EUROPA-
KOMMISSIONEN

Bruxelles, den 11.12.2025
COM(2025) 752 final

RAPPORT FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om evaluering og vurdering af den operationelle virkning af gennemførelsen af de opgaver, der er foreskrevet i forordning (EU) 2022/991, navnlig i artikel 4, stk. 1, litra t), artikel 18, stk. 2, litra e), artikel 18, stk. 6a, og artikel 18a, 26, 26a og 26b, med hensyn til Europols målsætninger og disse opgavers indvirkning på de grundlæggende rettigheder og frihedsrettigheder, som er nedfældet i chartret, i henhold til artikel 68, stk. 3, i forordning (EU) 2016/794

{SWD(2025) 404 final}

1. Evalueringens omfang

Siden **Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol)** begyndte at fungere i 1999, har det spillet **en central rolle i bekæmpelsen af grov grænseoverskridende kriminalitet og terrorisme** og er blevet en vigtig drivkraft for retshåndhævelsessamarbejde i Europa. Sikkerhedslandskabet har ændret sig dramatisk i løbet af de sidste 30 år med et tilsvarende skift i DNA'et for grov og organiseret kriminalitet[1]. Medlemsstaterne har nye operationelle behov for effektivt at imødegå nye trusler, og deres **forventninger til Europols støtte har** også **udviklet sig**. Europols mandat er derfor blevet erstattet eller ændret flere gange for at opretholde og styrke agenturets relevans.

Europols mandat, som er fastsat i forordning (EU) 2016/794[2] ("Europolforordningen"), blev senest ændret i 2022 ved forordning (EU) 2022/991[3] for at imødegå nye sikkerhedstrusler. Europolforordningen var ikke længere egnet til formålet i en ny virkelighed, hvor kriminelle udnytter fordelene ved **digital omstilling**, **nye teknologier**, **globalisering** og **mobilitet**[4].

De **specifikke målsætninger** i forordning (EU) 2022/991[5] var at:

- muliggøre et effektivt samarbejde mellem **private parter** og retshåndhævende myndigheder for at bekæmpe kriminelles misbrug af grænseoverskridende tjenesteydelser
- gøre det muligt for de retshåndhævende myndigheder at analysere store og komplekse datasæt med henblik på at opdage grænseoverskridende forbindelser i fuld overensstemmelse med de **grundlæggende rettigheder**
- sætte medlemsstaterne i stand til at anvende **nye teknologier** til retshåndhævelse.

Desuden ændrede forordning (EU) 2022/991 de databeskyttelsesregler, der gælder for Europol, for at opretholde et **højt niveau af databeskyttelse** og finde en balance mellem agenturets nye beføjelser til at behandle personoplysninger og enkeltpersoners ret til privatlivets fred og beskyttelse af personoplysninger. Den tilpassede i vid udstrækning de databeskyttelsesregler, der gælder for Europol, til de regler, der gælder for andre EU-agenturer og -organer inden for retlige og indre anliggender (RIA) i henhold til kapitel IX i forordning (EU) 2018/1725 ("EU's databeskyttelsesforordning" eller "EUDPR"), og de regler, der gælder for medlemsstaternes retshåndhævende myndigheder ("kompetente myndigheder") i henhold til deres nationale lovgivning til gennemførelse af direktiv (EU) 2016/680 ("retshåndhævelsesdirektivet")[6] for at **lette informationsstrømmen**.

Denne rapport er vedtaget i overensstemmelse med Kommissionens forpligtelse i henhold til **Europolforordningens artikel 68, stk. 3,** til at evaluere[7] og vurdere den operationelle virkning af Europols opgaver som fastsat i forordning (EU) 2022/991 tre år efter dens ikrafttræden. Som

---

1 Europol, 2025, *EU Serious and Organised Crime Threat Assessment (SOCTA) – The changing DNA of serious and organised crime*, tilgængelig online her: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf ("EU SOCTA 2025"). Se også *Customs threat assessment (CTA) 2025*, tilgængelig online her: https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

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

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

4 SWD(2020) 543 final af 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 af 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

7 Denne evaluering, der foretages i overensstemmelse med Europolforordningens artikel 68, stk. 3, er ikke den evaluering, der skal foretages i henhold til retningslinjerne for bedre regulering med henblik på et eventuelt forslag til revision af Europolforordningen. Se også afsnit 4 nedenfor.

pålagt af fælleslovgiverne har Kommissionen: for det første evalueret og vurderet **de operationelle virkninger** af nogle af de nye regler for behandling af personoplysninger i forhold til Europols målsætninger i henhold til Europolforordningens artikel 3 (nemlig: støtte og styrke medlemsstaternes kompetente myndigheders indsats for og deres indbyrdes samarbejde om at forebygge og bekæmpe grov kriminalitet, der er omfattet af Europols mandat), for det andet vurderet virkningen af disse regler på **grundlæggende rettigheder og frihedsrettigheder** ("grundlæggende rettigheder") som nedfældet i chartret[8], og for det tredje foretaget en **cost-benefit-analyse** af de dermed forbundne databehandlingsopgaver.

For at forberede revisionen indsamlede Kommissionens tjenestegrene oplysninger og feedback fra forskellige kilder og afholdt ad hoc-høringer med Europol og medlemsstaterne. Det ledsagende **arbejdsdokument fra Kommissionens tjenestegrene** indeholder en detaljeret beskrivelse af den generelle kontekst og metode for revisionen samt en omfattende redegørelse for dokumentationskilder og høringer, der underbygger de vigtigste resultater, som er sammenfattet i denne rapport.

2. Generel baggrund

I overensstemmelse med Europolforordningens artikel 68, stk. 3, omhandler denne rapport fra Kommissionen udvalgte bestemmelser i forordning (EU) 2022/991 med fokus på fem centrale aspekter af Europols arbejde.

(1) Ekstern dimension: Europolforordningens artikel 4, stk. 1, litra t), om indberetninger med oplysninger om tredjelandsstatsborgere i Schengeninformationssystemet (SIS) efter forslag fra Europol

I betragtning af den **globale karakter af grov kriminalitet og terrorisme** er de oplysninger, som tredjelande og internationale organisationer er i besiddelse af om gerningsmænd til grov kriminalitet og terrorisme og om personer, der mistænkes for at have begået grov kriminalitet og terrorisme, i stigende grad relevante for EU's indre sikkerhed. Den eksterne dimension af EU's retshåndhævelsessamarbejde er derfor blevet afgørende for medlemsstaterne, og det samme er **Europols rolle med hensyn til at støtte medlemsstaterne i deres partnerskaber med tredjelande** eller enheder, der er beliggende i disse lande. Yderligere indsats vil også i fremtiden være **afgørende** for at styrke den globale sikkerhed[9].

Allerede ved forordning (EU) 2022/991 blev der indført væsentlige ændringer af Europolforordningen for at styrke **den eksterne dimension af Europols aktiviteter**, navnlig ved at lette udvekslingen af oplysninger med tredjelande[10] og ved at kræve, at Europol medtager en strategi for forbindelser med tredjelande og internationale organisationer i sin flerårige programmering og sine årlige arbejdsprogrammer[11].

Ved **Europolforordningens artikel 4, stk. 1, litra t),** fik Europol tildelt en ny opgave: at støtte medlemsstaterne i behandlingen af oplysninger, der er meddelt Europol af tredjelande eller internationale organisationer, om personer, der er involveret i terrorisme eller i grov

---

8 Den Europæiske Unions charter om grundlæggende rettigheder, (EUT C 326 af 26.10.2012, s. 391, ELI: http://data.europa.eu/eli/treaty/char_2012/oj).

9 Se ProtectEU – en EU-strategi for indre sikkerhed (COM(2025) 148 final), 1.4.2025, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52025DC0148.

10 Se f.eks. Europolforordningens artikel 25, stk. 4a, der giver Europol mulighed for at videregive oplysninger til tredjelande efter Europols egen vurdering af alle forhold i forbindelse med videregivelsen af personoplysninger og har konkluderet, at der findes de fornødne garantier hvad angår beskyttelsen af personoplysninger, samt Europolforordningens artikel 25, stk. 5, der udvider anvendelsesområdet for de behørigt begrundede tilfælde, hvor Europol kan give ad hoc-tilladelse til videregivelse eller en kategori af videregivelser af personoplysninger til tredjelande og internationale organisationer.

11 Europolforordningens artikel 12, stk. 2.

kriminalitet. Dette omfatter **at foreslå medlemsstaterne eventuel indlæsning af indberetninger med oplysninger om tredjelandsstatsborgere i Unionens interesse i Schengeninformationssystemet (SIS)**. Denne nye kategori af indberetninger med oplysninger blev indført i 2022[12] efter en ændring af forordning (EU) 2018/1862 om brug af SIS på området politisamarbejde og strafferetligt samarbejde[13].

Visse oplysninger, især når den pågældende person ikke er EU-borger, og der ikke er nogen forbindelse til en national sag, deles af tredjelandet kun med Europol, som behandler oplysningerne og deler sine analyseresultater med alle medlemsstater. Formålet med de nye bestemmelser var at **maksimere udnyttelsen af oplysninger** modtaget af Europol fra tredjelande ved at gøre dem mere tilgængelige, end hvis de kun var tilgængelige via Europols eget system. Dette supplerede andre foranstaltninger, f.eks. den europæiske søgeportal (ESP) og interoperabilitetsrammen[14] mellem EU's informationssystemer for sikkerheds-, grænse- og migrationsforvaltning, som skulle afhjælpe de strukturelle mangler ved disse systemer, der hæmmer de nationale myndigheders og navnlig grænsevagternes arbejde.

SIS anses for at være en **vigtig supplerende formidlingskanal**: Det er den mest udbredte database i Europa for retshåndhævelse, grænsekontrol og migration. I 2024 blev der foretaget over 15 mia. søgninger i SIS, sammenlignet med ca. 14 mio. søgninger i Europols informationssystem (EIS) og færre end 3 mia. søgninger (på verdensplan) i de 19 Interpol-databaser, som er de to andre førende informationssystemer for kompetente myndigheder[15].

(2) Innovation: Europolforordningens artikel 18, stk. 2, litra e), og artikel 33a om Europols behandling af personoplysninger med henblik på innovations- og forskningsprojekter

Den teknologiske udvikling medfører både enorme muligheder og betydelige udfordringer for EU's indre sikkerhed[16] og har haft en så dybtgående indvirkning på kriminaliteten, at den har ændret selv den grundlæggende karakter, "DNA'et", af trusler om grov og organiseret kriminalitet[17]. Kriminelle er hurtige til at integrere nye teknologier i deres aktiviteter, skabe nye forretningsmodeller og forfine deres taktik. Samtidig giver disse fremskridt **de retshåndhævende myndigheder hidtil usete muligheder for at styrke deres kapaciteter**. Derfor spiller forskning og innovation en afgørende rolle for den indre sikkerhed, idet der derigennem kan udvikles løsninger til at imødegå nye trusler og holde trit med de kriminelle netværks hastigt udviklende former og arbejdsmetoder, herunder dem, der opstår som følge af misbrug af teknologi. EU har investeret og vil fortsat investere i udviklingen af innovative værktøjer gennem EU-finansieret forskning og innovation på sikkerhedsområdet under **ProtectEU**, EU-strategien for indre sikkerhed[18].

---

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

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

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

15 eu-LISA's årsrapport om SIS 2024, tilgængelig online her: https://www.eulisa.europa.eu/sites/default/files/documents/sis-annual-report-2024.pdf, Europols konsoliderede årsberetning (CAAR) 2024, tilgængelig online her: https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF, og https://www.interpol.int/How-we-work/Databases.

16 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2024*, tilgængelig online her: Internet Organised Crime Threat Assessment (IOCTA) 2024 | Europol.

17 Europol, EU SOCTA 2025, s. 19.

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

Europols innovationslaboratorium (EIL)[19] blev oprettet i slutningen af 2019 på mandat fra EU-medlemsstaternes RIA-ministre og har til formål at fremme Europols engagement i innovation inden for retshåndhævelse. Ved forordning (EU) 2022/991 blev der indført væsentlige ændringer af Europolforordningen for at styrke Europols mandat på innovationsområdet med henblik på både at støtte EIL's potentiale og fremme synergier med andre forsknings- og innovationsaktiviteter på EU-plan, herunder navnlig i Kommissionen, inden for rammerne af **Det Europæiske Innovationscenter for Indre Sikkerhed**[20].

Europolforordningens artikel 18, stk. 2, om formålene med informationsbehandlingsaktiviteter blev ændret for at gøre det muligt for Europol at **behandle operationelle personoplysninger med henblik på forsknings- og innovationsprojekter**. Tilgængeligheden af datasæt af høj kvalitet, der muliggør empirisk prøvning af nye værktøjers gyldighed, betragtes i vid udstrækning som en central forudsætning for udvikling af teknologier. Derimod kan anvendelse af upålidelige eller skæve datasæt i prøvninger bevirke, at der udvikles dårlige teknologier[21].

Skræddersyede databeskyttelsesgarantier for en sådan behandling blev fastlagt i **Europolforordningens artikel 18, stk. 3a, artikel 30, stk. 2 og 3, og artikel 33a**. I henhold til sidstnævnte artikel skal der oprettes et **sandkassemiljø**, idet det fastsættes, at personoplysninger, der behandles i forbindelse med et projekt, midlertidigt skal kopieres til et separat, isoleret og beskyttet databehandlingsmiljø i Europol, som udelukkende må anvendes til det pågældende projekt.

(3) <u>Strafferetlig efterforskning</u>: Europolforordningens artikel 18, stk. 6a, og artikel 18a om betingelserne for behandling af personoplysninger, der modtages uden kategorisering af registrerede

I sin rolle som **EU's knudepunkt for strafferetlige oplysninger** letter Europol ikke blot indsamlingen og udvekslingen af oplysninger, men hjælper også med at **øge effektiviteten af efterforskninger gennem avanceret dataanalyse** og ved at afsløre forbindelser mellem strafbare handlinger og kriminelle netværk på tværs af grænser, som ikke er synlige på nationalt plan. Disse kapaciteter støtter medlemsstaterne ved at berige de oplysninger, der er tilgængelige for deres strafferetlige efterforskninger.

Med den omfattende og intensive brug af teknologi **er store og komplekse datasæt blevet det nye normale i alle aspekter af tilværelsen**, herunder kriminalitet[22]. Efterforskninger af organiseret kriminalitet eller terrorisme står i dag over for udfordringen med at analysere store mængder elektronisk lagrede data, ofte mange terabytes, herunder lyd-, video- og maskingenererede data, der er beslaglagt under efterforskningerne. Efterforskerne i den fælles efterforskning for at demontere EncroChat-netværket[23] analyserede f.eks. flere millioner meddelelser, som kriminelle udvekslede for at planlægge alvorlige forbrydelser. På denne baggrund er det afgørende, at de retshåndhævende og retslige myndigheder har adgang til IKT-værktøjer, -ekspertise og -ressourcer, der kræves for at analysere store og komplekse datasæt (også kaldet "big data"[24]).

---

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

20 Se navnlig Europolforordningens artikel 4, stk. 1, litra v) og w).

21 SWD(2020) 543 final af 9.12.2020, 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 EDPS, udtalelse 7/2015, s. 7, findes på https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf. "Som en fællesnævner for de forskellige tilgængelige definitioner henviser "**big data**"

Selv om Europolforordningen, der blev vedtaget i 2016, ikke som sådan indførte begrænsninger for analysen af big data, manglede den strukturerede bestemmelser, som fastsætter betingelserne for analysen af denne type data. Det mest **kritiske punkt** var **kravet om kategorisering af registrerede**. Kategorisering af registrerede henviser til behovet for at screene datasættene for at sortere personoplysninger i henhold til forskellige kategorier, der er udtømmende anført i bilag II.A og bilag II.B til Europolforordningen, inden der foretages en egentlig behandling af oplysningerne til efterforskningsformål, herunder inden der foretages krydstjek af oplysninger for at opdage forbindelser, eller inden der foretages analyser af strategisk eller tematisk art eller operationelle analyser[25]. De relevante kategorier er knyttet til forskellige former for involvering i strafferetlige efterforskninger, herunder i) mistænkte, potentielle fremtidige lovovertrædere, samt ii) kontakter, samarbejdspartnere, ofre, vidner og informanter med tilknytning til kriminelle aktiviteter. Generelt kan Europol ikke behandle eller endda lagre personoplysninger om personer, der ikke falder ind under nogen af disse kategorier.

Dataleverandører, f.eks. **medlemsstater** eller **EU-organer og -agenturer**, udfører typisk allerede kategorisering af registrerede, inden personoplysningerne overføres til Europol[26]. I henhold til EU-retten er de alle forpligtet til at udføre kategorisering af registrerede i forbindelse med deres egen behandling og efterforskning, uanset overførslen af oplysninger til Europol, og i overensstemmelse med regler, der svarer til, men ikke er identiske med, de regler, der gælder for Europol[27]. For store og komplekse datasæt er manuel forbehandling dog en ressourcekrævende og tidskrævende opgave. Analyse af data i en enkelt mobiltelefon kan med halvautomatisk behandling tage op til tre dage, og der beslaglægges måske flere hundrede mobiltelefoner under en efterforskning. Kategorisering af registrerede **i forbindelse med big data** er **ikke altid muligt** som følge af datasættenes store omfang, den måde, hvorpå dataene er (u)strukturerede, manglen på ressourcer eller den uforholdsmæssige **manuelle indsats, der kræves**. I praksis er den eneste mulighed først at analysere dataene mere indgående ud fra et operationelt synspunkt eller at opdage forbindelser, også gennem halvautomatisk behandling, ved at krydstjekke tilgængelige data.

I forordning (EU) 2022/991 præciseres betingelserne for, at kategorisering af registrerede kan give **retssikkerhed** i forbindelse med behandlingen af store og komplekse datasæt. Europol og Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) havde forskellige fortolkninger af Europolforordningens ordlyd og ånd med hensyn til den gældende datalagringsperiode. Ifølge Europol bør denne periode være tre år. Ifølge EDPS bør den være seks måneder[28]. Der var også behov for nye bestemmelser for at give **yderligere fleksibilitet** og sikre en passende balance mellem databeskyttelse og sikkerhed.

---

generelt til den praksis, hvor enorme mængder meget forskellige oplysninger kombineres og analyseres, ofte ved hjælp af selvlærende algoritmer, med henblik på at træffe informerede beslutninger. Big data udnytter ikke kun teknologiens stigende evne til at understøtte indsamling og lagring af store mængder data, men også dens evne til at analysere, forstå og udnytte den fulde værdi af data (især ved hjælp af analyseapplikationer)".

25 Se Europolforordningens artikel 18, stk. 2.

26 Medlemsstaterne overfører data til Europol via dets netværksprogram til sikker informationsudveksling (SIENA), hvor kategorisering af registrerede er implementeret som et obligatorisk felt.

27 Se f.eks. artikel 6 i direktiv (EU) 2016/680 ("retshåndhævelsesdirektivet" for så vidt angår indirekte kompetente myndigheder) EUT L 119 af 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj), artikel 51 i Rådets forordning (EU) 2017/1939 ("EPPO-forordningen") (EUT L 283 af 31.10.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj) og artikel 27, stk. 3, i forordning (EU) 2018/1727 ("Eurojustforordningen") (EUT L 295 af 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.

I Europolforordningens artikel 18, stk. 5a, sammenholdt med artikel 73 i EUDPR, præciseres først yderligere det generelle princip for kategorisering af registrerede i henhold til artikel 18, stk. 2, og bilag II. Europol har til opgave, hvor det er relevant og så vidt muligt, at foretage en **klar tildeling af personoplysninger til en bestemt kategori af registrerede**. I praksis bør Europol som hovedregel fastlægge den præcise rolle i den kriminelle aktivitet (f.eks. om en person er mistænkt, offer eller kun vidne) for hver person, hvis personoplysninger skal behandles, og ikke på et aggregeret niveau for alle personer i en datafil, der skal behandles, eller en del heraf (f.eks. ved blot at fastslå, at alle de nævnte personer er involveret i en kriminel aktivitet, der falder ind under dens mandat, på grundlag af en undersøgelse af de generelle omstændigheder, der genererede datafilen), før personoplysninger kan behandles.

I Europolforordningens artikel 18, stk. 6a, tillades udtrykkeligt behandling af personoplysninger, der modtages uden kategorisering af registrerede, i **op til 18 måneder**, hvilket kan forlænges til op til 36 måneder i begrundede tilfælde, udelukkende med **det formål at færdiggøre kategorisering af registrerede**. I Europolforordningens artikel 18, stk. 6a, henvises der ikke udtrykkeligt til store og komplekse datasæt, idet der generelt kun kræves en test af "**streng nødvendighed**".

I Europolforordningens artikel 18a fastsættes der en undtagelse, som gør det muligt for Europol at behandle personoplysninger, der modtages fra en **kompetent myndighed**, Den Europæiske Anklagemyndighed (**EPPO**) eller **Eurojust**, hvor det er nødvendigt for at støtte en **igangværende strafferetlig efterforskning**, uden at det er nødvendigt at udføre kategorisering af registrerede, hvis dette ikke allerede er udført, og ud over de kategorier af registrerede, der er anført i Europolforordningen. Europol kan behandle oplysningerne gennem **operationel analyse** eller i særlige og behørigt begrundede tilfælde ved **krydstjek** for at finde sammenhænge eller andre relevante forbindelser. Denne undtagelse var udformet med henblik på at afhjælpe forskellene mellem de regler om kategorisering af registrerede, der gælder for Europol, og de regler, der gælder for de kompetente myndigheder, EPPO og Eurojust.

(4) Samarbejde med tredjemand: Europolforordningens artikel 26, 26a og 26b om udveksling af personoplysninger mellem Europol og private parter

Kriminelle misbruger i stigende grad private parters (grænseoverskridende) tjenester – internetbaserede, finansielle og klassiske telekommunikationstjenester. Som følge heraf **er private parter i besiddelse af en stor mængde personoplysninger, der er relevante for strafferetlige efterforskninger**. Internettet har skabt et offentligt rum, der reelt er på private hænder, og det gør det vanskeligt at håndhæve regler online med henblik på retshåndhævelse lige så effektivt som offline[29].

På denne baggrund er **samarbejde mellem retshåndhævende myndigheder og private parter** blevet **en nødvendighed.** Som anført i **ProtectEU**, EU-strategien for indre sikkerhed, vil det være afgørende at styrke partnerskaber med den private sektor for at lette udvekslingen af oplysninger[30]. Politicheferne har også i deres fælles erklæring om Europols fremtid[31] opfordret til, at Europol skal fungere som en **vital gateway til indhentning af oplysninger fra private enheder**. Karakteren af dette samarbejde spænder fra udveksling af oplysninger og levering af kommercielle open source-data til deltagelse i forsknings- og innovationsprojekter

29 SWD(2020) 543 final af 9.12.2020, s. 16.

30 Se ProtectEU – en EU-strategi for indre sikkerhed, s. 6.

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

og levering af tjenester, der understøtter virksomheders funktion[32]. Eksempelvis lykkedes det i 2025 Europol at forstyrre Lumma Stealer, verdens mest betydningsfulde infostealer-trussel, gennem samarbejde med Microsoft, som havde identificeret over 394 000 Windows-computere globalt, der var inficeret med Lumma-malware[33].

Ved forordning (EU) 2022/991 fik Europol **yderligere muligheder** for at udveksle personoplysninger med private parter. Tidligere kunne Europol kun modtage personoplysninger fra private parter via en national Europolenhed (ENU) eller gennem forhåndsudpegede kontaktpunkter eller myndigheder i tredjelande eller internationale organisationer. Formålet med Europols behandling var begrænset til at identificere den relevante ENU eller det kontaktpunkt eller den myndighed i tredjelandet og den internationale organisation, der kunne påtage sig ansvaret for sagen.

Ved den **ændrede artikel 26 i Europolforordningen blev Europols opgave** udvidet, og agenturet fik mulighed for at behandle oplysninger (herunder personoplysninger) fra private parter på en omfattende måde. Et primært formål med behandlingen er fortsat at identificere den pågældende nationale Europolenhed (ENU). Europol har imidlertid nu også mulighed for at supplere oplysningerne med sin egen analyse for at lette den videre behandling af en sag på nationalt plan.

Ud over de horisontale bestemmelser i Europolforordningens artikel 26 blev der ved forordningens artikel 26a indført regler for **onlinekrisesituationer**, og artikel 26b omhandlede **onlineudbredelsen af onlinemateriale, der viser seksuelt misbrug af børn**. I sådanne tilfælde kan Europol bistå medlemsstaterne ved at behandle personoplysninger, der modtages direkte fra private parter. Europol kan også på ad hoc-grundlag videregive personoplysninger til private parter.

Ved forordning (EU) 2022/991 blev der indført mulighed for at anvende Europols infrastruktur til udveksling af oplysninger mellem kompetente myndigheder og private parter samt mulighed for, at Europol kan anmode medlemsstaterne om – i overensstemmelse med deres nationale lovgivning – at indhente personoplysninger fra private parter.

Disse bestemmelser blev vedtaget i sammenhæng med andre initiativer, f.eks. forordningen om håndtering af udbredelsen af terrorrelateret indhold online[34] og forordningen om digitale tjenester[35]. Der planlægges yderligere foranstaltninger med henblik på at styrke inddragelsen af private parter i bekæmpelsen af kriminalitet og lette lovlig adgang til data for at realisere "en ambition om at ændre kulturen på sikkerhedsområdet" (**en tilgang, som inddrager hele samfundet**) under **ProtectEU**, EU-strategien for indre sikkerhed[36].

(5) Internt og eksternt tilsyn med Europols overholdelse af grundlæggende rettigheder

---

32 Europol, *Cooperation with Private Parties*, 31.5.2023, EDOC #1306090v13. Se også Milieu Consulting, *Study on the Practice of direct exchanges with of personal data between Europol and Private Parties*, Final Report, september 2020.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Flere eksempler kan i det ledsagende arbejdsdokument fra Kommissionens tjenestegrene.

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

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

36 Se ProtectEU – en EU-strategi for indre sikkerhed, s. 2.

I forordning (EU) 2022/991 understreges Europols forpligtelse til at respektere de grundlæggende rettigheder i henhold til de bestemmelser, der definerer Europols opgaver, og de styrkede relaterede garantier, navnlig ved **at styrke agenturets interne og eksterne tilsyn**.

På databeskyttelsesområdet indebar tilpasningen af Europolforordningen til databeskyttelsesgarantierne i henhold til EUDPR, at der blev indført nye regler for det tilsyn, der udføres af **databeskyttelsesrådgiveren** og **Den Europæiske Tilsynsførende for Databeskyttelse** (EDPS). Forpligtelsen til at foretage en konsekvensanalyse vedrørende databeskyttelse og forudgående høring af EDPS er f.eks. blevet systematisk for enhver ny type behandling. Ved forordning (EU) 2022/991 blev der også indført en ny kompetence for Europol vedrørende anmodninger om indsigt. Tidligere var de nationale kompetente myndigheder ansvarlige for at behandle anmodninger om indsigt, hvis medlemsstaterne var dataleverandører.

Ved forordning (EU) 2022/991 blev der også oprettet en **ny stilling som ansvarlig for grundlæggende rettigheder** i Europol, som bl.a. har til opgave at underrette Europols administrerende direktør om mulige krænkelser af de grundlæggende rettigheder i forbindelse med agenturets aktiviteter.

Derudover blev **demokratisk kontrol og ansvarlighed styrket** gennem politisk overvågning af Europols aktiviteter af **Europa-Parlamentet og de nationale parlamenter**, jf. artikel 88, stk. 2, andet afsnit, i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Forordning (EU) 2022/991 styrkede den overvågning, der foretages af **Gruppen for Fælles Parlamentarisk Kontrol** (JPSG)[37]. Det bestemmes f.eks., at det er obligatorisk at høre JPSG om Europols udkast til flerårig programmering og årlige arbejdsprogrammer, at JPSG kan rette ikkebindende specifikke henstillinger til Europol og forelægge dem for Europa-Parlamentet og de nationale parlamenter, og at der oprettes et rådgivende forum, der på anmodning skal bistå JPSG ved at yde uafhængig rådgivning om spørgsmål vedrørende grundlæggende rettigheder.

3. De vigtigste resultater af evalueringen

3.1. Status for den operationelle gennemførelse af Europols nye beføjelser og opgaver vedrørende behandling af personoplysninger

Forordning (EU) 2022/991 **trådte i kraft den 28. juni 2022**. Dens operationelle gennemførelse var imidlertid afhængig af forskellige forvaltningsmæssige, tekniske og administrative foranstaltninger samt operationelle krav som f.eks. oprettelse af nye IKT-strukturer i visse tilfælde.

Tre år senere er **næsten alle de bestemmelser**, der er opført i artikel 68, stk. 3, i forordning (EU) 2022/991, **blevet operationelle**. Bestemmelserne vedrørende analyse af store og komplekse datasæt (Europolforordningens artikel 18, stk. 6a, og artikel 18a) og samarbejde med private parter (Europolforordningens artikel 26, 26a og 26b) begyndte at finde anvendelse fra den 28. juni 2022 eller kort tid derefter. Behandlingen af personoplysninger til forsknings- og innovationsprojekter (Europolforordningens artikel 18, stk. 2, litra e)) begyndte i 2023, efter at sandkassemiljøet, kaldet ODIN, blev oprettet for at opfylde de specifikke databeskyttelseskrav i Europolforordningens artikel 33a. Den 29. juni 2025 var muligheden for, at Europol kan foreslå **SIS-indberetninger** til medlemsstaterne i overensstemmelse med Europolforordningens artikel 4, stk. 1, litra t), endnu ikke blevet operationel, da den tekniske gennemførelse af den nye type indberetning stadig er i gang. Denne mulighed forventes at blive operationel i **2026**.

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

3.2. Evaluering af den operationelle indvirkning af Europols nye beføjelser og opgaver vedrørende behandling af personoplysninger på agenturets målsætninger i henhold til Europolforordningens artikel 3

Med hensyn til den operationelle virkning af Europols nye beføjelser og opgaver vedrørende behandling af personoplysninger fremgik det af høringen, at **medlemsstaterne generelt har et positivt syn** på deres relevans, effektivitet og merværdi samt på Europols støtte til deres kompetente myndigheder på de relevante områder[38].

De undersøgelsesbeføjelser, der er omfattet af denne evaluering, anvendes ikke løbende eller systematisk til at behandle oplysninger med henblik på overvågning. Nogle er endda af ekstraordinær karakter, mens andre efter behov anvendes mere regelmæssigt i undersøgelser. **Kvantitativt** afveg den **operationelle anvendelse af de nye bestemmelser** i referenceperioden **væsentligt** afhængigt af de forskellige tekniske karakteristika og retlige betingelser, der er forbundet med de nye bestemmelser.

Europol har modtaget et **ikke uvæsentligt** antal **nye bidrag uden kategorisering af registrerede** fra medlemsstaterne i henhold til Europolforordningens artikel 18, stk. 6a, som nåede op på 653 i 2023 og 597 i 2024. Der var ingen kortsigtet stigning i antallet af bidrag uden kategorisering af registrerede, og antallet af tilfælde, hvor artikel 18, stk. 6a, blev anvendt, forblev **stabilt** sammenlignet med tilsvarende sager i perioden før den 28. juni 2022. De nye bestemmelser havde heller ingen negativ indvirkning på medlemsstaternes engagement i gennemførelsen af kategorisering af registrerede[39]. Mellem 2023 og 2024 udgjorde andelen af bidrag uden kategorisering af registrerede **mindre end 1 % af alle bidrag**, som Europol accepterede fra medlemsstaterne (0,85 % i 2023 og 0,71 % i 2024). Siden juni 2022 har Europol konsekvent afsluttet kategoriseringen af registrerede inden for 18 måneder uden at benytte den forlængede periode på 36 måneder. Europol og seks medlemsstater understregede, at **den administrative byrde** – på trods af den forbedrede retssikkerhed – **forblev betydelig** for både Europol og de kompetente myndigheder på grund af den indsats, der kræves for at overholde kategoriseringen af personoplysninger efter den enkeltes deltagelse i den strafbare handling. Dette krav gennemføres meget strengt af Europol[40].

Europol rapporterede, at udvekslingen af oplysninger med **private parter** stadig var ubetydelig i 2023, da der kun blev registreret 26 tilfælde, hvor Europolforordningens artikel 26 blev gennemført (ud over de tilfælde, der falder ind under retsakten om digitale tjenester)[41]. I **2024** viste statistikkerne imidlertid en **kraftig stigning til 284** (næsten + 1 000 %) sager, der involverede samarbejde med private parter under Europolforordningens artikel 26. Dette var især tilfældet for data fra private virksomheder til brug for efterforskning af **finansiel og økonomisk kriminalitet**. Europol gjorde også betydelig brug af Europolforordningens artikel 26b i bekæmpelsen af seksuel udnyttelse af børn, hvor samarbejdet med private parter allerede tidligere var meget omfattende. I begge tilfælde omfatter dataene også samarbejde, der var muligt under den tidligere retlige ramme. Det fremgår ikke af de tilgængelige data, i hvilket

---

38 Se dokumentation fremlagt i afsnit 5 i det arbejdsdokument fra Kommissionens tjenestegrene, der ledsager denne rapport, og navnlig Europols indlæg og medlemsstaternes svar på spørgsmål 2, 4 og 5 i det korte spørgeskema af 2.6.2025 i bilag III til arbejdsdokumentet fra Kommissionens tjenestegrene.

39 Som en medlemsstat understregede under høringen, kan "[medlemsstaterne] klart skelne mellem, hvilken type data [de] skal håndtere, hvilket kan være meget vigtigt i selve efterforskningen".

40 Se underafsnit 7.1.3. i det arbejdsdokument fra Kommissionens tjenestegrene, der ledsager denne rapport, samt medlemsstaternes svar på spørgsmål 9 i det korte spørgeskema af 2.6.2025 i bilag III til arbejdsdokumentet fra Kommissionens tjenestegrene.

41 Europol, 2023-rapport i henhold til Europolforordningens artikel 16, stk. 11.

omfang disse nye sager falder ind under de nye bestemmelser eller skyldes en øget anvendelse af de eksisterende muligheder.

I **2025** vedtog Europol en **ny strategi** for yderligere at styrke samarbejdet med private parter. Der er også truffet foranstaltninger med det formål at opgradere Europols IKT-infrastruktur, som er tilgængelig for de kompetente myndigheder med henblik på udveksling af oplysninger med private parter. I **2023** lancerede Europol *Plateforme Européenne de Retraits de Contenus Illégaux sur Internet* (**PERCI**), som skal lette gennemførelsen af forordningen om håndtering af udbredelsen af terrorrelateret indhold online og i fremtiden muligvis også artikel 18 i forordningen om digitale tjenester, samt *EU Child Abuse Referral Service* **(EU CARES)**. PERCI er ikke integreret i Europols informationssystem (EIS)[42].

Andre bestemmelser blev **slet ikke anvendt** (Europolforordningens artikel 26a), selv om de var operationelle, **eller** blev kun anvendt **undtagelsesvis** (ét tilfælde, hvor Europolforordningens artikel 18a blev anvendt i 2024, ét projekt blev gennemført med behandling af personoplysninger i henhold til Europolforordningens artikel 18, stk. 1, litra t), i 2025, og tre nye projekter er allerede i pipelinen).

På grund af den begrænsede periode for den operationelle gennemførelse af de bestemmelser, der blev indført ved forordning (EU) 2022/991, og den langvarige karakter af strafferetlige efterforskninger og retssager var medlemsstaterne ikke i stand til at fremlægge kvantitative data om virkningen af disse bestemmelser i operationel henseende. De gav i stedet nogle eksempler på vellykkede efterforskninger, der viser de **håndgribelige fordele ved de nye efterforskningsmuligheder i virkelige situationer** for de bestemmelser, der allerede er i brug, f.eks. EncroChat, Sky ECC, Balkanbaserede kriminelle netværk, der er involveret i kokainhandel, eller Lumma Stealer.

Europol og otte medlemsstater pegede også på enkelte **områder, hvor der kan ske forbedringer**, for at maksimere den effektive og sammenhængende anvendelse af den nye retlige ramme og styrke Europols rolle i fremtiden. Der er bekymring, navnlig fra Europols side, for, at de alt for komplekse, fragmenterede og omfattende retlige bestemmelser kan afholde fagfolk eller private parter fra at anvende de nye tilgængelige instrumenter. Medlemsstaternes bemærkninger vedrører snarere den måde, hvorpå Europol restriktivt gennemfører databeskyttelsesgarantier under EDPS' tilsyn, hvilket risikerer at underminere effektiviteten og merværdien af visse bestemmelser.

3.3. Vurdering af indvirkningen af Europols nye beføjelser og opgaver vedrørende behandling af personoplysninger på de grundlæggende rettigheder

Kommissionen fandt **ingen** dokumentation for en **negativ indvirkning på de grundlæggende rettigheder** som følge af den operationelle anvendelse af de nye beføjelser til behandling af personoplysninger baseret på den indtil videre begrænsede anvendelse af de nye beføjelser til behandling af personoplysninger.

Ud over at gennemføre de specifikke databeskyttelseskrav, der er forbundet med de nye beføjelser til behandling af personoplysninger, har Europol gradvist truffet alle nødvendige foranstaltninger for at gennemføre de nye horisontale tilsynsmekanismer vedrørende grundlæggende rettigheder.

I 2024 vedtog Europols bestyrelse de reviderede gennemførelsesbestemmelser for databeskyttelsesrådgiveren som en af de sidste nødvendige gennemførelsesretsakter vedrørende den nye databeskyttelsesordning. Den indsamlede dokumentation tyder på, at Europol og dets bestyrelse også i samarbejde med Europols databeskyttelsesrådgiver og EDPS

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

har sikret en **streng gennemførelse af de nye databeskyttelsesgarantier**, der blev indført i 2022. Denne tilgang har umiddelbart effektivt forhindret enhver negativ indvirkning eller indblanding fra den første anvendelse af de nye beføjelser til behandling af personoplysninger på personers ret til privatlivets fred og beskyttelse af personoplysninger. Ifølge medlemsstaterne har Europol aktuelt indført en **solid retlig ramme for databeskyttelse**, hvilket sikrer tilstrækkelige garantier for den potentielt øgede anvendelse af agenturets nye beføjelser. Syv medlemsstater understregede også, at denne ramme **letter informationsstrømmen** ved at øge tilliden, selv om der stadig er plads til forbedringer. Kun én medlemsstat gav udtryk for en negativ holdning[43].

Ud over de specifikke **udfordringer** vedrørende kategorisering af registrerede betegnede Europol og fire medlemsstater de omkostninger og den tid, der er forbundet med **konsekvensanalyser vedrørende databeskyttelse** og **forudgående høring** af Den Europæiske Tilsynsførende for Databeskyttelse, som i praksis gennemføres som standard, som områder, der kan forbedres. En yderligere udfordring, som seks medlemsstater nævnte, er Europols håndtering af **registreredes anmodninger om indsigt**, som Europol nu har kompetence til at behandle, selv når en medlemsstat er dataansvarlig.

Den **første ansvarlige for grundlæggende rettigheder** blev udnævnt i december **2022**. I de første to år af sit mandat har han **ikke** modtaget eller fremsat **klager** til den administrerende direktør. Gruppen for Fælles Parlamentarisk Kontrol har fortsat nøje overvåget Europols aktiviteter og har ikke fremsat henstillinger, siden de nye bestemmelser trådte i kraft. Europa-Parlamentet oprettede **det rådgivende forum for grundlæggende rettigheder under Gruppen for Fælles Parlamentarisk Kontrol** i februar **2024**.

3.4. Cost-benefit-analyse af Europols nye beføjelser og opgaver vedrørende behandling af personoplysninger

I betragtning af den tidlige fase af gennemførelsen af de bestemmelser, der blev indført ved forordning (EU) 2022/991, og de begrænsede erfaringer med dem, er det **for tidligt** for Kommissionen at drage meningsfulde konklusioner om de nye bestemmelser på baggrund af en **cost-benefit-analyse**.

Kommissionens tjenestegrene har indsamlet oplysninger fra Europol om de omkostninger, der hidtil er afholdt i forbindelse med den operationelle gennemførelse af forordning (EU) 2022/991 for de omhandlede bestemmelser. Disse omkostninger beløb sig til ca. **25 mio. EUR** (ca. 5 % af den samlede tildeling til Europol[44]) mellem 2022 og 2025 og bestod primært af engangsomkostninger. Medlemsstaterne har til dato ikke afholdt relevante nye omkostninger, der specifikt er knyttet til forordning (EU) 2022/991.

De fleste omkostninger (næsten 17 mio. EUR) bestod af betydelige investeringer i **udvikling af nye IKT-strukturer**, gennemførelse af bestemmelser om forskning og innovation (sandkassen ODIN) samt informationssystemer til udveksling af personoplysninger med private parter (PERCI og EU CARES). Omkostninger til **menneskelige ressourcer (HR)**, både i forbindelse med IKT og drift, udgjorde cirka en tredjedel af de samlede udgifter (ca. 8 mio. EUR). HR vil tegne sig for **de vigtigste tilbagevendende omkostninger på lang sigt**.

Det skal bemærkes, at ovennævnte 8 mio. EUR ikke omfatter personaleomkostninger for Information Management Unit (IMU) eller de ressourcer, der er forbundet med (tidligere og

---

[43] Se medlemsstaternes svar på spørgsmål 9 i det korte spørgeskema af 2.6.2025 i bilag III til det ledsagende arbejdsdokument fra Kommissionens tjenestegrene.

[44] I samme periode beløb det samlede budget, der var afsat til Europol, sig til ca. **860 mio. EUR** (med en gradvis stigning fra 192 mio. EUR i 2022 til 241 mio. EUR i 2025). Nærmere oplysninger findes i det ledsagende arbejdsdokument fra Kommissionens tjenestegrene.

nye) tilsynsforanstaltninger af horisontal karakter, og for hvilke en opdeling på gennemførelsesniveau for specifikke bestemmelser ikke er mulig. Omkostningerne ved sådanne ressourcer er ikke ubetydelige. I 2023 blev det f.eks. anslået, at **60 årsværk** (næsten **5 %** af Europols personale) var involveret i aktiviteter i **sikrings-/tilsynsorganer og tilsyns-/rådgivningsenheder**. Europol afsatte 25 årsværk til arbejdet med databeskyttelsestilsyn og tilsvarende sikringsforanstaltninger. Dette omfatter opfølgning på EDPS' henstillinger samt arbejde, der er genereret i forbindelse med forudgående høringer om operationel databehandling. 16 af disse 25 årsværk er specifikt beskæftiget med aktiviteter vedrørende EDPS' krav. Pr. juni 2025 har Europol et særligt team på otte fuldtidsansatte inden for databeskyttelse, herunder den databeskyttelsesansvarlige.

Ifølge Europol og 15 medlemsstater forventes det, at **fordelene** ved de nye beføjelser og opgaver vedrørende behandling af personoplysninger, navnlig analyse af store og komplekse datasæt samt samarbejde med private parter, vil være betydelige og **opveje de dermed forbundne omkostninger**. Ingen medlemsstat var af en anden opfattelse. Der kan med rimelighed forventes visse effektivitetsgevinster på længere sigt, takket være stordriftsfordele og faldende marginalomkostninger. En medlemsstat understregede, at "det er vigtigt, at Europol stiller de nødvendige IKT-ressourcer til rådighed for at tilvejebringe og videreudvikle værktøjerne til gennemførelse af de nye muligheder i forordning (EU) 2022/991", hvilket også blev støttet af to andre medlemsstater og andre interessenter[45].

Efter Europols og fem medlemsstaters opfattelse skal mulig **ineffektivitet** i forbindelse med gennemførelsen også håndteres inden for **den eksisterende ramme for forvaltning, administration og databeskyttelse** for at undgå at underminere den operationelle effekt af de nye opgaver vedrørende behandling af personoplysninger ved at forsinke eller begrænse deres anvendelse. Fem medlemsstater satte spørgsmålstegn ved Europols og dets bestyrelses alt for forsigtige gennemførelse af databeskyttelsesreglerne under vejledning af EDPS. De foreslår, at den fleksibilitet, som fælleslovgiverne har givet, bør udnyttes tilstrækkeligt til at maksimere effektiviteten og virkningen af Europols opgaver og sikre deres relevans og langsigtede rentabilitet.

En evaluering af Europols arbejdsmetoder og potentielle områder for forenkling ligger uden for rapportens omfang Europolforordningens i henhold til artikel 68, stk. 3, og vil blive gennemført inden for rammerne af evalueringen i henhold til Europolforordningens artikel 68, stk. 1.

4. Konklusioner og det videre forløb

Alt i alt er Kommissionens foreløbige hovedkonklusion, at medlemsstaterne fastholder **deres støtte til den rolle, Europol spiller** på de nøgleområder, hvor agenturet i øjeblikket bistår medlemsstaterne med dets **nye opgaver vedrørende behandling af personoplysninger**. For at **maksimere fordelene** ved de nye beføjelser til behandling af personoplysninger er der ifølge nogle interessenter imidlertid behov for at **afhjælpe eventuel ineffektivitet**, navnlig inden for de eksisterende rammer for forvaltning, administration og databeskyttelse. Det vil også være nyttigt at mindske **kompleksiteten og fragmenteringen** af de retlige rammer, der kan afholde fagfolk fra at gøre brug af de nye muligheder.

Kommissionen fandt generelt ikke bevis for, at de nye regler havde en **negativ indvirkning på de grundlæggende rettigheder,** navnlig takket være solide databeskyttelsesgarantier, som

[45] Se dokumentation fremlagt i afsnit 5 i det arbejdsdokument fra Kommissionens tjenestegrene, der ledsager denne rapport, og navnlig Europols indlæg og medlemsstaternes svar på spørgsmål 2, 4 og 5 i det korte spørgeskema af 2.6.2025 i bilag III til arbejdsdokumentet fra Kommissionens tjenestegrene, og den fælles erklæring fra de europæiske politichefer om Europols fremtid.

også letter informationsstrømmen ved at øge partnernes tillid. For nogle medlemsstater valgte agenturet en konservativ tilgang, mens **der bør gøres passende brug af den fleksibilitet, som fælleslovgiverne har givet** for så vidt angår kategoriseringen af registrerede, konsekvensanalysen vedrørende databeskyttelse, forudgående høring af Europols tilsynsførende for databeskyttelse og behandlingen af anmodninger om indsigt.

I betragtning af den generelt korte gennemførelsesperiode for de nye regler om beskyttelse af personoplysninger, der er fastsat i forordning (EU) 2022/991, er det imidlertid ikke muligt at drage endelige konklusioner på alle spørgsmål ud fra det indsamlede materiale.

I **ProtectEU**, EU-strategien for indre sikkerhed[46], meddelte Kommissionen, at den vil foreslå en ambitiøs revision af Europols mandat for at imødegå de eskalerende sikkerhedsudfordringer. I overensstemmelse med sine retningslinjer for bedre regulering[47] indledte Kommissionen forberedelserne til at evaluere Europolforordningen og Europols arbejdsmetoder og banede vejen for et **forslag fra Kommissionen i 2026 om at gøre agenturet mere operationelt, som fastsat i de politiske retningslinjer**[48]. I juli 2025 offentliggjorde Kommissionen en opfordring til indsendelse af dokumentation[49] og indgik kontrakt om en ekstern undersøgelse til støtte for evalueringen af Europolforordningen og konsekvensanalysen af det nye forslag. Den evaluering af Europolforordningen, der er gennemført med henblik på udarbejdelsen af denne rapport, har til formål at bidrage til denne evaluering.

46 ProtectEU – en EU-strategi for indre sikkerhed, s. 10.

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

48 Kommissionens formand, Ursula von der Leyen, Politiske retningslinjer for den næste Europa-Kommission 2024-2029, e6cd4328-673c-4e7a-8683-f63ffb2cf648_da.

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