EUROPEISKA
KOMMISSIONEN

Bryssel den 11.12.2025
COM(2025) 752 final

RAPPORT FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Utvärdering och bedömning av de operativa konsekvenserna av genomförandet av de uppgifter som föreskrivs i förordning (EU) 2022/991, särskilt i artiklarna 4.1 t, 18.2 e, 18.6a, 18a, 26, 26a och 26b, med avseende på Europols mål samt dessa uppgifters inverkan på de grundläggande fri- och rättigheterna enligt stadgan, i enlighet med artikel 68.3 i förordning (EU) 2016/794

{SWD(2025) 404 final}

1. Utvärderingens omfattning

Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) har sedan den inledde sin verksamhet 1999 spelat **en central roll i kampen mot grov gränsöverskridande brottslighet och terrorism** och blivit en viktig drivkraft för brottsbekämpningssamarbetet i Europa. Säkerhetssituationen har förändrats drastiskt under de senaste 30 åren och motsvarande förändring har skett i den allvarliga och organiserade brottslighetens struktur[1]. Medlemsstaternas behov när det gäller att hantera nya hot på ett effektivt sätt i den operativa verksamheten och deras **förväntningar på Europols stöd har** också **förändrats**. Europols uppdrag har därför ersatts eller ändrats flera gånger för att upprätthålla och öka byråns relevans.

Europols uppdrag enligt förordning (EU) 2016/794[2] (*Europolförordningen*) ändrades senast 2022 genom förordning (EU) 2022/991[3] i syfte att hantera nya säkerhetshot. Europolförordningen var inte längre ändamålsenlig i en ny verklighet där brottslingar drar nytta av de fördelar som **digital omvandling, ny teknik, globalisering** och **rörlighet** för med sig[4].

De **särskilda målen** för förordning (EU) 2022/991[5] var att

- möjliggöra effektivt samarbete mellan **privata parter** och brottsbekämpande myndigheter för att motverka brottslingars missbruk av gränsöverskridande tjänster,
- göra det möjligt för brottsbekämpande myndigheter att analysera **stora och komplexa dataset** för att upptäcka gränsöverskridande kopplingar, i full överensstämmelse med **de grundläggande rättigheterna**,
- göra det möjligt för medlemsstaterna att använda **ny teknik** för brottsbekämpning.

Genom förordning (EU) 2022/991 ändrades dessutom de dataskyddsregler som är tillämpliga på Europol för att upprätthålla en **hög dataskyddsnivå** och uppnå en balans mellan å ena sidan byråns nya befogenheter att behandla personuppgifter och å andra sidan enskilda personers integritet och skyddet av personuppgifter. Förordningen anpassade i stor utsträckning de dataskyddsregler som är tillämpliga på Europol till de regler som är tillämpliga på andra EU-byråer och EU-organ som hanterar rättsliga och inrikes frågor enligt kapitel IX i förordning (EU) 2018/1875 (*EU:s dataskyddsförordning*) och de regler som är tillämpliga på medlemsstaternas brottsbekämpande myndigheter (*behöriga myndigheter*) enligt deras nationella lagstiftning som införlivar direktiv (EU) 2016/680 (*brottsdatadirektivet*)[6] i syfte att **underlätta informationsflödet**.

Denna rapport har antagits i enlighet med kommissionens skyldighet enligt **artikel 68.3 i Europolförordningen** att utvärdera[7] och bedöma de operativa konsekvenserna av Europols uppgifter enligt förordning (EU) 2022/991 tre år efter dess ikraftträdande. I enlighet med medlagstiftarnas uppdrag har kommissionen gjort följande: För det första har den utvärderat

---

1 Europol, Europeiska unionens hotbildsbedömning avseende grov och organiserad brottslighet (Socta) 2025 – *The changing DNA of serious and organised crime, available online under* https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf (*EU Socta 2025*). Se även tullens hotbildsbedömning (CTA) 2025, som finns online på https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

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

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

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

5 *Ibid.*

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

7 Denna utvärdering, som genomförs i enlighet med artikel 68.3 i Europolförordningen, är inte den utvärdering som ska utföras i enlighet med riktlinjerna för bättre lagstiftning inför ett eventuellt förslag till översyn av Europolförordningen. Se även avsnitt 4 nedan.

och bedömt de **operativa konsekvenserna** av vissa av de nya reglerna för behandling av personuppgifter, i förhållande till Europols mål enligt artikel 3 i Europolförordningen (dvs. att stödja och stärka de insatser som medlemsstaternas behöriga myndigheter gör och deras ömsesidiga samarbete för att förebygga och bekämpa brott som omfattas av Europols uppdrag). För det andra har den bedömt hur dessa regler påverkar de **grundläggande fri- och rättigheterna** (*grundläggande rättigheter*) enligt stadgan[8]. För det tredje har den genomfört en **kostnads-nyttoanalys** av databehandlingsuppgifterna i fråga.

För att förbereda utvärderingen samlade kommissionens avdelningar in information och återkoppling från olika källor och höll särskilda samråd med Europol och medlemsstaterna. Det åtföljande **arbetsdokumentet från kommissionens avdelningar** innehåller en detaljerad beskrivning av den allmänna bakgrunden och metoden för utvärderingen samt en utförlig redogörelse för de källor till underlag och de samråd som styrker de huvudsakliga resultat som sammanfattas i denna rapport.

2. Allmän bakgrund

I enlighet med artikel 68.3 i Europolförordningen omfattar kommissionens rapport utvalda bestämmelser i förordning (EU) 2022/991, med fokus på fem centrala aspekter av Europols arbete.

(1) Den externa dimensionen: Artikel 4.1 t i Europolförordningen om informationsregistrering av tredjelandsmedborgare i Schengens informationssystem (SIS) på förslag av Europol

Med tanke på **den allvarliga brottslighetens och terrorismens globala karaktär** är information som innehas av tredjeländer och internationella organisationer om förövare och personer som misstänks för sådana brott alltmer relevant för EU:s inre säkerhet. Den externa dimensionen av EU:s brottsbekämpningssamarbete har därför blivit avgörande för medlemsstaterna, liksom **Europols roll när det gäller att stödja medlemsstaterna i deras partnerskap med tredjeländer** och enheter i dessa länder. Ytterligare insatser kommer att vara **nödvändiga** för att stärka den globala säkerheten **i framtiden**[9].

Redan genom förordning (EU) 2022/991 infördes betydande ändringar av Europolförordningen i syfte att stärka den **externa dimensionen av Europols verksamhet**, särskilt genom att informationsutbytet med tredjeländer underlättades[10] och Europol ålades att inkludera en strategi för förbindelserna med tredjeländer och internationella organisationer i sin fleråriga programplanering och sina årliga arbetsprogram[11].

I artikel 4.1 t i Europolförordningen tilldelas Europol en ny uppgift: att stödja medlemsstaterna vid behandling av uppgifter som lämnas till Europol av tredjeländer eller internationella organisationer om personer som är inblandade i terrorism eller grov brottslighet. Detta inbegriper att **föreslå medlemsstaterna ett eventuellt införande av informationsregistreringar av tredjelandsmedborgare i Schengens informationssystem**

---

8 Europeiska unionens stadga om de grundläggande rättigheterna, EUT C 326, 26.10.2012, s. 391. http://data.europa.eu/eli/treaty/char_2012/oj.

9 Se ProtectEU: Europeisk strategi för inre säkerhet, COM(2025) 148 final av den 1 april 2025, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52025DC0148.

10 Se t.ex. artikel 25.4a i Europolförordningen som ger Europol möjlighet att överföra uppgifter till tredjeländer efter att byrån har bedömt alla omständigheter kring en överföring av personuppgifter och dragit slutsatsen att lämpliga skyddsåtgärder vad gäller skydd av de uppgifterna föreligger och artikel 25.5 i Europolförordningen som utvidgar tillämpningsområdet för de undantagsfall där Europol i vederbörligen motiverade fall kan överföra (kategorier av) uppgifter till tredjeländer och internationella organisationer.

11 Artikel 12.2 i Europolförordningen.

(SIS) i unionens intresse. Denna nya kategori av informationsregistreringar infördes 2022[12] efter en ändring av förordning (EU) 2018/1862 om användning av SIS på området polissamarbete och straffrättsligt samarbete[13].

Vissa uppgifter, särskilt när den berörda personen inte är EU-medborgare och det inte finns något samband med ett nationellt ärende, delas av tredjelandet endast med Europol, som behandlar uppgifterna och delar sina analysresultat med alla medlemsstater. Syftet med de nya bestämmelserna var att **maximera utnyttjandet av den information** som Europol tar emot från tredjeländer genom att göra den mer tillgänglig än den skulle vara om den endast fanns tillgänglig genom Europols eget system. Detta kompletterade andra åtgärder, såsom den europeiska sökportalen (ESP) och interoperabilitetsramen[14] mellan EU:s informationssystem för säkerhet, gräns- och migrationshantering. Syftet var att ta itu med strukturella brister i dessa system som hindrar de nationella myndigheternas, och särskilt gränskontrolltjänstemännens, arbete.

SIS ses som en **viktig ytterligare spridningskanal.** Det är den mest använda databasen i Europa för brottsbekämpning, gränskontroll och migration. Under 2024 genomfördes över 15 miljarder sökningar i SIS, jämfört med cirka 14 miljoner sökningar i Europols informationssystem (EIS) och färre än 3 miljarder sökningar (i hela världen) i Interpols 19 databaser, som är de två andra ledande informationssystemen för behöriga myndigheter[15].

(2) Innovation: Artiklarna 18.2 e och 33a i Europolförordningen om Europols behandling av personuppgifter för innovations- och forskningsprojekt

Den tekniska utvecklingen innebär både enorma möjligheter och betydande utmaningar för EU:s inre säkerhet[16] och har haft en så djupgående inverkan på brottsligheten att även den inneboende strukturen hos allvarliga och organiserade brottshot har förändrats[17]. Brottslingar integrerar snabbt ny teknik i sin verksamhet, skapar nya affärsmodeller och förfinar sin taktik. Samtidigt erbjuder dessa framsteg **bättre möjligheter än någonsin för brottsbekämpande myndigheter att förbättra sin kapacitet**. Forskning och innovation har därför en avgörande roll för den inre säkerheten, genom att skapa lösningar för att motverka framväxande hot, t.ex. från missbruk av teknik, och hålla jämna steg med de kriminella nätverkens snabbt föränderliga strukturer och *modus operandi*. Unionen har investerat, och kommer att fortsätta att investera, i utvecklingen av innovativa verktyg med hjälp av EU-finansierad forskning och innovation på säkerhetsområdet inom ramen för **ProtectEU**, den europeiska strategin för inre säkerhet[18].

Europols innovationslaboratorium[19], som inrättades i slutet av 2019 på uppdrag av EU:s medlemsstaters ministrar med ansvar för rättsliga och inrikes frågor, syftar till att driva på Europols engagemang för innovation inom brottsbekämpning. Genom förordning (EU) 2022/991 infördes väsentliga ändringar av Europolförordningen för att stärka Europols

---

12 Förordning (EU) 2022/1190; EUT L 185, 12.7.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 Förordning (EU) 2018/1862; EUT L 312, 7.12.2018, s. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 Förordning (EU) 2019/818; EUT L 135, 22.5.2019, s. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

15 eu-LISA, *SIS Annual Report 2024*, finns online på https://www.eulisa.europa.eu/sites/default/files/documents/sis-annual-report-2024.pdf, Europol, *Consolidated Annual Activity Report* (CAAR) 2024, finns online på https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF och https://www.interpol.int/How-we-work/Databases.

16 Europol, *Internet Organised Crime Threat Assessment* (Iocta) 2024, finns online på Internet Organised Crime Threat Assessment (IOCTA) 2024 || Europol.

17 Europol, EU Socta 2025, s. 19.

18 COM(2025) 148 final av den 1 april 2025, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52025DC0148&from=SV, s. 9.

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

uppdrag när det gäller innovation, i syfte att både stärka Europols innovationslaboratoriums potential och främja synergier med annan forsknings- och innovationsverksamhet på EU-nivå, särskilt inom kommissionen, inom ramen för **EU:s innovationsknutpunkt** för inre säkerhet[20].

Artikel 18.2 i Europolförordningen om syftet med informationsbehandling ändrades för att göra det möjligt för Europol att **behandla operativa personuppgifter** även **för forsknings- och innovationsprojekt**. Tillgången till högkvalitativa dataset för att kunna empiriskt testa de nya verktygens giltighet betraktas allmänt som en viktig förutsättning för att utveckla teknik. Otillförlitliga eller skeva dataset för testning kan tvärtom leda till att dålig teknik produceras[21].

Skräddarsydda uppgiftsskyddsgarantier för sådan behandling fastställdes i artiklarna 18.3a, 30.2, 30.3 och **33a i Europolförordningen**. Den senare artikeln innebär att en s.k. **sandlåda** måste inrättas, eftersom den föreskriver att personuppgifter som behandlas inom ramen för ett projekt tillfälligt ska kopieras till en separat, isolerad och skyddad uppgiftsbehandlingsmiljö inom Europol endast i syfte att genomföra projektet.

(3) <u>Brottsutredningar</u>: Artiklarna 18.6a och 18a i Europolförordningen om villkoren för behandling av personuppgifter som tas emot utan kategorisering av registrerade

I sin roll som **EU:s informationsknutpunkt för brott** underlättar Europol inte bara insamling och utbyte av information, utan bidrar också till att **göra utredningarna mer effektiva med hjälp av avancerad dataanalys** och genom att upptäcka gränsöverskridande kopplingar mellan brott och kriminella nätverk som inte är synliga på nationell nivå. Dessa möjligheter gynnar medlemsstaterna på så sätt att den information som finns tillgänglig för deras brottsutredningar blir fylligare.

Med den omfattande och intensiva användningen av teknik har **stora och komplexa dataset blivit det nya normala i alla aspekter av livet**, även när det gäller brottslighet[22]. Inom ramen för utredningar av organiserad brottslighet och terrorism har man börjat ta itu med utmaningen att analysera stora volymer elektroniskt lagrade data, som ofta uppgår till flera terabyte, inbegripet ljud-, video- och maskingenererade data som beslagtagits under utredningarna. I den gemensamma utredningen för att avveckla EncroChat-nätverket[23] analyserade utredarna till exempel miljontals meddelanden som brottslingar utbytt för att planera allvarliga brott. Mot denna bakgrund är tillgången till de verktyg, den expertis och de resurser på informations- och kommunikationsteknikområdet (IKT) som krävs för att analysera stora och komplexa dataset (som på teknisk jargong kallas *stordata*[24]) avgörande för brottsbekämpande och rättsliga myndigheter.

Även om Europolförordningen, som antogs 2016, inte i sig innebar några begränsningar för analys av stordata saknade den strukturerade bestämmelser som angav villkoren för analys av denna typ av uppgifter. Den mest **avgörande punkten** var **kravet på kategorisering av**

---

20 Se särskilt artikel 4.1 v och w i Europolförordningen.

21 SWD(2020) 543 final av den 9 december 2020, s. 29.

22 Europol, EU Socta 2025, *passim*.

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

24 Europeiska datatillsynsmannen, yttrande 7/2015, s. 7, finns på https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf. ”I allmänhet avser ***stordata***, som en gemensam benämning på de flera olika definitioner som existerar, ett tillvägagångssätt som består i att kombinera enorma volymer av information från olika källor och analysera dem med hjälp av mer sofistikerade algoritmer som underlag för beslut. Stordata bygger inte bara på teknikens ökade förmåga att stödja insamling och lagring av stora mängder data, utan även på dess förmåga att analysera, förstå och dra nytta av datas fulla värde (särskilt genom att använda analysapplikationer).”

registrerade. Kategorisering av registrerade avser kravet på att dataseten ska granskas så att man kan sortera personuppgifter enligt olika kategorier – en uttömmande förteckning finns i bilaga II.A och bilaga II.B till Europolförordningen – innan man börjar med den faktiska behandlingen av uppgifterna för utredningsändamål. Detta ska ske innan man samkör uppgifterna för att upptäcka kopplingar eller utför analyser av strategisk eller tematisk karaktär eller operativa analyser[25]. De relevanta kategorierna är kopplade till olika typer av inblandning i brottsutredningar, däribland i) misstänkta och potentiella framtida gärningsmän samt ii) kontakter, medarbetare, offer, vittnen och informatörer som har anknytning till brottslig verksamhet. I allmänhet kan Europol inte behandla eller ens lagra personuppgifter för personer som inte omfattas av någon av dessa kategorier.

Dataleverantörer, t.ex. **medlemsstater** eller **EU-organ och EU-byråer**, gör **vanligtvis** en kategorisering av registrerade redan innan personuppgifterna överförs till Europol[26]. Enligt EU-lagstiftningen är de alla skyldiga att kategorisera registrerade för den egna behandlingen och de egna utredningarna, oberoende av överföringen av uppgifter till Europol, och på grundval av motsvarande bestämmelser som emellertid ännu inte är överensstämmer med Europols regler[27]. När det gäller stora och komplexa dataset är manuell förbehandling dock en tids- och resurskrävande uppgift. Det kan ta upp till tre dagar att med en halvautomatiserad metod analysera data i en enda mobiltelefon, och hundratals mobiltelefoner kan beslagtas under en undersökning. Kategorisering av registrerades personuppgifter i syfte att använda dem för **analys av stordata** är **inte alltid möjlig** på grund av datasetens stora volym, hur berörda data är strukturerade (eller inte strukturerade), bristen på resurser och den ofantligt stora **manuella arbetsinsats som krävs**. I praktiken är den enda möjligheten att först analysera uppgifterna mer ingående ur ett operativt perspektiv eller att identifiera kopplingar, t.ex. med en halvautomatiserad metod, genom att samköra de uppgifter som finns tillgängliga.

Genom förordning (EU) 2022/991 förtydligades villkoren för kategorisering av den registrerade för att skapa **rättssäkerhet** när det gäller behandling av stora och komplexa dataset. Europol och Europeiska datatillsynsmannen gjorde olika tolkningar av Europolförordningens bokstav och anda när det gäller den tillämpliga datalagringsperioden. Enligt Europol bör denna period vara tre år, men enligt Europeiska datatillsynsmannen bör den vara sex månader[28]. Nya bestämmelser behövdes också för att uppnå **större flexibilitet** och en lämplig balans mellan uppgiftsskydd och säkerhetsaspekter.

I artikel 18.5a i Europolförordningen och artikel 73 i EU:s dataskyddsförordning gjordes först ett ytterligare förtydligande av den allmänna principen för kategorisering av registrerade i enlighet med artikel 18.2 och bilaga II. Europol har i uppdrag att i tillämpliga fall och möjligaste mån göra en **tydlig uppdelning av personuppgifter enligt vissa kategorier av registrerade**. I praktiken bör Europol som regel, innan personuppgifterna kan behandlas, fastställa exakt vilken roll varje person vars personuppgifter kommer att behandlas hade i den brottsliga verksamheten (t.ex. om en person är misstänkt, brottsoffer eller endast vittne). Uppgifterna för alla personer bör alltså inte behandlas tillsammans i en och samma datafil, eller som en del av en datafil (t.ex. genom att man helt enkelt fastställer att alla personer som nämns

---

25 Se artikel 18.2 i Europolförordningen.

26 Medlemsstaterna överför uppgifter till Europol via sin nätapplikation för säkert informationsutbyte (Siena), där kategorisering av de registrerade är obligatoriskt.

27 Se t.ex. artikel 6 i direktiv (EU) 2016/680 (*brottsdatadirektivet*, om indirekt behöriga myndigheter); EUT L 119, 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj, Artikel 51 i rådets förordning (EU) 2017/1939 (*Eppo-förordningen*); EUT L 283, 31.10.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj; Artikel 27.3 i förordning (EU) 2018/1727 (*Eurojustförordningen*); EUT L 295, 21.11.2018, s. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

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

är inblandade i en brottslig verksamhet som omfattas av Europols uppdrag på grundval av en undersökning av de allmänna omständigheter som genererade datafilen).

Enligt artikel 18.6a i Europolförordningen tillåts uttryckligen behandling av personuppgifter som mottagits utan kategorisering av registrerade i **upp till 18 månader**, vilket i motiverade fall kan förlängas med upp till 36 månader, endast i **syfte att komplettera kategoriseringen av registrerade**. I artikel 18.6a i Europolförordningen hänvisas det inte uttryckligen till stora och komplexa dataset, utan mer allmänt krävs det att behandlingen ska vara ”**strikt nödvändig**”.

I artikel 18a i Europolförordningen föreskrivs ett undantag som tillåter Europol att vid behov behandla personuppgifter som mottagits från en **behörig myndighet**, Europeiska åklagarmyndigheten (**Eppo**) eller **Eurojust**, för att stödja en **pågående brottsutredning**, utan att behöva utföra en kategorisering av registrerade, om detta inte redan har utförts, och utöver de kategorier av registrerade som förtecknas i Europolförordningen. Europol kan behandla uppgifterna genom **operativ analys** eller i vederbörligen motiverade undantagsfall genom **samkörning av uppgifter** för att identifiera kopplingar eller andra relevanta samband. Detta undantag utformades för att hantera skillnaderna mellan de bestämmelser om kategorisering av registrerade som är tillämpliga på Europol och de som är tillämpliga på de behöriga myndigheterna, Eppo och Eurojust.

(4) Samarbete med tredje parter: Artiklarna 26, 26a och 26b i Europolförordningen om utbyte av personuppgifter mellan Europol och privata parter

Brottslingar missbrukar i allt högre grad (gränsöverskridande) privata parters tjänster, såsom internetbaserade, finansiella och klassiska telekommunikationstjänster. Följaktligen **innehar privata parter en stor mängd personuppgifter som är relevanta för brottsutredningar**. Internet har skapat ett offentligt utrymme som i praktiken är i privata händer, vilket gör det svårt att verkställa regler för brottsbekämpande ändamål lika effektivt online som offline[29].

Därför har **samarbete mellan brottsbekämpande myndigheter och privata parter** blivit **nödvändigt**. Som fastställs i **ProtectEU**, den europeiska strategin för inre säkerhet, kommer det att vara viktigt att stärka partnerskapen med den privata sektorn för att underlätta informationsutbytet[30]. Ett antal polischefer har också i ett gemensamt uttalande om Europols framtid[31] uppmanat Europol att fungera som en **”central ingång för att få information från privata enheter”**. Detta samarbete omfattar allt från utbyte av information och tillhandahållande av kommersiella data med öppen källkod till engagemang i forsknings- och innovationsprojekt och tillhandahållande av tjänster som stöder företagens verksamhet[32]. Europol stängde under 2025 till exempel ned Lumma Stealers verksamhet, det program för att stjäla information som utgör det största globala hotet i detta sammanhang. Nedstängningen blev möjlig tack vare ett samarbete med Microsoft, som hade identifierat över 394 000 Windows-datorer runtom i världen som hade fått den skadliga Lumma-programvaran installerad[33].

---

29 SWD(2020) 543 final av den 9 december 2020, s. 16.

30 Se ProtectEU: Europeisk strategi för inre säkerhet, 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*, 31 maj 2023, EDOC #1306090v13. Se även Milieu Consulting, *Study on the Practice of direct exchanges with of personal data between Europol and Private Party*, slutrapport, september 2020.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Fler exempel finns i det åtföljande arbetsdokumentet från kommissionens avdelningar.

Genom förordning (EU) 2022/991 infördes **ytterligare möjligheter** för Europol att utbyta personuppgifter med privata parter. Tidigare kunde Europol ta emot personuppgifter från privata parter endast via någon av Europols nationella enheter, eller genom på förhand identifierade kontaktpunkter och myndigheter i tredjeländer eller internationella organisationer. Syftet med Europols behandling var begränsad till att identifiera den berörda nationella enheten, det tredjeland, den internationella organisationskontaktpunkt eller den myndighet som skulle kunna ta på sig ansvaret för ärendet.

Genom den **ändrade artikel 26 i Europolförordningen utvidgades Europols uppgift** och Europol kan nu behandla information (inbegripet personuppgifter) från privata parter på ett omfattande sätt. Att identifiera den berörda nationella Europolenheten är fortfarande ett av de främsta syftena med behandlingen. Men Europol får nu också komplettera informationen med sin egen analys för att underlätta vidare behandling av ett ärende på nationell nivå.

Utöver de övergripande bestämmelserna i artikel 26 i Europolförordningen infördes genom artikel 26a i Europolförordningen regler för **krissituationer online**, och artikel 26b i Europolförordningen gällde **spridning av material med sexuella övergrepp mot barn på nätet**. I sådana fall får Europol bistå medlemsstaterna genom att behandla personuppgifter som mottagits direkt från privata parter. Europol får också överföra personuppgifter till privata parter från fall till fall.

Genom förordning (EU) 2022/991 infördes möjligheten att använda Europols infrastruktur för informationsutbyte mellan behöriga myndigheter och privata parter samt möjligheten för Europol att begära att medlemsstaterna i enlighet med sin nationella lagstiftning tar emot personuppgifter från privata parter.

Dessa bestämmelser antogs i överensstämmelse med andra initiativ, såsom förordningen om terrorisminnehåll online[34] och förordningen om digitala tjänster[35]. Ytterligare åtgärder planeras för att öka privata parters deltagande i kampen mot brottslighet och underlätta laglig tillgång till uppgifter för att förverkliga ”ambition[en] att förändra säkerhetskulturen” (**samhälleligt helhetsgrepp**) inom ramen för **ProtectEU,** den europeiska strategin för inre säkerhet[36].

(5) Intern och extern tillsyn av Europols efterlevnad av de grundläggande rättigheterna

I förordning (EU) 2022/991 betonas Europols skyldighet att respektera de grundläggande rättigheterna enligt bestämmelserna om Europols uppgifter och förstärkta skyddsåtgärder, särskilt genom att **stärka den interna och externa tillsynen av byrån**.

När det gäller dataskydd innebar anpassningen av Europolförordningen till de dataskyddsgarantier som omfattas av EU:s dataskyddsförordning att nya regler infördes för den tillsyn som utförs av **dataskyddsombudet** och **Europeiska datatillsynsmannen**. Skyldigheten att tillhandahålla en konsekvensbedömning avseende dataskydd och hålla förhandssamråd med Europeiska datatillsynsmannen tillämpas till exempel systematiskt på alla nya typer av behandling. Genom förordning (EU) 2022/991 fick Europol också ny behörighet i fråga om begäranden om tillgång till personuppgifter. Tidigare var de nationella behöriga myndigheterna ansvariga för att hantera begäranden om tillgång till personuppgifter om medlemsstaterna var uppgiftslämnare.

Genom förordning (EU) 2022/991 inrättades också en **ny befattning som ombud för grundläggande rättigheter** vid Europol, med bland annat uppdraget att informera Europols

---

34 Förordning (EU) 2021/784; EUT L 172, 17.5.2021, s. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj.

35 Förordning (EU) 2022/2065; EUT L 277, 27.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

36 Se ProtectEU: Europeisk strategi för inre säkerhet, s. 2.

verkställande direktör om eventuella kränkningar av de grundläggande rättigheterna i samband med byråns verksamhet.

Den **demokratiska tillsynen och ansvarsskyldigheten förstärktes** också genom **Europaparlamentets och de nationella parlamentens** politiska övervakning av Europols verksamhet, i enlighet med artikel 88.2 andra stycket i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*). Vidare stärktes den **gemensamma parlamentariska kontrollgruppens** övervakningsroll genom förordning (EU) 2022/991[37]. Till exempel föreskrev förordningen obligatoriska samråd med den gemensamma kontrollgruppen om Europols utkast till den fleråriga programplaneringen och de årliga arbetsprogrammen och en möjlighet för den gemensamma parlamentariska kontrollgruppen att utfärda icke-bindande särskilda rekommendationer till Europol och överlämna dem till Europaparlamentet och de nationella parlamenten. Vidare föreskrev förordningen inrättandet av ett rådgivande forum för att på begäran bistå den gemensamma parlamentariska kontrollgruppen genom att tillhandahålla oberoende råd i frågor som rör grundläggande rättigheter.

3. Utvärderingens viktigaste resultat

3.1. Lägesrapport om det operativa genomförandet av Europols nya befogenheter och uppgifter för behandling av personuppgifter

Förordning (EU) 2022/991 trädde **i kraft den 28 juni 2022**. Det operativa genomförandet var dock beroende av en rad styrningsåtgärder, tekniska och administrativa åtgärder samt operativa krav. Till exempel blev det nödvändigt att i vissa fall inrätta nya IKT-strukturer.

Tre år senare har **nästan alla bestämmelser** i artikel 68.3 i förordning (EU) 2022/991 **börjat tillämpas**. Bestämmelserna om analys av stora och komplexa dataset (artiklarna 18.6a och 18a i Europolförordningen) och samarbete med privata parter (artiklarna 26, 26a och 26b i Europolförordningen) började gälla från och med den 28 juni 2022, eller kort därefter. Behandlingen av personuppgifter för forsknings- och innovationsprojekt (artikel 18.2 e i Europolförordningen) inleddes 2023 efter att en s.k. sandlåda, som fick namnet Odin, inrättades för att uppfylla de särskilda dataskyddskraven i artikel 33a i Europolförordningen. Den 29 juni 2025 hade Europols möjlighet att föreslå **registreringar om SIS-information** till medlemsstaterna i enlighet med artikel 4.1 t i Europolförordningen ännu inte börjat tillämpas, eftersom det tekniska genomförandet av den nya typen av registrering fortfarande pågår. Denna möjlighet **förväntas finnas tillgänglig 2026**.

3.2. Utvärdering av de operativa konsekvenserna av Europols nya befogenheter och uppgifter för behandling av personuppgifter med avseende på byråns mål enligt artikel 3 i Europolförordningen

När det gäller de operativa konsekvenserna av Europols nya befogenheter och uppgifter för behandling av personuppgifter visade samrådet att **medlemsstaterna på det hela taget har en positiv bild** av deras relevans, effektivitet och mervärde samt av Europols stöd till de nationella behöriga myndigheterna på de berörda områdena[38].

De utredningsbefogenheter som omfattas av denna utvärdering används inte kontinuerligt eller systematiskt för att behandla uppgifter i övervakningssyfte. Vissa används enbart i undantagsfall, medan andra används mer regelbundet på behovsbasis i undersökningar. Den **operativa användningen av de nya bestämmelserna** under referensperioden **varierade**

---

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

38 Se de bevis som läggs fram i avsnitt 5 i det arbetsdokument från kommissionens avdelningar som åtföljer denna rapport, särskilt Europols inlagor och medlemsstaternas svar på frågorna 2, 4 och 5 i det korta frågeformuläret av den 2 juni 2025, i bilaga III till arbetsdokumentet från kommissionens avdelningar.

avsevärt i **kvantitativa termer**, beroende på de olika tekniska egenskaper och de rättsliga villkor som är sammanbundna med de nya bestämmelserna.

Europol mottog från medlemsstaterna ett **icke försumbart** antal **nya bidrag utan kategorisering av registrerade** enligt artikel 18.6a i Europolförordningen. Bidragen uppgick år 2023 till 653 och år 2024 till 597. Det skedde ingen kortsiktig ökning av bidragen utan kategorisering av registrerade, och antalet fall där artikel 18.6a tillämpades förblev **konstant** jämfört med motsvarande fall under perioden före den 28 juni 2022. De nya bestämmelserna hade heller inte någon negativ inverkan på medlemsstaternas engagemang i genomförandet av kategoriseringen av registrerade[39]. Mellan 2023 och 2024 stod andelen bidrag utan kategorisering av registrerade för **mindre än 1 % av alla de bidrag** från medlemsstaterna som godtagits av Europol (0,85 % 2023 och 0,71 % 2024). Sedan juni 2022 har Europol konsekvent slutfört kategoriseringen av registrerade inom 18 månader, utan att utnyttja den förlängda tidsfristen på 36 månader. Europol och sex medlemsstater betonade att den **administrativa bördan**, trots den förbättrade rättssäkerheten, **förblev betydande** för både Europol och de behöriga myndigheterna på grund av de insatser som krävdes för att efterleva kravet på kategorisering av personuppgifter enligt den roll personen i fråga hade i brottet. Detta krav tillämpas mycket strikt av Europol[40].

Europol rapporterade att informationsutbytet med **privata parter** fortfarande var försumbart 2023, eftersom endast 26 fall som gällde genomförandet av artikel 26 i Europolförordningen registrerades (utöver de fall som omfattas av förordningen om digitala tjänster)[41]. Under **2024** visade statistiken dock en **kraftig ökning till 284** fall (nästan +1 000 %) som omfattade samarbete med privata parter enligt artikel 26 i Europolförordningen. Detta gällde särskilt uppgifter från privata företag för att utreda **finansiella och ekonomiska brott**. Europol utnyttjade också artikel 26b i Europolförordningen i betydande utsträckning i kampen mot sexuell exploatering av barn, där samarbetet med privata parter redan tidigare var mycket omfattande. I båda fallen omfattar uppgifterna även samarbete som var möjligt enligt den tidigare rättsliga ramen. De tillgängliga uppgifterna avslöjar inte i vilken utsträckning dessa nya fall omfattas av de nya bestämmelserna eller en ökad användning av befintliga möjligheter.

Europol antog **2025** en **ny strategi** för att ytterligare förbättra samarbetet med privata parter. Dessutom har Europol vidtagit åtgärder för att uppgradera den IKT-infrastruktur som behöriga myndigheter kan använda för informationsutbyte med privata parter. Europol lanserade **2023** *Plateforme Européenne de Retraits de Contenus Illégaux sur Internet* (**PERCI**, EU:s plattform för avlägsnande av olagligt innehåll på internet) för att underlätta genomförandet av förordningen om terrorisminnehåll online och, i framtiden, eventuellt även artikel 18 i förordningen om digitala tjänster, samt **EU Cares**, EU:s tjänst för barn som far illa. PERCI ingår inte i Europols informationssystem (EIS)[42].

Vissa bestämmelser användes inte alls (artikel 26a i Europolförordningen), trots att de kunde tillämpas, **eller** tillämpades **endast undantagsvis** (ett fall där artikel 18a i Europolförordningen användes 2024, och ett projekt som genomfördes med behandling av personuppgifter enligt artikel 18.1 t i Europolförordningen 2025, med tre nya projekt redan på gång).

---

39 Som en medlemsstat betonade under samrådet kan ”[medlemsstaterna] tydligt urskilja vilken typ av uppgifter [de] behandlar, vilket kan vara mycket viktigt för själva utredningen”.

40 Se avsnitt 7.1.3 i det arbetsdokument från kommissionens avdelningar som åtföljer denna rapport och medlemsstaternas svar på fråga 9 i det korta frågeformuläret av den 2 juni 2025, i bilaga III till arbetsdokumentet från kommissionens avdelningar.

41 Europols rapport från 2023 i enlighet med artikel 16.11 i Europolförordningen (*2023 Report pursuant to Article 16(11) ER*).

42 Förordning (EU) 2019/818; EUT L 135, 22.5.2019, s. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

På grund av att de bestämmelser som infördes genom förordning (EU) 2022/991 endast har tillämpats under en begränsad period och att brottsutredningar och rättsliga förfaranden är långdragna till sin karaktär kunde medlemsstaterna inte lämna några kvantitativa uppgifter om vilka effekter bestämmelserna hade fått i praktiken. De gav i stället några exempel på framgångsrika utredningar där de **nya utredningsmöjligheterna** i kombination med de bestämmelser som redan används har lett till **påtagliga fördelar i verkliga situationer**, såsom EncroChat, Sky ECC, Balkanbaserade kriminella nätverk som sysslar med kokainhandel och Lumma Stealer.

Europol och åtta medlemsstater flaggade också några **områden där det finns utrymme för förbättring** för att få till stånd en så effektiv och konsekvent användning som möjligt av den nya rättsliga ramen och stärka Europols framtida roll. Det finns farhågor, särskilt från Europols sida, om att de rättsliga bestämmelserna är överdrivet komplexa, fragmenterade och omfångsrika och att detta skulle kunna avskräcka olika aktörer eller privata parter från att använda de nya tillgängliga instrumenten. Medlemsstaternas kommentarer rör snarare Europols restriktiva tillämpning av uppgiftsskyddsgarantierna under tillsyn av Europeiska datatillsynsmannen, vilken riskerar att undergräva vissa bestämmelsers effektivitet och mervärde.

3.3. Bedömning av effekterna av Europols nya befogenheter och uppgifter för behandling av personuppgifter med avseende på de grundläggande rättigheterna

Kommissionen fann **inga** bevis på **negativa konsekvenser med avseende på de grundläggande rättigheterna** till följd av hur de nya befogenheterna för behandling av personuppgifter används operativt, på grundval av den begränsade tillämpningen hittills av de nya befogenheterna för behandling av personuppgifter.

Utöver genomförandet av de särskilda dataskyddskrav som är knutna till de nya befogenheterna för behandling av personuppgifter har Europol successivt vidtagit alla nödvändiga åtgärder för att genomföra de nya övergripande tillsynsmekanismerna avseende de grundläggande rättigheterna.

Europols styrelse antog 2024 de reviderade genomförandebestämmelserna för dataskyddsombudet som en av de sista nödvändiga genomförandeakterna med koppling till det nya dataskyddssystemet. Det underlag som samlats in tyder på att Europol och dess styrelse i samarbete med Europols dataskyddsombud och Europeiska datatillsynsmannen också har säkerställt ett **strikt genomförande av de nya dataskyddsgarantier** som infördes 2022. Det strikta genomförandet har vid första påseendet effektivt förhindrat eventuella negativa effekter och negativ påverkan på grund av hur de nya befogenheterna för behandling av personuppgifter användes initialt, med avseende på enskilda personers rätt till integritet och skydd av personuppgifter. Enligt medlemsstaterna har Europol för närvarande en **robust rättslig ram för uppgiftsskydd** som säkerställer tillräckliga skyddsåtgärder för en potentiellt ökad användning av dess nya befogenheter. Sju medlemsstater betonade också att denna ram **underlättar informationsflödet** genom att öka förtroendet, även om det fortfarande finns utrymme för förbättring. Endast en medlemsstat uttryckte en negativ åsikt[43].

Utöver de särskilda **utmaningarna** i samband med kategoriseringen av registrerade nämnde Europol och fyra medlemsstater att det fanns utrymme för förbättring när det gäller de kostnader och den tid som tas i anspråk av **konsekvensbedömningen avseende dataskydd** och **förhandssamrådet med** Europeiska datatillsynsmannen, som i praktiken utförs som standard. En ytterligare utmaning som sex medlemsstater tog upp är Europols behandling av

[43] Se medlemsstaternas svar på fråga 9 i det korta frågeformuläret av den 2 juni 2025 i bilaga III till det åtföljande arbetsdokumentet från kommissionens avdelningar.

de registrerades begäranden om tillgång till personuppgifter, för vilka Europol nu har behörighet även i de fall där en medlemsstat äger uppgifterna.

Det första **ombudet för grundläggande rättigheter** utsågs i december **2022**. Ombudet har under de två första åren av sin mandatperiod **inte** mottagit eller framfört **några klagomål** till den verkställande direktören. Den gemensamma parlamentariska kontrollgruppen har fortsatt att noga övervaka Europols verksamhet och har inte utfärdat några rekommendationer sedan de nya bestämmelserna trädde i kraft. Europaparlamentet inrättade den **gemensamma parlamentariska kontrollgruppens rådgivande forum för grundläggande rättigheter** i februari **2024**.

3.4. Kostnads-nyttoanalys av Europols nya befogenheter och uppgifter för behandling av personuppgifter

Med tanke på att de bestämmelser som infördes genom förordning (EU) 2022/991 endast har tillämpats under en relativt kort period och att erfarenheterna av dem därför är begränsade är det **för tidigt** för kommissionen att dra meningsfulla slutsatser om de nya bestämmelserna utifrån en **kostnads-nyttoanalys**.

Kommissionens avdelningar har samlat in information från Europol om de kostnader som hittills uppstått i samband med det operativa genomförandet av förordning (EU) 2022/991 för de bestämmelser som omfattas av översynen. Dessa kostnader uppgick till cirka **25 miljoner euro** (cirka 5 % av det totala anslaget till Europol[44]) mellan 2022 och 2025, vilket främst omfattade engångskostnader. Medlemsstaterna har hittills inte ådragit sig några betydande nya kostnader som är specifikt kopplade till förordning (EU) 2022/991.

De flesta kostnaderna (nästan 17 miljoner euro) bestod av betydande investeringar i **utvecklingen av nya IKT-strukturer**, genomförandet av bestämmelser om forskning och innovation (den s.k. sandlådan Odin) och informationssystem för utbyte av personuppgifter med privata parter (PERCI och EU Cares). **Kostnaderna för personalresurser**, både i samband med IKT och den operativa verksamheten, stod för ungefär en tredjedel av de totala utgifterna (cirka 8 miljoner euro). Personalresurser kommer att utgöra de **huvudsakliga återkommande kostnaderna på lång sikt**.

Det är värt att notera att de 8 miljoner euro som nämns ovan inte omfattar personalkostnader för enheten för informationshantering eller de resurser som är förknippade med (tidigare och nya) tillsynsåtgärder av övergripande karaktär, för vilka ett särskiljande av enskilda bestämmelser på genomförandenivå inte är möjligt. Kostnaderna för dessa resurser är inte försumbara. Under 2023 uppskattades till exempel att **60 heltidsekvivalenter** (nästan **5 %** av Europols personal) deltog i verksamhet inom **försäkrings-, tillsyns- och rådgivningsorgan**. Europol avsatte 25 heltidsekvivalenter till insatser för tillsyn av dataskyddet och motsvarande säkerhetsåtgärder. Detta inbegriper uppföljning av Europeiska datatillsynsmannens rekommendationer samt arbete i samband med förhandssamråd inför operativ uppgiftsbehandling. Av dessa 25 heltidsekvivalenter var 16 specifikt inriktade på verksamhet med anknytning till datatillsynsmannens krav. Sedan juni 2025 har Europol en särskild grupp bestående av åtta heltidsanställda på dataskyddsområdet, däribland dataskyddsombudet.

Enligt Europol och 15 medlemsstater förväntas **fördelarna** med de nya befogenheterna och uppgifterna med koppling till behandling av personuppgifter, särskilt när det gäller analys av stora och komplexa dataset, samt samarbete med privata parter vara betydande och **uppväga de därmed förbundna kostnaderna**. Ingen medlemsstat hade en avvikande uppfattning.

---

[44] Under samma tidsperiod uppgick den budget som anslagits till Europol totalt till ungefär **860 miljoner euro** (vilket stegvis ökade från 192 miljoner euro 2022 till 241 miljoner euro 2025). För mer information, se det åtföljande arbetsdokumentet från kommissionens avdelningar.

Vissa effektivitetsvinster kan rimligen förväntas på lång sikt, tack vare stordriftsfördelar och minskade marginalkostnader. En medlemsstat betonade att ”det är viktigt att Europol står för de IKT-resurser som krävs för att tillhandahålla och vidareutveckla verktygen för genomförandet av de nya möjligheterna i förordning (EU) 2022/991”. Detta stöddes också av två andra medlemsstater och andra intressenter[45].

Enligt Europol och fem medlemsstater måste eventuell **bristande effektivitet** i genomförandet också åtgärdas inom den **befintliga ramen för styrning, administration och dataskydd** för att undvika att Europols nya uppgifter avseende personuppgiftsbehandling försenas eller begränsas och att deras inverkan på den operativa verksamheten därmed undergrävs. Fem medlemsstater ifrågasatte Europols och dess styrelses alltför försiktiga genomförande av dataskyddsreglerna, under ledning av Europeiska datatillsynsmannen. De föreslår att den flexibilitet som beviljas av medlagstiftarna bör utnyttjas på lämpligt sätt för att se till att Europols uppgifter utförs så effektivt och ändamålsenligt som möjligt och att de är relevanta och lönsamma på lång sikt.

En utvärdering av Europols arbetsmetoder och de områden där det skulle kunna finnas utrymme för förenkling ligger utanför rapportens tillämpningsområde enligt artikel 68.3 i Europolförordningen och kommer att genomföras inom ramen för utvärderingen enligt artikel 68.1 i Europolförordningen.

4. Slutsatser och det fortsatta arbetet

Sammantaget är kommissionens huvudsakliga preliminära slutsatser att medlemsstaterna fortsatt **stöder Europols roll** på de nyckelområden där Europol för närvarande bistår medlemsstaterna med sina **nya uppgifter avseende personuppgiftsbehandling**. För att **dra största möjliga nytta** av de nya befogenheterna för behandling av personuppgifter anser vissa intressenter dock att man behöver **ta itu med eventuell bristande effektivitet**, särskilt inom den befintliga ramen för styrning, administration och dataskydd. Det skulle också vara lämpligt att göra den rättsliga ramen mindre **komplex och fragmenterad**, för att inte avskräcka aktörer från att utnyttja de nya möjligheterna.

På det hela taget fann kommissionen inga bevis för att de nya reglerna hade en **negativ inverkan på de grundläggande rättigheterna**, särskilt tack vare robusta dataskyddsgarantier som också underlättar informationsflödet genom att öka partnernas förtroende. Vissa medlemsstater ansåg att byrån har tillämpat en konservativ strategi, och att man i stället **på lämpligt sätt bör utnyttja den flexibilitet som medlagstiftarna har beviljat** när det gäller kategoriseringen av de registrerade, konsekvensbedömningen av dataskyddet, förhandssamråden med Europols datatillsynsman och hanteringen av begäranden om tillgång till personuppgifter.

Med tanke på att de nya regler om skydd av personuppgifter som föreskrivs i förordning (EU) 2022/991 endast har tillämpats under en relativt kort tidsperiod är det insamlade underlaget dock inte avgörande i alla frågor.

Kommissionen tillkännagav i **ProtectEU**: En europeisk strategi för inre säkerhet[46], att den kommer att föreslå en ambitiös översyn av Europols uppdrag för att ta itu med växande säkerhetsutmaningar. Kommissionen inledde, i enlighet med sina riktlinjer för bättre

---

45 Se de bevis som läggs fram i avsnitt 5 i det arbetsdokument från kommissionens avdelningar som åtföljer denna rapport, särskilt Europols inlagor och medlemsstaternas svar på frågorna 2, 4 och 5 i det korta frågeformuläret av den 2 juni 2025, i bilaga III till arbetsdokumentet från kommissionens avdelningar och det gemensamma uttalandet från europeiska polischefer om Europols framtid.

46 ProtectEU: Europeisk strategi för inre säkerhet, s. 10.

lagstiftning[47], ett förberedande arbete för att utvärdera Europolförordningen och Europols arbetsmetoder, vilket banade väg för ett **förslag från kommissionen 2026 om att göra Europol mer operativ, i enlighet med de politiska riktlinjerna**[48]. I juli 2025 offentliggjorde kommissionen en inbjudan att lämna synpunkter[49] och beställde en extern studie till stöd för utvärderingen av Europolförordningen och konsekvensbedömningen av det nya förslaget. Den utvärdering av Europolförordningen som gjordes i samband med utarbetandet av denna rapport ska bidra till utvärderingen.

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

48 Ursula von der Leyen, *Politiska riktlinjer för nästa europeiska kommission 2024–2029*, e6cd4328-673c-4e7a-8683-f63ffb2cf648_sv.

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