справяне с новите заплахи за сигурността. Регламентът за Европол вече не беше пригоден за използване по предназначение в една нова реалност, в която престъпниците се възползват от предимствата на **цифровата трансформация**, **новите технологии**, **глобализацията** и **мобилността**[4].

**Специфичните цели** на Регламент (ЕС) 2022/991 бяха[5], както следва:

- да се даде възможност за ефективно сътрудничество между **частноправните субекти** и правоприлагащите органи с цел борба със злоупотребите с трансгранични услуги от страна на престъпниците;
- да се даде възможност на правоприлагащите органи да анализират **големи и сложни набори от данни** с цел откриване на трансгранични връзки, при пълно зачитане на **основните права**;
- да се даде възможност на държавите членки да използват **новите технологии** за целите на правоприлагането.

Освен това, с Регламент (ЕС) 2022/991 се внесоха изменения в приложимите по отношение на Европол правила за защита на данните, като целта беше да се поддържа **високо равнище на защита на данните** чрез постигане на баланс между новите правомощия на Агенцията да обработва лични данни и неприкосновеността на личния живот и защитата на личните данни на физическите лица. С него правилата за защита на данните, приложими по отношение на Европол, до голяма степен се уеднаквиха с правилата, приложими по отношение на други агенции и органи на ЕС в областта на правосъдието и вътрешните работи (ПВР) съгласно Глава IX от Регламент (ЕС) [2018/1725] („Регламента относно защитата на личните данни от институциите, органите, службите и агенциите на Съюза“ или „РЗЛД“), както и с тези, приложими по отношение на правоприлагащите органи на държавите членки („компетентните органи“) съгласно националното им законодателство за транспониране

---

1 Европол, Оценка на заплахата от тежката и организираната престъпност в ЕС (SOCTA) за 2025 г. – Променящата се „ДНК“ на тежката и организираната престъпност, достъпна онлайн на адрес: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf („EU SOCTA 2025“). Вж. също Оценка на заплахите в митниците (CTA) за 2025 г., достъпна онлайн на адрес: https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

2 ОВ L 135, 24.5.2016 г., стр. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj.

3 ОВ L 169, 27.6.2022 г., стр. 1., ELI: http://data.europa.eu/eli/reg/2022/991/oj.

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

5 *Пак там.*

на Директива (ЕС) 2016/680 („Директивата относно правоприлагането“),[6] с цел **улесняване на информационния поток**.

Настоящият доклад е приет в съответствие със задължението на Комисията по член 68, параграф 3 от РЕ да оцени[7] и анализира оперативното въздействие от изпълнението на задачите на Европол, предвидени в Регламент (ЕС) 2022/991, три години след влизането му в сила. Съгласно възложения ѝ от съзаконодателите мандат Комисията: първо, оцени и анализира **оперативното въздействие** на някои от новите правила за обработването на лични данни във връзка с целите на Европол, посочени в член 3 от РЕ (а именно: да подкрепя и засилва действията на компетентните органи на държавите членки и взаимното им сътрудничество за предотвратяване и борба с престъпленията, попадащи в обхвата на мандата на Европол); второ, оцени въздействието на тези правила върху **основните права и свободи** („основните права“), залегнали в Хартата[8], и трето, извърши **анализ на разходите и ползите** от съответните задачи за обработване на данни.

За да подготвят прегледа, службите на Комисията събраха информация и обратна връзка от различни източници и проведоха ad hoc консултации с Европол и държавите членки. В придружаващия **работен документ на службите** се съдържа подробно описание на общия контекст и методологията на прегледа, както и изчерпателен отчет за източниците на данни и консултациите, потвърждаващи основните констатации, обобщени в настоящия доклад.

## 2. Общ контекст

В съответствие с член 68, параграф 3 от РЕ настоящият доклад на Комисията обхваща избрани разпоредби на Регламент (ЕС) 2022/991 с акцент върху пет ключови аспекта от работата на Европол.

### (1) Външно измерение: Член 4, параграф 1, буква у) от РЕ за въвеждане на информационни сигнали относно граждани на трети държави в Шенгенската информационна система (ШИС) по предложение на Европол

Предвид **глобалния характер на тежката престъпност и тероризма** информацията за лица, извършили или заподозрени в извършването на такива престъпления, съхранявана от трети държави и международни организации, придобива все по-голямо значение за вътрешната сигурност на ЕС. Следователно външното измерение на сътрудничеството на ЕС в областта на правоприлагането става изключително важно за държавите членки, както и **ролята на Европол в оказването на подкрепа на държавите членки в партньорствата им с трети държави** или със субекти, установени в тези държави. **В бъдеще ще бъдат необходими** допълнителни усилия за укрепване на световната сигурност[9].

Регламент (ЕС) 2022/991 вече въведе съществени изменения в Регламента за Европол с цел засилване на **външното измерение на дейностите на Европол**, по-специално като

---

6 ОВ L 119, 4.5.2016 г., стр. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

7 Тази оценка, извършена в съответствие с член 68, параграф 3 от РЕ, не е оценката, която ще трябва да се извърши съгласно Насоките за по-добро регулиране с оглед на евентуално предложение за преразглеждане на Регламента за Европол. Вж. също раздел 4 по-долу.

8 Харта на основните права на Европейския съюз, ОВ C 326, 26.10.2012 г., стр. 391,ELI: http://data.europa.eu/eli/treaty/char_2012/oj.

9 Вж. ProtectEU: европейска стратегия за вътрешна сигурност, COM(2025) 148 final от 1 април 2025 г., https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52025DC0148.

улесни обмена на информация с трети държави[10] и задължи Европол да включи стратегия за отношенията с трети държави и международни организации в своята многогодишна програма и в годишните си работни програми[11].

**Член 4, параграф 1, буква у от РЕ** възложи на Европол нова задача: да подкрепя държавите членки при обработването на данни относно лица, замесени в тероризъм или тежка престъпност, предоставени от трети държави или международни организации. Това включва възможността **да предлага на държавите членки евентуално въвеждане в Шенгенската информационна система (ШИС) на информационни сигнали относно граждани на трети държави в интерес на Съюза**. Тази нова категория информационни сигнали беше въведена през 2022 г.[12] вследствие на изменение на Регламент (ЕС) 2018/1862 за използването на ШИС в областта на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси[13].

Някои информации, особено когато засегнатото лице не е гражданин на ЕС и когато няма връзка с национален случай, третата държава споделя само с Европол, която ги обработва и споделя резултатите от анализа си с всички държави членки. Целта на новите разпоредби беше **да се постигне максимално използване на информацията**, изпратена на Европол от трети държави, като бъде направена по-достъпна, отколкото би била, ако до нея можеше да се стига само чрез системата на самата Европол. Те допълват други мерки, като Европейския портал за търсене (ESP) и рамката за оперативна съвместимост[14] между информационните системи за сигурност и за управление на границите и миграцията на ЕС, чрез преодоляване на структурните недостатъци, свързани с тези системи, които възпрепятстват работата на националните органи, и по-специално на граничните служители.

**ШИС** се счита за **ключов допълнителен канал за разпространение**: тя е най-широко използваната база данни в Европа в областта на правоприлагането, граничния контрол и миграцията. През 2024 г. в ШИС са извършени над 15 милиарда търсения спрямо приблизително 14 милиона в информационната система на Европол (EIS) и по-малко от 3 милиарда (в световен мащаб) в 19-те бази данни на Интерпол, които са другите две водещи информационни системи за компетентните органи[15].

**(2) Иновации: Член 18, параграф 2, буква д) и член 33а от РЕ относно обработването на лични данни от Европол за иновационни и научноизследователски проекти**

---

10 Вж. например член 25, параграф 4а от РЕ, в който на Европол се предоставя възможността да предава данни на трети държави след извършена самооценка на всички обстоятелства около предаването на тези данни, водеща до заключението, че са налице подходящи гаранции за тяхната защита, и член 25, параграф 5 от РЕ, в който се разширява обхватът на изключителните случаи, при които Европол може да предава ad hoc (категории) данни на трети държави и международни организации в надлежно обосновани случаи.

11 Член 12, параграф 2 от РЕ.

12 Регламент (ЕС) 2022/1190; ОВ L 185, 12.7.2022 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 Регламент (ЕС) 2018/1862; ОВ L 312, 7.12.2018 г., стр. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 Регламент (ЕС) 2019/818; ОВ L 135, 22.5.2019 г., стр. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

15 Годишен доклад на eu-LISA относно ШИС, 2024 г., достъпен онлайн на адрес https://www.eulisa.europa.eu/sites/default/files/documents/sis-annual-report-2024.pdf, Европол, Консолидиран годишен доклад за дейността (CAAR), 2024 г., достъпен онлайн на адрес https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF, и https://www.interpol.int/How-we-work/Databases.

**Технологичното развитие** е огромна възможност, но и значително предизвикателство за вътрешната сигурност на ЕС[16], и оказа толкова голямо въздействие върху престъпността, че промени дълбоката същност, „ДНК“ на заплахите, свързани с тежката и организираната престъпност[17]. Престъпниците бързо внедряват новите технологии в своите операции, като създават нови бизнес модели и усъвършенстват тактиките си. Едновременно с това, този напредък предоставя на **правоприлагащите органи безпрецедентни възможности да подобрят своя капацитет**. Ето защо научните изследвания и иновациите имат ключова роля за вътрешната сигурност, с това че се разработват решения, позволяващи да се противодейства на възникващите заплахи и да не се изостава от бързо развиващите се форми и *начини на работа* на престъпните мрежи, включително тези, които произтичат от злоупотребата с технологии. Съюзът е инвестирал и ще продължава да инвестира в разработването на иновативни инструменти чрез финансирани от ЕС изследвания и иновации в сферата на сигурността, съгласно **ProtectEU**, европейската стратегия за вътрешна сигурност[18].

Създадена в края на 2019 г. с мандата на министрите на правосъдието и вътрешните работи на държавите членки на ЕС, **Лабораторията за иновации на Европол (ЛИЕ)**[19] има за цел да насочва ангажиментите на Европол за иновации в областта на правоприлагането. Регламент (ЕС) 2022/991 въведе съществени изменения в Регламента за Европол, насочени към засилване на мандата за иновации на Европол, така че да се подкрепи потенциалът на ЛИЕ, като едновременно с това се насърчат полезните взаимодействия с други научноизследователски и иновационни дейности на равнището на ЕС, включително по-специално в Комисията, в рамките на **Иновационния център на ЕС** за вътрешна сигурност[20].

Член 18, параграф 2 от РЕ относно целите на дейностите по обработване на информацията беше изменен, за да се даде възможност на Европол да **обработва лични данни от оперативен характер** също и **за научноизследователски и иновационни проекти**. Счита се, че наличието на висококачествени набори от данни, които позволяват валидността на новите инструменти да се тества емпирично, е ключово предварително условие за разработването на технологии. Обратно, при тестване на ненадеждни или пристрастни набори от данни може да се стигне до създаване на негодни технологии.[21]

Специални гаранции за защита на данните при такова обработване са заложени в член 18, параграф 3а, член 30, параграфи 2 и 3 и **член 33а от РЕ**. В последния член се изисква създаването на **тестова среда**, като се посочва, че всички лични данни, обработвани в контекста на даден проект, трябва да се копират временно в отделна, изолирана и защитена среда за обработване на данни в рамките на Европол, за да бъдат използвани единствено за този проект.

---

16 Европол, Оценка на заплахата от организираната престъпност в интернет (IOCTA), 2024 т., достъпна онлайн на адрес Оценка на заплахата от организираната престъпност в интернет (IOCTA), 2024 г. Европол.

17 Европол, EU SOCTA 2025 г., стр. 19.

18 COM(2025) 148 final от 1 април 2025 г., https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52025DC0148, стр. 9.

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

20 Вж. по-специално член 4, параграф 1, букви х) и ц) от РЕ.

21 SWD(2020) 543 final от 9 декември 2020 г., стр. 29.

**(3) <u>Наказателни разследвания</u>: Член 18, параграф 6а и член 18а от РЕ относно условията за обработване на лични данни, получени без да е извършено категоризиране на субектите на данни (КСД)**

В качеството си на **информационен център на ЕС по въпросите, свързани с престъпността,** Европол не само улеснява събирането и обмена на информация, а помага за **повишаването на ефективността на разследванията чрез усъвършенстван анализ на данни** и чрез установяване на трансгранични връзки между престъпления и престъпни мрежи, които не могат да бъдат забелязани на национално равнище. Тези възможности подкрепят държавите членки, като обогатяват информацията, налична за наказателните им разследвания.

С разширеното и интензивно използване на технологиите **големите и сложни набори от данни навлязоха във всички аспекти на живота**, включително престъпността.[22] Разследванията, свързани с организираната престъпност или тероризма, вече се сблъскват с предизвикателствата, свързани с анализа на големи обеми електронно съхранявани данни, които често се измерват в терабайти, в това число конфискувани в хода на разследванията аудио-, видео- и машинногенерирани данни. Например, в съвместното разследване, целящо разбиването на мрежата EncroChat[23], следователите са анализирали милиони съобщения, които престъпниците са си изпращали, за да планират тежки престъпления. В този контекст, наличността на необходимите инструменти, експертен опит и ресурси в областта на информационните и комуникационните технологии (ИКТ) за целите на анализа на големи и сложни набори от данни (на технически жаргон „големи информационни масиви“[24]) е от ключово значение за правоприлагащите и съдебните органи.

Тъй като в Регламента за Европол, който беше приет през 2016 г., не бяха поставени конкретни ограничения, що се отнася до анализа на големите информационни масиви, в него липсваха структурирани разпоредби, които да определят условията за анализирането на този вид данни. **Най-критичната точка** беше **изискването за КСД**. КСД се отнася до необходимостта наборите от данни да се подлагат на скрининг, така че личните данни да се разпределят в различните категории, изчерпателно изброени в приложение II, части А и Б към Регламента за Европол, преди да се пристъпи към действителното им обработване за целите на разследването, включително преди кръстосаната проверка на данните за откриване на връзки или за извършване на анализи от стратегическо или тематично естество или на оперативни анализи[25]. Съответните категории са свързани с различните видове участие в наказателни разследвания, включително: i) заподозрени лица, потенциални бъдещи нарушители; или ii) лица за контакт, сътрудници, жертви, свидетели и информатори, свързани с престъпна дейност.

---

22 Европол, EU SOCTA, 2025 г., *в целия текст*.

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 ЕНОЗД, Становище 7/2015, стр. 7, достъпно на адрес https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf. „Общо казано, свързващият елемент в различните налични определения е, че „**големите информационни масиви**“ представляват начин да се комбинират огромни обеми информация от различни източници и да се анализират чрез използване на по-сложни алгоритми за целите на вземането на информирани решения. Големите информационни масиви разчитат не само на нарастващите технологични възможности, подкрепящи събирането и съхранението на големи количества данни, но и на възможностите да се анализират, разбират и извличат ползи от пълната стойност на данните (по-специално чрез използване на приложения за анализ).

25 Виж член 18, параграф 2 от РЕ.

По принцип Европол не може да обработва, нито дори да съхранява лични данни на лица, които не попадат в нито една от тези категории.

Доставчиците на данни, като **държавите членки** или **органите и агенциите на ЕС, обикновено** вече са извършили КСД преди да предадат личните данни на Европол[26]. Съгласно законодателството на ЕС всички те са длъжни да извършват КСД за собствените си обработване и разследвания, независимо от предаването на данни на Европол, и въз основа на правила, които са равностойни, но не и еднакви с тези на Европол[27]. За големи и сложни набори от данни обаче ръчното предварително обработване изисква ресурси и време. Анализирането на данните в един-единствен мобилен телефон по полуавтоматичен начин може да отнеме до три дни, а в хода на дадено разследване понякога могат да се изземат стотици мобилни телефони. КСД **за големи информационни масиви не винаги** е **възможно,** предвид огромния обем набори от данни, начина, по който те са (не са) структурирани, липсата на ресурси или необходимостта от твърде много **ръчен труд**. На практика единствената възможност е данните първо да бъдат анализирани в по-голяма дълбочина от оперативна гледна точка или да бъдат установени връзки, пак по полуавтоматичен начин, чрез кръстосана проверка на наличните данни.

В Регламент (ЕС) 2022/991 се изясняват условията за КСД, необходими за гарантирането на **правна сигурност** при обработването на големи и сложни набори от данни. Европол и Европейският надзорен орган по защита на данните (ЕНОЗД) тълкуват по различен начин буквата и духа на Регламента за Европол, що се отнася до приложимия срок за съхранение на данните. Според Европол този срок следва да бъде три години; а според ЕНОЗД – шест месеца[28]. Необходими бяха също така нови разпоредби, за да се осигури **допълнителна гъвкавост** чрез постигане на подходящ баланс между защитата на данните и аспектите, свързани със сигурността.

Член 18, параграф 5а от РЕ във връзка с член 73 от РЗЛД първо внася допълнителни пояснения относно общия принцип на КСД съгласно член 18, параграф 2 и приложение II. Европол е натоварена със задачата, когато е приложимо и доколкото е възможно, да извършва ясно разпределяне на **личните данни в конкретна категория субекти на данни**. На практика, Европол по принцип следва да установи точната роля в престъпната дейност (например дали лицето е заподозряно лице, жертва или само свидетел) за всяко отделно лице, чиито лични данни ще бъдат обработвани, а не в съвкупен вид за всички лица в даден файл с данни, който подлежи на обработване, или в част от него (например като установи, че всички споменати лица са замесени в престъпна дейност, попадаща в обхвата на нейния мандат, въз основа на проверка на общите обстоятелства, наложили създаването на файла с данни), преди личните данни да могат да бъдат обработвани.

Член 18, параграф 6а от РЕ изрично позволява обработването на лични данни, получени без КСД, за срок до **18 месеца**, който може да бъде удължен до 36 месеца в обосновани

---

26 Държавите членки предават данни на Европол през нейното мрежово приложение за защитен обмен на информация (SIENA), в което КСД е включено като задължително поле.

27 Вж. например член 6 от Директива (ЕС) 2016/680 („Директивата относно правоприлагането“, що се отнася до непряко компетентните органи); ОВ L 119, 4.5.2016 г., стр. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj; Член 51 от Регламент (ЕС) 2017/1939 на Съвета („Регламентът за създаване на Европейска прокуратура“); ОВ L 283, 31.10.2017 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj; Член 27, параграф 3 от Регламент (ЕС) 2018/1727 („Регламентът относно Евроюст“); ОВ L 295, 21.11.2018 г., стр. 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.

случаи, единствено с **цел попълване на КСД**. Член 18, параграф 6а от РЕ не препраща конкретно към големи и сложни набори от данни, а изисква, по-общо, тестване в случай на „**изрична необходимост**“.

В член 18а от РЕ е предвидена дерогация, като на Европол се позволява да обработва лични данни, получени от **компетентен орган,** Европейската прокуратура (**ЕРРО**) или **Евроюст**, когато това е необходимо с цел оказване на подкрепа по **текущо наказателно разследване**, без да трябва да се извършва КСД, ако такова все още не е направено, и извън категориите субекти на данни, изброени в Регламента за Европол. Европол може да обработва данните чрез **оперативен анализ** или — в изключителни и надлежно обосновани случаи – чрез **кръстосана проверка**, за да установява връзки или други относими отношения. Тази дерогация е замислена с цел преодоляване на различията между правилата относно КСД, които са приложими по отношение на Европол, и правилата, приложими по отношение на компетентните органи, Европейската прокуратура и Евроюст.

**(4) Сътрудничество с трети държави: Членове 26, 26а и 26б от РЕ относно обмена на лични данни между Европол и частноправни субекти**

Престъпниците все повече злоупотребяват с (трансграничните) услуги на частноправни субекти – основани на интернет, финансови и класически телекомуникационни услуги. Поради това **частноправните субекти притежават голямо количество лични данни от значение за наказателните разследвания**. По-специално, интернет създаде публично пространство, което на практика е в частни ръце, а това затруднява онлайн изпълнението на правилата за целите на правоприлагането, като го прави по-малко ефективно от това във физическия свят.[29]

В този контекст **сътрудничеството между правоприлагащите органи и частноправните субекти** стана **задължително.** Както е посочено в **ProtectEU**, европейската стратегия за вътрешна сигурност, от съществено значение ще е да се усилят партньорствата с частния сектор, за да се улесни обменът на информация[30]. В съвместното си изявление относно бъдещето на Европол[31] полицейските началници призоваха също така тя да служи като „**жизненоважен портал за получаване на информация от частноправни субекти**“. По естеството си това сътрудничество включва диапазона от споделяне на информация и предоставяне на търговски данни с отворен код до участие в научноизследователски и иновационни проекти и предоставяне на услуги, подпомагащи функционирането на корпорациите.[32] Например през 2025 г. Европол успешно разби Lumma Stealer, най-значимата световна заплаха, свързана с кражба на информация, чрез сътрудничество с Microsoft, което идентифицира над 394 000 Windows компютъра в цял свят, заразени със зловредния софтуер Lumma[33].

С Регламент (ЕС) 2022/991 бяха въведени **допълнителни възможности** за Европол да обменя лични данни с частноправни субекти. Преди това Европол можеше да получава

---

29 SWD(2020) 543 final от 9 декември 2020 г., стр. 16—17.

30 Вж. ProtectEU: европейска стратегия за вътрешна сигурност, стр. 6.

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

32 Европол, Сътрудничество с частноправни субекти, 31 май 2023 г., EDOC #1306090v13. Вж. също Milieu Consulting, Study on the Practice of direct exchanges with of personal data between Europol and Private Parties, Final Report (Проучване на практиката за директен обмен на лични данни между Европол и частноправни субекти, окончателен доклад), септември 2020 г.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Още примери са дадени в придружаващия работен документ на службите на Комисията.

лични данни от частноправни субекти само посредством дадено национално звено на Европол (НЗЕ) или през предварително установени точки за контакт или органи на трети държави или международни организации. Целта на обработването на Европол се свеждаше до идентифициране на съответното НЗЕ или на точката за контакт или органа на третата държава или международната организация, които биха могли да поемат отговорност за дадения случай.

**Измененият член 26 от РЕ разшири задачата на Европол,** като я упълномощи да обработва всеобхватно информацията (включително личните данни), получена от частноправни субекти. Основната цел на обработването остава идентифицирането на съответното национално звено на Европол (НЗЕ). Европол обаче може също така да допълва информацията със собствен анализ, за да улесни по-нататъшното обработване на даден случай на национално равнище.

В допълнение към хоризонталните разпоредби на член 26 от РЕ, член 26а от РЕ въвежда правила за справяне с **онлайн кризисни ситуации**, а член 26б се занимава с **онлайн разпространението на материали, съдържащи сексуално насилие над деца**. В тези случаи Европол може да съдейства на държавите членки, като обработва лични данни, получени пряко от частноправни субекти. Европол може също така да изпраща лични данни на частноправни субекти, въз основа на преценка на всеки отделен случай.

Регламент (ЕС) 2022/991 позволи инфраструктурата на Европол да се използва за обмен на информация между компетентните органи и частноправни субекти, и упълномощи Европол да иска държавите членки да получават — в съответствие с националното им законодателство — лични данни от частноправни субекти.

Тези разпоредби бяха приети съвместно с други инициативи, като Регламента относно терористичното съдържание онлайн (ТСО)[34] и Акта за цифровите услуги (АЦУ)[35]. Предвидени са допълнителни мерки, които да засилят участието на частноправните субекти в борбата с престъпността и да улеснят законния достъп до данни, като целта е да се осъществи „амбицията за промяна на културата в областта на сигурността“ (**подход, засягащ обществото като цяло**) съгласно **ProtectEU**, европейската стратегия за вътрешна сигурност[36].

### (5) Вътрешен и външен контрол на спазването на основните права от страна на Европол

Регламент (ЕС) 2022/991 акцентира върху задължението на Европол да зачита основните права чрез разпоредбите, в които се определят нейните задачи, и укрепва свързаните с тях гаранции, по-специално като **засилва вътрешния и външния контрол на Агенцията**.

В областта на защитата на данните, привеждането на Регламента за Европол в съответствие с гаранциите за защита на данните съгласно РЗЛД предполагаше въвеждане на нови правила относно контрола, осъществяван от **длъжностното лице по защита на данните** (ДЛЗД) и от **Европейския надзорен орган по защита на данните** (ЕНОЗД). Например, задължението за предоставяне на оценка на въздействието върху защитата на данните (ОВЗД) и за предварителна консултация с ЕНОЗД вече се изпълняват систематично за всеки нов вид обработване. Също така с Регламент (ЕС) 2022/991 беше въведена нова компетентност на Европол относно исканията за получаване на право на достъп. Преди това националните компетентни

[34] Регламент (ЕС) 2021/784; ОВ L 172, 17.5.2021 г., стр. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj.
[35] Регламент (ЕС) 2022/2065; ОВ L 277, 27.10.2022 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.
[36] Вж. ProtectEU: европейска стратегия за вътрешна сигурност, стр. 2.

органи бяха отговорни за обработването на исканията за получаване на право на достъп, ако държавите членки бяха доставчиците на данни.

С Регламент (ЕС) 2022/991 беше създадена **нова позиция към Европол — служител по въпросите на основните права** (СОП) — който трябва, наред с другото, да уведомява изпълнителния директор на Европол за евентуални нарушения на основните права в хода на дейностите на Агенцията.

Освен това **демократичният контрол и отчетността** бяха **засилени** чрез политическото наблюдение на дейностите на Европол от **Европейския парламент и националните парламенти**, предвидено в член 88, параграф 2, втора алинея от Договора за функционирането на Европейския съюз (ДФЕС). Регламент (ЕС) 2022/991 засили наблюдението от страна на **Съвместната група за парламентарен контрол** (СГПК)[37]. Например, в него се предвиждаше задължителна консултация със СГПК относно проекта на многогодишната програма и годишната работна програма на Европол, възможността СГПК да отправя конкретни препоръки без задължителен характер до Европол и да ги представя на Европейския парламент и на националните парламенти, както и създаването на консултативен форум, който да съдейства на СГПК при поискване, като предоставя независими консултации по въпроси, свързани с основните права.

## 3. Основни констатации от оценката

### *3.1. Актуално състояние на оперативното изпълнение от страна на Европол на новите правомощия и задачи за обработване на лични данни*

Регламент (ЕС) 2022/991 влезе **в сила на 28 юни 2022 г.** Оперативното му изпълнение обаче зависеше от различни управленски, технически и административни мерки, както и от оперативни изисквания, като създаване на нови ИКТ структури в някои случаи.

Три години по-късно **почти всички разпоредби**, изброени в член 68, параграф 3 от Регламент (ЕС) 2022/991, **вече се изпълняват**. Разпоредбите относно анализа на големи и сложни набори от данни (член 18, параграф 6а и член 18а от РЕ) и сътрудничеството с частноправни субекти (членове 26, 26а и 26б от РЕ) започнаха да се прилагат, считано от 28 юни 2022 г. или малко след това. Обработването на лични данни за научноизследователски и иновационни проекти (член 18, параграф 2, буква д) от РЕ) започна през 2023 г., след като беше създадена тестова среда, наречена ODIN, с цел постигане на съответствие със специфичните изисквания за защита на данните съгласно член 33а от РЕ. Към 29 юни 2025 г. възможността Европол да предлага на държавите членки **информационни сигнали в ШИС** в съответствие с член 4, параграф 1, буква у) от РЕ все още не е налична, тъй като техническото въвеждане на новия вид сигнали не е приключило. Влизането в действие е **предвидено за 2026 г.**.

### *3.2. Оценка на оперативното въздействие на новите правомощия и задачи на Европол за обработване на лични данни върху целите на Агенцията съгласно член 3 от РЕ*

Що се отнася до оперативното въздействие на новите правомощия и задачи на Европол за обработване на лични данни, консултацията показа, че **държавите членки като цяло оценяват положително** тяхната релевантност, ефективност и добавена стойност, както

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

и подкрепата, която Европол оказва на компетентните им органи в съответните области[38].

Правомощията за разследване, попадащи в настоящата оценка, не се използват постоянно или систематично за обработване на данни с цел наблюдение; някои от тях дори се задействат само по изключение, а други — по-често, при възникнала необходимост в хода на разследвания. **Оперативното използване на новите разпоредби** през референтния период **е доста различно** в **количествено отношение,** в зависимост от различните технически характеристики и от правните условия, свързани с тях.

Европол е получила **нов информационен принос без КСД** от държавите членки съгласно член 18, параграф 6а от РЕ, който не е пренебрежимо малък, а именно 653 през 2023 г. и 597 през 2024 г. Краткосрочно увеличение на информацията без КСД не се наблюдава, като броят на случаите на прилагане на член 18, параграф 6а е останал **стабилен** спрямо еквивалентните случаи за периода преди 28 юни 2022 г. Новите разпоредби не са оказали отрицателно въздействие върху ангажимента на държавите членки да извършват КСД[39]. Между 2023 и 2024 г. делът на информацията без КСД е възлизал на **по-малко от 1 % от всички данни**, които Европол е приела от държавите членки (0,85 % през 2023 г. и 0,71 % през 2024 г.). След юни 2022 г. Европол систематично завършва КСД в рамките на 18 месеца, без да използва удължения 36-месечен срок. Европол и шест държави членки изтъкнаха, че макар правната сигурност да е подобрена, **административната тежест остава значителна** както за Европол, така и за компетентните органи поради усилията, необходими за постигане на съответствие с категоризацията на личните данни според индивидуалното участие в престъплението. Това изискване се изпълнява много стриктно от Европол[40].

Европол докладва, че обменът на информация с **частноправни субекти** през 2023 г. е бил все още незначителен, като регистрираните случаи на прилагане на член 26 от РЕ са само 26 (в допълнение към случаите, попадащи в обхвата на Акта за цифровите услуги)[41]. През **2024 г.** обаче статистиката показа **рязко увеличение до 284** (почти +1 000 %) случая на сътрудничество с частноправни субекти съгласно член 26 от РЕ. Това се отнася по-специално за данни от частни предприятия за разследване на **финансови и икономически престъпления**. Европол е използвала доста активно и член 26б от РЕ в борбата срещу сексуалната експлоатация на деца (СЕД), където сътрудничеството с частноправни субекти вече беше значително. И в двата случая данните включват също и сътрудничеството, станало възможно по силата на предишната правна рамка. От наличните данни не става ясно доколко тези нови случаи се дължат на новите разпоредби и доколко на нарастващо използване на съществуващите възможности.

През **2025 г.** Европол прие **нова стратегия** за по-нататъшно засилване на сътрудничеството с частноправни субекти. Освен това бяха предприети мерки за модернизиране на ИКТ инфраструктурата на Европол, до която компетентните органи

---

38 Вж. данните, представени в раздел 5 от работния документ на службите, приложен към настоящия доклад, и по-специално данните на Европол и отговорите на държавите членки на въпроси 2, 4 и 5 от краткия въпросник от 2 юни 2025 г. в приложение III към работния документ на службите.

39 Както една държава членка подчерта по време на консултацията „[държавите членки] могат ясно да разграничат с какъв вид данни работят, което може да бъде много важно в самото разследване“.

40 Вж. подраздел 7.1.3 от работния документ на службите, приложен към настоящия доклад, и отговорите на държавите членки на въпрос 9 от краткия въпросник от 2 юни 2025 г. в приложение III към работния документ на службите.

41 Европол, Доклад съгласно член 16, параграф 11 от РЕ за 2023 г.

имат достъп за целите на обмена на информация с частноправни субекти. През **2023 г.** Европол инициира създаването на *европейската платформа за премахване на незаконно онлайн съдържание* (*Plateforme Européenne de Retraits de Contenus Illégaux sur Internet* (**PERCI**), с цел да се улесни прилагането на Регламента относно ТСО, а в бъдеще евентуално и на член 18 от Акта за цифровите услуги, както и *референтната служба на ЕС за борба с насилието над деца* **(EU CARES)**. PERCI не е включена в информационната система на Европол (EIS)[42].

**Други разпоредби изобщо** не бяха **използвани** (член 26а от РЕ), въпреки че с тях може да се работи, **или** бяха прилагани **само по изключение** (един-единствен случай на използване на член 18а от РЕ през 2024 г. и един проект, осъществен чрез обработване на лични данни съгласно член 18, параграф 1, буква у) от РЕ през 2025 г., като вече има три нови проекта в процес на разработка).

Поради ограничения период за оперативно изпълнение на разпоредбите, въведени с Регламент (ЕС) 2022/991, и продължителността на наказателните разследвания и съдебните производства държавите членки не можаха да предоставят количествени данни за въздействието на тези разпоредби в оперативно отношение. Вместо това те представиха някои примери за успешни разследвания, които илюстрират **осезаемите ползи от новите възможности за разследване в реални ситуации** за разпоредбите, които вече се използват, а именно по-специално EncroChat, Sky ECC, базирани на Балканите престъпни мрежи, участващи в трафик на кокаин, или Lumma Stealer.

Европол и осем държави членки посочиха също така няколко **области за подобрение** с цел максимално ефикасно и съгласувано използване на новата правна рамка и засилване на ролята на Европол в бъдеще. Съществуват опасения, особено от страна на Европол, че прекомерните сложност, фрагментираност и дължина на правните разпоредби могат да възпрат практикуващите юристи или частноправните субекти от използването на новите налични инструменти. Коментарите на държавите членки засягат по-скоро рестриктивния начин, по който Европол прилага гаранциите за защита на данните под контрола на ЕНОЗД и който рискува да подкопае ефективността и добавената стойност на някои разпоредби.

### *3.3. Оценка на въздействието на новите правомощия и задачи на Европол за обработване на лични данни върху основните права*

Комисията **не** откри **никакви** данни за **отрицателно въздействие върху основните права**, произтичащо от оперативното използване на новите правомощия за обработване на лични данни от ограниченото досега използване на новите правомощия за обработване на лични данни.

Освен че приложи специфичните изисквания за защита на данните, свързани с новите правомощия за обработване на лични данни, Европол постепенно предприе всички необходими мерки за прилагане на новите хоризонтални механизми за контрол, имащи отношение към основните права.

През 2024 г. управителният съвет на Европол прие преработените правила за изпълнение, отнасящи се до ДЛЗД, като един от последните необходими актове за изпълнение във връзка с новия режим за защита на данните. Съгласно събраните данни Европол и неговият управителен съвет, в сътрудничество с ДЛЗД на Европол и ЕНОЗД, **са осигурили също така стриктно изпълнение на новите гаранции за защита на данните**, въведени през 2022 г. Този подход prima facie ефективно е предотвратил

[42] Регламент (ЕС) 2019/818; ОВ L 135, 22.5.2019 г., стр. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

всякакво отрицателно въздействие или намеса от първоначалното използване на новите правомощия за обработване на лични данни върху правата на физическите лица на неприкосновеност на личния живот и защита на личните данни. Според държавите членки към момента Европол разполага със **стабилна правна рамка за защита на данните**, която осигурява достатъчна защита при потенциално засилено използване на новите ѝ правомощия. Седем държави членки подчертаха още, че тази рамка **улеснява информационния поток,** като засилва доверието, въпреки че все още има какво да се подобрява. Една-единствена държава членка изрази отрицателно становище[43].

Освен специфичните **предизвикателства,** свързани с КСД, Европол и четири държави членки посочиха като области за подобрение разходите и времето, свързани с **оценката на въздействието върху защитата на данните** (ОВЗД) и **предварителната консултация** с ЕНОЗД, които на практика се извършват по подразбиране. Друго предизвикателство, изтъкнато от шест държави членки, е капацитетът на Европол да се справи с **исканията за получаване на достъп до данни на субекти**, които вече са в обхвата на нейната компетентност, дори ако собственик на данните е държава членка.

Първият **служител по въпросите на основните права** беше назначен през декември 2022 г. През първите две години от мандата си той **не** е получавал и не е представял **жалби** до изпълнителния директор. СГПК продължава да наблюдава внимателно дейностите на Европол, като от влизането в сила на новите разпоредби не е издала никакви препоръки. Европейският парламент създаде **консултативния форум за основните права на СГПК** през февруари **2024 г.**.

### *3.4. Анализ на разходите и ползите от въведените нови правомощия и задачи на Европол за обработване на лични данни*

Предвид ранния етап на изпълнение на разпоредбите, въведени с Регламент (ЕС) 2022/991, и ограничения опит с тях, за Комисията е **твърде рано** да прави сериозни заключения относно новите разпоредби от един **анализ на разходите и ползите**.

Службите на Комисията са събрали информация от Европол относно направените до момента разходи за оперативното изпълнение на Регламент (ЕС) 2022/991, що се отнася до разглежданите разпоредби. Тези разходи като цяло възлизат на приблизително **25 милиона евро** (около 5 % от общия размер на средствата, отпуснати на Европол[44]) за периода 2022—2025 г., и включват предимно еднократни разходи. До момента държавите членки не са направили никакви съответни нови разходи, изрично свързани с Регламент (ЕС) 2022/991.

**Повечето разходи** (почти 17 милиона евро) са съставлявали значителни инвестиции в **разработването на нови ИКТ структури,** в изпълнението на разпоредбите относно научните изследвания и иновациите (тестова среда ODIN) и в информационни системи за обмен на лични данни с частноправни субекти (PERCI и EU CARES). Разходите за **човешки ресурси (ЧР)**, свързани както с ИКТ, така и с операциите, представляват приблизително една трета от всички разходи (около 8 милиона евро). В дългосрочен план разходите за ЧР ще съставляват **основните периодични разходи**.

---

[43] Вж. отговорите на държавите членки на въпрос 9 от краткия въпросник от 2 юни 2025 г. в приложение III към работния документ на службите.

[44] През същия период целият бюджет, отпуснат на Европол, възлиза на приблизително **860 милиона евро** (при постепенно нарастване от 192 милиона евро през 2022 г. до 241 милиона евро през 2025 г.). За повече подробности вж. придружаващия работен документ на службите.

Струва си да се отбележи, че гореспоменатите 8 милиона евро не включват разходите за ЧР в звеното за управление на информацията (IMU), нито ресурсите, свързани с (предишни и нови) мерки за контрол, които имат хоризонтален характер и които не могат да бъдат разделени на равнище изпълнение на конкретни разпоредби. Разходите за такива ресурси не са пренебрежими. Например за 2023 г. е изчислено, че **60 служители в еквивалент на пълно работно време (ЕПРВ)** (близо **5 %** от персонала на Европол) са били ангажирани в дейности на **органи по обезпечаване/надзор и субекти за контрол/консултации**. Европол е възложила на 25 служители в ЕПРВ да поемат надзора на защитата на данните и съответните действия по обезпечаване. Тук влизат проследяването съгласно препоръките на ЕНОЗД, както и работата, генерирана в контекста на предходни консултации за оперативно обработване на данни. Шестнадесет от тези 25 служители в ЕПРВ са ангажирани конкретно в дейности, свързани с изискванията на ЕНОЗД. Към юни 2025 г. Европол разполага със специален екип от осем служители на пълно работно време, които се занимават със защитата на данните, включително ДЛЗД.

Според Европол и петнадесет държави членки се очаква **ползите** от новите правомощия и задачи за обработване на лични данни, и по-специално анализът на големи и сложни набори от данни, както и сътрудничеството с частноправни субекти, да бъдат значителни и **да надвишат свързаните с тях разходи**. Нито една държава членка не беше на различно мнение. В дългосрочен план е разумно да се очаква известно повишаване на ефективността в резултат на икономиите от мащаба и намаляването на пределните разходи. Една държава членка подчерта, че „е важно Европол да предостави необходимите ИКТ ресурси, за да се осигурят и доразвият инструментите за изпълнение на новите възможности на Регламент (ЕС) 2022/991“ — мнение, което беше подкрепено от още две държави членки и други заинтересовани страни[45].

Според Европол и пет държави членки евентуалната **неефективност** при изпълнението също трябва да бъде разгледана в рамките на **съществуващата рамка на управление, администриране и защита на данните,** за да не може забавянето или ограничаването на използването на новите задачи за обработване на лични данни да застраши тяхното оперативно въздействие. Пет държави членки повдигнаха въпроса за твърде предпазливото изпълнение на правилата за защита на данните от Европол и неговия управителен съвет съгласно насоките на ЕНОЗД. Те предлагат гъвкавостта, предоставена от съзаконодателите, да бъде използвана по подходящ начин, с цел постигане на максимална ефективност и ефикасност на задачите на Европол и гарантиране на тяхната релевантност и дългосрочна рентабилност.

Оценката на методите на работа на Европол и на потенциалните области за опростяване е извън обхвата на доклада по член 68, параграф 3 от РЕ, като ще бъде извършена в рамките на оценката по член 68, параграф 1 от РЕ.

## 4. Заключения и следващи стъпки

Като цяло, предварителните основни констатации на Комисията са, че държавите членки продължават да **подкрепят ролята, изпълнявана от Европол** в ключовите области, в които тя понастоящем съдейства на държавите членки посредством **новите си задачи за обработване на лични данни**. Някои заинтересовани страни обаче считат, че за да се **извлекат максимални ползи** от новите правомощия за обработване на лични данни

[45] Вж. данните, представени в раздел 5 от работния документ на службите, приложен към настоящия доклад, и по-специално данните на Европол и отговорите на държавите членки на въпроси 2, 4 и 5 от краткия въпросник от 2 юни 2025 г. в приложение III към работния документ на службите и съвместното изявление на европейските полицейски началници относно бъдещето на Европол.

съществува нужда **да се намери решение на проблема с евентуалната неефективност**, особено в рамките на съществуващата уредба на управление, администриране и защита на данните. Би било от полза също така да се намалят **сложността и фрагментирането** на правната рамка, които може да възпрепятстват практикуващите да се възползват от новите възможности.

Като цяло, Комисията не откри данни за **отрицателно въздействие на новите правила върху основните права,** по-специално благодарение на стабилните гаранции за защита на данните, които също така улесняват информационния поток, като увеличават доверието на партньорите. Според някои държави членки Агенцията е предпочела консервативния подход, вместо **да използва по подходящ начин предоставената от съзаконодателите гъвкавост** при категоризирането на субектите на данни, оценката на въздействието върху защитата на данните, предварителната консултация с надзорния орган по защита на данните на Европол, разглеждането на исканията за получаване на право на достъп.

Предвид като цяло краткия срок за прилагане на новите правила за защита на личните данни, предвидени в Регламент (ЕС) 2022/991, събраните данни обаче не са окончателни по всички въпроси.

В **ProtectEU** — европейската стратегия за вътрешна сигурност[46], Комисията обяви, че ще предложи амбициозен преглед на мандата на Европол, с цел справяне с нарастващите предизвикателства пред сигурността. В съответствие с насоките си за по-добро регулиране[47] Комисията започна да подготвя оценката на Регламента за Европол и нейните методи на работа, проправяйки път за изготвянето през 2026 г. на **предложение на Комисията за подобряване на оперативността на Агенцията, съгласно посоченото в политическите насоки**[48]. През юли 2025 г. Комисията публикува покана за предоставяне на данни[49] и поръча външно проучване, което да подкрепи оценката на Регламента за Европол и оценката на въздействието на новото предложение. Оценката на Регламента за Европол, извършена за целите на изготвянето на настоящия доклад, има за цел да допринесе за тази оценка.

---

46 ProtectEU: европейска стратегия за вътрешна сигурност, стр. 10.

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

48 Урсула фон дер Лайен, Политически насоки за следващата Европейска комисия (2024—2029 г.), e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

49 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Law-enforcement-cooperation-new-Europol-regulation-proposal-en.