EUROPESE
COMMISSIE

Brussel, 11.12.2025
COM(2025) 752 final

VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

ter evaluatie en beoordeling van de operationale impact van de uitvoering van de taken waarin in Verordening (EU) 2022/991 wordt voorzien, met name in artikel 4, lid 1, punt t), artikel 18, lid 2, punt e), artikel 18, lid 6 bis, en de artikelen 18 bis, 26, 26 bis en 26 ter, met betrekking tot de doelstellingen van Europol, en de impact van die taken op de grondrechten en fundamentele vrijheden, zoals die zijn vastgelegd in het Handvest, overeenkomstig artikel 68, lid 3, van Verordening (EU) 2016/794

{SWD(2025) 404 final}

1. Reikwijdte van de evaluatie

Sinds het operationeel werd in 1999, heeft **het EU-agentschap voor samenwerking op het gebied van rechtshandhaving (Europol) een centrale rol gespeeld bij de bestrijding van zware grensoverschrijdende criminaliteit en terrorisme**, waardoor het een belangrijke drijvende kracht voor samenwerking bij de rechtshandhaving in Europa is geworden. De veiligheidssituatie is de afgelopen dertig jaar drastisch veranderd, met een overeenkomstige verschuiving in het DNA van de zware en georganiseerde criminaliteit[1]. De lidstaten hebben nieuwe operationele behoeften op het gebied van de effectieve aanpak van opkomende dreigingen, en hun **verwachtingen ten aanzien van de steun van Europol zijn** eveneens **veranderd**. Het mandaat van Europol is derhalve herhaaldelijk vernieuwd of gewijzigd om de relevantie van het agentschap te behouden en te vergroten.

Het mandaat van Europol, zoals vastgesteld in Verordening (EU) 2016/794[2] ("de Europol-verordening"), werd voor het laatst in 2022 gewijzigd bij Verordening (EU) 2022/991[3] om nieuwe veiligheidsdreigingen aan te pakken. De Europol-verordening was niet langer geschikt voor het beoogde doel in een nieuwe realiteit waarin criminelen de voordelen van **digitale transformatie**, **nieuwe technologieën**, **globalisering** en **mobiliteit** uitbuiten[4].

De **specifieke doelstellingen** van Verordening (EU) 2022/991[5] waren:

- een doeltreffende samenwerking tussen **particuliere partijen** en rechtshandhavingsautoriteiten mogelijk maken om misbruik van grensoverschrijdende diensten door criminelen tegen te gaan;
- rechtshandhavingsautoriteiten in staat stellen **grote en complexe datasets** te analyseren om grensoverschrijdende verbanden op te sporen, met volledige inachtneming van de **grondrechten**;
- lidstaten in staat stellen **nieuwe technologieën** te gebruiken voor rechtshandhaving.

Daarnaast zijn bij Verordening (EU) 2022/991 de op Europol van toepassing zijnde gegevensbeschermingsvoorschriften gewijzigd om een **hoog niveau van gegevensbescherming** te behouden, waarmee een evenwicht is bereikt tussen de nieuwe bevoegdheden van het agentschap om persoonsgegevens te verwerken en de bescherming van de persoonlijke levenssfeer en persoonsgegevens. Om **de informatiestroom te vergemakkelijken**, zijn bij deze verordening de op Europol van toepassing zijnde gegevensbeschermingsvoorschriften grotendeels in overeenstemming gebracht met die welke op andere EU-agentschappen en -organen op het gebied van justitie en binnenlandse zaken van toepassing zijn krachtens hoofdstuk IX van Verordening (EU) 2018/1725 ("de gegevensbeschermingsverordening van de EU" of "EUVG") en die welke op de rechtshandhavingsautoriteiten van de lidstaten ("bevoegde autoriteiten") van toepassing zijn krachtens hun nationale wetgeving tot omzetting van Richtlijn (EU) 2016/680 ("de richtlijn rechtshandhaving")[6].

---

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

2 PB L 135 van 24.5.2016, blz. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj.

3 PB L 169 van 27.6.2022, blz. 1, ELI: http://data.europa.eu/eli/reg/2022/991/oj.

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

5 Idem.

6 PB L 119 van 4.5.2016, blz. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

Dit verslag is vastgesteld in overeenstemming met de verplichting van de Commissie krachtens **artikel 68, lid 3, van de Europol-verordening** om de operationele impact van de in Verordening (EU) 2022/991 vastgelegde taken van Europol drie jaar na de inwerkingtreding van deze verordening te evalueren[7] en te beoordelen. Overeenkomstig het mandaat van de medewetgevers heeft de Commissie ten eerste de **operationele impact** van enkele van de nieuwe regels voor de verwerking van persoonsgegevens geëvalueerd en beoordeeld, ten opzichte van de doelstellingen van Europol, krachtens artikel 3 van de Europol-verordening (namelijk het ondersteunen en versterken van het optreden van de bevoegde autoriteiten van de lidstaten en hun wederzijdse samenwerking bij de voorkoming en bestrijding van strafbare feiten die onder het mandaat van Europol vallen), ten tweede de impact van die regels op de in het Handvest[8] vastgelegde **grondrechten en fundamentele vrijheden** ("grondrechten") beoordeeld, en ten derde een **kosten-batenanalyse** van de daarmee verband houdende gegevensverwerkingstaken uitgevoerd.

Ter voorbereiding van de herziening hebben de diensten van de Commissie informatie en feedback verzameld uit verschillende bronnen en ad-hocraadplegingen gehouden met Europol en de lidstaten. Het begeleidende **werkdocument van de diensten van de Commissie** bevat een gedetailleerde beschrijving van de algemene context en methodologie van de herziening, alsook een uitgebreid overzicht van de bronnen van bewijsmateriaal en raadplegingen die de in dit verslag samengevatte belangrijkste bevindingen bevestigen.

2. Algemene context

Overeenkomstig artikel 68, lid 3, van de Europol-verordening heeft dit verslag van de Commissie betrekking op een aantal bepalingen van Verordening (EU) 2022/991, waarbij de nadruk ligt op vijf belangrijke aspecten van de werkzaamheden van Europol.

(1) Externe dimensie: artikel 4, lid 1, punt t), van de Europol-verordening over informatiesignaleringen van onderdanen van derde landen in het Schengeninformatiesysteem (SIS) op voorstel van Europol

Gezien de **mondiale aard van zware criminaliteit en terrorisme** wordt informatie in handen van derde landen en internationale organisaties over daders en personen die van dergelijke strafbare feiten worden verdacht, steeds relevanter voor de interne veiligheid van de EU. De externe dimensie van de samenwerking bij de rechtshandhaving in de EU is voor de lidstaten dan ook van cruciaal belang geworden, evenals de **rol van Europol in de ondersteuning van de lidstaten bij hun partnerschappen met derde landen** of in die landen gevestigde entiteiten. Verdere inspanningen zullen **in de toekomst essentieel** zijn om de mondiale veiligheid te versterken[9].

Bij Verordening (EU) 2022/991 zijn reeds substantiële wijzigingen in de Europol-verordening ingevoerd om de **externe dimensie van de activiteiten van Europol** te versterken, met name de vergemakkelijking van de uitwisseling van informatie met derde landen[10] en de verplichting

---

7 Deze evaluatie, die is uitgevoerd in overeenstemming met artikel 68, lid 3, van de Europol-verordening, is niet de evaluatie die volgens de richtsnoeren voor betere regelgeving moet worden uitgevoerd met het oog op een mogelijk voorstel voor een herziening van de Europol-verordening. Zie ook punt 4 hieronder.

8 Handvest van de grondrechten van de Europese Unie (PB C 326 van 26.10.2012, blz. 391, ELI: http://data.europa.eu/eli/treaty/char_2012/oj).

9 Zie ProtectEU: een Europese strategie voor interne veiligheid, COM(2025) 148 final van 1 april 2025, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52025DC0148.

10 Zie bijvoorbeeld artikel 25, lid 4 bis, van de Europol-verordening, dat Europol de mogelijkheid biedt gegevens aan derde landen over te dragen nadat het zelf alle omstandigheden in verband met de overdracht van persoonsgegevens heeft beoordeeld en tot de conclusie is gekomen dat er passende waarborgen bestaan

voor Europol om in zijn meerjarenprogrammering en jaarlijkse werkprogramma's een strategie voor de betrekkingen met derde landen en internationale organisaties op te nemen[11].

In **artikel 4, lid 1, punt t), van de Europol-verordening** is een nieuwe taak aan Europol toegewezen: het ondersteunen van de lidstaten bij de verwerking van door derde landen of internationale organisaties verstrekte gegevens over personen die betrokken zijn bij terrorisme of zware criminaliteit, onder meer **het doen van voorstellen aan de lidstaten om informatiesignaleringen over onderdanen van derde landen in het belang van de Unie in het Schengeninformatiesysteem (SIS) op te nemen**. Deze nieuwe categorie informatiesignaleringen is in 2022 ingevoerd[12], na een wijziging van Verordening (EU) 2018/1862 over het gebruik van het SIS op het gebied van politiële en justitiële samenwerking in strafzaken[13].

Bepaalde informatie, met name wanneer de betrokkene geen EU-burger is en er geen verband is met een nationale zaak, wordt door het derde land alleen gedeeld met Europol, dat de gegevens verwerkt en zijn analyseresultaten met alle lidstaten deelt. Het doel van de nieuwe bepalingen was **de exploitatie van informatie** die Europol van derde landen heeft ontvangen, **te maximaliseren** door deze toegankelijker te maken dan wanneer zij enkel via het eigen systeem van Europol beschikbaar zou zijn. Dit vormde een aanvulling op andere maatregelen, zoals het Europees zoekportaal (ESP) en het interoperabiliteitskader[14] tussen de Unie-informatiesystemen voor veiligheid, grensbeheer en migratiebeheer, met als doel de structurele tekortkomingen in verband met deze systemen te verhelpen, die het werk van de nationale autoriteiten, met name grenswachters, hinderen.

Het **SIS** wordt beschouwd als een **belangrijk aanvullend verspreidingskanaal**: het is de meest gebruikte databank in Europa voor rechtshandhaving, grenstoezicht en migratie. In 2024 werden meer dan 15 miljard zoekopdrachten uitgevoerd in het SIS, tegenover ongeveer 14 miljoen zoekopdrachten in het Europol-informatiesysteem (EIS) en minder dan 3 miljard zoekopdrachten (wereldwijd) in de 19 Interpoldatabanken, de twee andere toonaangevende informatiesystemen voor bevoegde autoriteiten[15].

(2) Innovatie: artikel 18, lid 2, punt e), en artikel 33 bis van de Europol-verordening over de verwerking van persoonsgegevens door Europol voor onderzoeks- en innovatieprojecten

Technologische ontwikkelingen brengen zowel enorme kansen als aanzienlijke uitdagingen voor de interne veiligheid van de EU[16] met zich mee en hebben een zodanig grote impact op

---

voor de bescherming van persoonsgegevens, en artikel 25, lid 5, van de Europol-verordening, dat voorziet in een uitbreiding van de werkingssfeer van de uitzonderlijke gevallen waarin Europol in naar behoren gemotiveerde gevallen ad hoc (categorieën van) gegevens aan derde landen en internationale organisaties kan overdragen.

11 Artikel 12, lid 2, van de Europol-verordening.

12 Verordening (EU) 2022/1190 (PB L 185 van 12.7.2022, blz. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 Verordening (EU) 2018/1862 (PB L 312 van 7.12.2018, blz. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 Verordening (EU) 2019/818 (PB L 135 van 22.5.2019, blz. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

15 eu-LISA, jaarverslag 2024 SIS, online beschikbaar op https://www.eulisa.europa.eu/sites/default/files/documents/sis-annual-report-2024.pdf, Europol, geconsolideerd jaarlijks activiteitenverslag 2024, online beschikbaar op https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF en https://www.interpol.int/How-we-work/Databases.

16 Europol, Internet Organised Crime Threat Assessment (Iocta) 2024, online beschikbaar op Internet Organised Crime Threat Assessment (IOCTA) 2024 | Europol.

de criminaliteit gehad dat zelfs de diepe aard, het "DNA", van dreigingen op het gebied van zware en georganiseerde criminaliteit is veranderd[17]. Criminelen integreren nieuwe technologieën snel in hun activiteiten, waarbij zij nieuwe bedrijfsmodellen creëren en hun tactieken verfijnen. Tegelijkertijd bieden deze vorderingen **rechtshandhavingsautoriteiten ongekende mogelijkheden om hun capaciteiten te versterken**. Onderzoek en innovatie spelen dan ook een cruciale rol bij de interne veiligheid door het ontwikkelen van oplossingen om opkomende dreigingen tegen te gaan en gelijke tred te houden met de snel veranderende vormen en werkwijzen van criminele netwerken, waaronder die welke voortvloeien uit het misbruik van technologie. De Unie heeft in de ontwikkeling van innovatieve instrumenten geïnvesteerd, en zal daarin blijven investeren, via door de EU gefinancierd veiligheidsonderzoek en -innovatie in het kader van **ProtectEU**, de Europese strategie voor interne veiligheid[18].

Het **innovatielab van Europol**, dat eind 2019 werd opgericht in opdracht van de ministers van Justitie en Binnenlandse Zaken van de EU-lidstaten[19]**,** heeft tot doel sturing te geven aan het streven van Europol naar innovatie op het gebied van rechtshandhaving. Bij Verordening (EU) 2022/991 zijn substantiële wijzigingen in de Europol-verordening ingevoerd om het innovatiemandaat van Europol te versterken, zowel om het potentieel van het innovatielab van Europol te ondersteunen als om synergieën met andere onderzoeks- en innovatieactiviteiten op EU-niveau, met name in de Commissie, te bevorderen in het kader van de **EU-innovatiehub** voor interne veiligheid[20].

Artikel 18, lid 2, van de Europol-verordening over de doeleinden van gegevensverwerking werd gewijzigd om Europol in staat te stellen **operationele persoonsgegevens** ook **voor onderzoeks- en innovatieprojecten te verwerken**. De beschikbaarheid van hoogwaardige datasets om een empirische toetsing van de validiteit van nieuwe instrumenten mogelijk te maken, wordt algemeen beschouwd als een belangrijke voorwaarde voor de ontwikkeling van technologieën. Onbetrouwbare of bevooroordeelde datasets voor de toetsing kunnen daarentegen leiden tot gebrekkige technologieën[21].

Op maat gesneden waarborgen inzake gegevensbescherming voor een dergelijke verwerking werden vastgelegd in artikel 18, lid 3 bis, artikel 30, leden 2 en 3, en **artikel 33 bis van de Europol-verordening**. Op grond van dat laatste artikel moest een **testomgeving** worden opgezet door te bepalen dat de in het kader van een project verwerkte persoonsgegevens tijdelijk moeten worden gekopieerd naar een afzonderlijke, geïsoleerde en beschermde gegevensverwerkingsomgeving binnen Europol die uitsluitend voor dat project mag worden gebruikt.

(3) <u>Strafrechtelijke onderzoeken</u>: artikel 18, lid 6 bis, en artikel 18 bis van de Europol-verordening over de voorwaarden voor de verwerking van persoonsgegevens die zijn ontvangen zonder indeling van de betrokkenen in categorieën

In zijn rol als **EU-informatiecentrum over criminaliteit** vergemakkelijkt Europol niet alleen het verzamelen en uitwisselen van informatie, maar helpt het ook **de effectiviteit van onderzoeken te vergroten via geavanceerde gegevensanalyse** en door het opsporen van verbanden tussen strafbare feiten en criminele netwerken over de grenzen heen die op nationaal

17 Europol, EU-Socta 2025, blz. 19.

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

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

20 Zie met name artikel 4, lid 1, punten v) en w), van de Europol-verordening.

21 SWD(2020) 543 final van 9 december 2020, blz. 29.

niveau niet zichtbaar zijn. Deze capaciteiten ondersteunen de lidstaten door de voor hun strafrechtelijke onderzoeken beschikbare informatie te verrijken.

Met het uitgebreide en intensieve gebruik van technologie **zijn grote en complexe datasets het nieuwe normaal geworden in alle aspecten van het leven**, waaronder criminaliteit[22]. Bij onderzoeken naar georganiseerde misdaad of terrorisme staat men nu voor de uitdaging om grote hoeveelheden elektronisch opgeslagen gegevens, vaak ter grootte van terabytes, te analyseren, waaronder audio-, video- en machinegegenereerde gegevens die tijdens onderzoeken in beslag zijn genomen. Zo hebben onderzoekers in het gezamenlijke onderzoek over de ontmanteling van het EncroChat-netwerk[23] miljoenen berichten geanalyseerd die criminelen hebben uitgewisseld om ernstige misdrijven te plannen. Tegen deze achtergrond is de beschikbaarheid van de noodzakelijke instrumenten op het gebied van informatie- en communicatietechnologie (ICT), expertise en middelen om grote en complexe datasets (in technisch jargon bekend als "big data"[24]) te analyseren, van essentieel belang voor rechtshandhavingsautoriteiten en justitiële autoriteiten.

De in 2016 vastgestelde Europol-verordening voorzag weliswaar niet in beperkingen als zodanig ten aanzien van de analyse van big data, maar daarin ontbraken gestructureerde bepalingen met de voorwaarden voor het analyseren van dit soort gegevens. Het meest **kritieke punt** was **het vereiste van indeling van de betrokkenen in categorieën**. Indeling van de betrokkenen in categorieën (categorisering) verwijst naar de noodzaak om de datasets te screenen om persoonsgegevens te sorteren volgens verschillende categorieën, die limitatief zijn opgesomd in bijlage II.A en bijlage II.B bij de Europol-verordening, voordat wordt overgegaan tot de daadwerkelijke verwerking van de gegevens voor onderzoeksdoeleinden en ook voordat de gegevens kruislings worden gecontroleerd om verbanden op te sporen, of analyses van strategische of thematische aard of operationele analyses worden uitgevoerd[25]. De desbetreffende categorieën zijn gekoppeld aan verschillende vormen van betrokkenheid bij strafrechtelijke onderzoeken, waaronder i) verdachten, potentiële toekomstige daders, alsook ii) contactpersonen, begeleidende personen, slachtoffers, getuigen en informanten die bij criminele activiteiten betrokken zijn. In het algemeen kan Europol de persoonsgegevens van personen die niet onder een van deze categorieën vallen, niet verwerken en zelfs niet opslaan.

Gegevensverstrekkers, zoals **lidstaten** of **EU-organen en agentschappen**, maken **doorgaans** reeds een categorisering alvorens de persoonsgegevens aan Europol over te dragen[26]. Op grond van het EU-recht moeten alle gegevensverstrekkers voor hun eigen verwerking en onderzoeken een categorisering maken, ongeacht de gegevensoverdracht aan Europol, op basis van regels

---

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, Advies 7/2015, blz. 7, beschikbaar op https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf. "In algemene zin verwijst "**big data**", als een gemeenschappelijke noemer van de verschillende beschikbare definities, naar de praktijk waarin grote hoeveelheden informatie afkomstig uit verschillende bronnen worden gecombineerd en geanalyseerd, met behulp van verfijnde algoritmen, om weldoordachte besluiten te nemen. Bij big data gaat het niet alleen om het toenemende vermogen van technologie om het verzamelen en opslaan van grote hoeveelheden gegevens te ondersteunen, maar ook om het vermogen ervan om de volledige waarde van gegevens te analyseren, te begrijpen en te benutten (met name met behulp van analytische toepassingen)".

25 Zie artikel 18, lid 2, van de Europol-verordening.

26 De lidstaten dragen gegevens aan Europol over via zijn applicatie voor veilige informatie-uitwisseling (Secure Information Exchange Network Application — Siena), waarin voor de categorisering een verplicht veld is opgenomen.

die weliswaar gelijkwaardig, maar niet identiek zijn aan die van Europol[27]. Bij grote en complexe datasets vergt handmatige voorverwerking evenwel veel tijd en middelen. Het analyseren van de gegevens op één enkele mobiele telefoon kan, op semigeautomatiseerde wijze, drie dagen in beslag nemen, en tijdens een onderzoek kunnen zelfs honderden mobiele telefoons in beslag worden genomen. Categorisering **voor big data** is **niet altijd mogelijk** gezien de grote omvang van de datasets, de wijze waarop gegevens zijn gestructureerd (of niet zijn gestructureerd), het gebrek aan middelen, of de buitensporige **handmatige inspanning die vereist is**. In de praktijk is de enige mogelijkheid de gegevens eerst grondiger te analyseren vanuit een operationeel oogpunt, of verbanden op te sporen, ook op semigeautomatiseerde wijze, door de beschikbare gegevens kruislings te controleren.

In Verordening (EU) 2022/991 zijn de voorwaarden verduidelijkt waaronder categorisering **rechtszekerheid** biedt met betrekking tot de verwerking van grote en complexe datasets. Europol en de Europese Toezichthouder voor gegevensbescherming (European Data Protection Supervisor – EDPS) hanteerden een verschillende interpretatie van de letter en de geest van de Europol-verordening wat de toepasselijke bewaartermijn betreft. Volgens Europol moest die termijn drie jaar bedragen; volgens de EDPS moest dat zes maanden zijn[28]. Er waren ook nieuwe bepalingen nodig om **aanvullende flexibiliteit** te bieden, waarbij het juiste evenwicht tussen gegevensbeschermings- en veiligheidsaspecten tot stand werd gebracht.

In artikel 18, lid 5 bis, van de Europol-verordening, in combinatie met artikel 73 van de EUVG, werd eerst het algemene beginsel van de categorisering overeenkomstig artikel 18, lid 2, en bijlage II verder verduidelijkt. Europol moet, indien van toepassing en voor zover mogelijk, **persoonsgegevens duidelijk toewijzen aan een specifieke categorie van betrokkenen**. In de praktijk moet Europol, voordat persoonsgegevens kunnen worden verwerkt, in de regel de precieze rol in de criminele activiteit bepalen (bijvoorbeeld of een persoon een verdachte, een slachtoffer of enkel een getuige is) voor elke persoon wiens persoonsgegevens worden verwerkt, en niet op een geaggregeerd niveau voor alle personen in een te verwerken gegevensbestand, of een deel daarvan (bijvoorbeeld door eenvoudigweg vast te stellen dat alle genoemde personen betrokken zijn bij een criminele activiteit die onder zijn mandaat valt, op basis van een onderzoek van de algemene omstandigheden naar aanleiding waarvan het gegevensbestand is aangemaakt).

In artikel 18, lid 6 bis, van de Europol-verordening is uitdrukkelijk bepaald dat zonder categorisering ontvangen persoonsgegevens mogen worden verwerkt voor **een periode van ten hoogste 18 maanden**, die in naar behoren gemotiveerde gevallen kan worden verlengd tot 36 maanden, uitsluitend **om de betrokkenen in categorieën in te delen**. In artikel 18, lid 6 bis, van de Europol-verordening wordt niet uitdrukkelijk verwezen naar grote en complexe datasets, maar wordt meer in het algemeen een toetsing van "**strikte noodzakelijkheid**" voorgeschreven.

Artikel 18 bis van de Europol-verordening voorziet in een afwijking door Europol in staat te stellen van een **bevoegde autoriteit,** het Europees Openbaar Ministerie (**EOM**) of **Eurojust** ontvangen persoonsgegevens te verwerken, wanneer dat nodig is om een **lopend strafrechtelijk onderzoek** te ondersteunen, zonder dat een categorisering nodig is, indien deze

---

27 Zie bijvoorbeeld artikel 6 van Richtlijn (EU) 2016/680 ("de richtlijn rechtshandhaving" met betrekking tot indirect bevoegde autoriteiten) (PB L 119 van 4.5.2016, blz. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj), artikel 51 van Verordening (EU) 2017/1939 van de Raad ("de EOM-verordening") (PB L 283 van 31.10.2017, blz. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj) en artikel 27, lid 3, van Verordening (EU) 2018/1727 ("de Eurojust-verordening") (PB L 295 van 21.11.2018, blz. 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.

nog niet heeft plaatsgevonden, en buiten de in de Europol-verordening genoemde categorieën van betrokkenen. Europol kan de gegevens verwerken via een **operationele analyse** of, in uitzonderlijke gevallen en mits behoorlijk gemotiveerd, door **het uitvoeren van kruiscontroles** om connecties of andere relevante verbanden op te sporen. Deze afwijking was bedoeld om rekening te houden met de verschillen tussen de regels voor categorisering die van toepassing zijn op Europol en die welke van toepassing zijn op de bevoegde autoriteiten, het EOM en Eurojust.

(4) Samenwerking met derden: artikel 26, 26 bis en 26 ter van de Europol-verordening over de uitwisseling van persoonsgegevens tussen Europol en particuliere partijen

Criminelen maken steeds vaker misbruik van de (grensoverschrijdende) diensten van particuliere partijen – internetgebaseerde, financiële en klassieke telecomdiensten. **Particuliere partijen bewaren dan ook een grote hoeveelheid persoonsgegevens die relevant zijn voor strafrechtelijke onderzoeken**. Met name is door het internet een openbare ruimte ontstaan die feitelijk in particuliere handen is, waardoor het moeilijk is regels voor rechtshandhavingsdoeleinden online even effectief te handhaven als offline[29].

Tegen deze achtergrond is **samenwerking tussen rechtshandhavingsautoriteiten en particuliere partijen onontbeerlijk** geworden. Zoals uiteengezet in **ProtectEU**, de Europese strategie voor interne veiligheid, zal het essentieel zijn de partnerschappen met de particuliere sector te versterken om de uitwisseling van informatie te vergemakkelijken[30]. De hoofden van politie hebben, in hun gezamenlijke verklaring over de toekomst van Europol[31], Europol opgeroepen om als een "**essentiële toegangspoort voor het verkrijgen van informatie van particuliere entiteiten**" te fungeren. De aard van deze samenwerking varieert van het delen van informatie en het verstrekken van commerciële opensourcegegevens tot het deelnemen aan onderzoeks- en innovatieprojecten en het leveren van diensten die de werking van ondernemingen ondersteunen[32]. Zo heeft Europol in 2025 met succes Lumma Stealer, de grootste bedreiging ter wereld op het gebied van het stelen van informatie, verstoord via samenwerking met Microsoft, dat wereldwijd meer dan 394 000 Windows-computers had gevonden die waren geïnfecteerd met de Lumma-malware[33].

Bij Verordening (EU) 2022/991 zijn **aanvullende mogelijkheden** voor Europol ingevoerd om persoonsgegevens uit te wisselen met particuliere partijen. Voorheen kon Europol alleen persoonsgegevens van particuliere partijen ontvangen via een nationale Europoleenheid (ENU) of vooraf aangewezen contactpunten of autoriteiten van derde landen of internationale organisaties. Het doel van de verwerking door Europol was beperkt tot het identificeren van de betrokken ENU, of het contactpunt of de autoriteit van het derde land en de internationale organisatie dat/die de verantwoordelijkheid voor de zaak op zich zou kunnen nemen.

Met het **gewijzigde artikel 26 van de Europol-verordening is de taak van Europol uitgebreid,** zodat het de informatie (inclusief persoonsgegevens) van particuliere partijen

---

29 SWD(2020) 543 final van 9 december 2020, blz. 16-17.

30 Zie ProtectEU: een Europese strategie voor interne veiligheid, blz. 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 (Samenwerking met particuliere partijen), 31 mei 2023, EDOC #1306090v13. Zie ook Milieu Consulting, Study on the Practice of direct exchanges of personal data between Europol and Private Parties (Studie naar de praktijk van rechtstreekse uitwisseling van persoonsgegevens tussen Europol en particuliere partijen), eindrapport, september 2020.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Verdere voorbeelden zijn te vinden in het begeleidende werkdocument van de diensten van de Commissie.

uitgebreid kan verwerken. Een primair doel van de verwerking is nog steeds het identificeren van de betrokken nationale Europoleenheid (ENU). Europol mag de informatie nu echter ook met zijn eigen analyse aanvullen om de verdere behandeling van een zaak op nationaal niveau te vergemakkelijken.

Naast de horizontale bepalingen van artikel 26 van de Europol-verordening zijn bij artikel 26 bis van die verordening ook regels voor **onlinecrisissituaties** ingevoerd, en artikel 26 ter heeft betrekking op de **verspreiding van online materiaal van seksueel misbruik van kinderen**. In die gevallen mag Europol de lidstaten bijstaan door persoonsgegevens te verwerken die rechtstreeks van particuliere partijen zijn ontvangen. Europol mag in individuele gevallen ook persoonsgegevens doorgeven aan particuliere partijen.

Bij Verordening (EU) 2022/991 is de mogelijkheid ingevoerd om de infrastructuur van Europol te gebruiken voor de uitwisseling van informatie tussen bevoegde autoriteiten en particuliere partijen, alsook de mogelijkheid voor Europol om de lidstaten te verzoeken om, overeenkomstig hun nationale wetten, persoonsgegevens te verkrijgen van particuliere partijen.

Deze bepalingen zijn vastgesteld in samenhang met andere initiatieven, zoals de verordening inzake terroristische online-inhoud (TCO-verordening)[34] en de digitaledienstenverordening (DSA)[35]. Er zijn verdere maatregelen ter versterking van de betrokkenheid van particuliere partijen bij de bestrijding van criminaliteit en ter vergemakkelijking van de rechtmatige toegang tot gegevens voorgesteld om "de ambitie van een cultuurverandering op het gebied van veiligheid" (**maatschappijbrede benadering**) te verwezenlijken in het kader van **ProtectEU**, de Europese strategie voor interne veiligheid[36].

(5) Intern en extern toezicht op de naleving van de grondrechten door Europol

In Verordening (EU) 2022/991 ligt de nadruk op de verplichting van Europol om de grondrechten te eerbiedigen krachtens de bepalingen waarin de taken van Europol en de daarmee verband houdende versterkte waarborgen worden omschreven, met name door **het interne en externe toezicht op het agentschap te versterken**.

Op het gebied van gegevensbescherming had de aanpassing van de Europol-verordening aan de waarborgen inzake gegevensbescherming uit hoofde van de EUVG tot gevolg dat er nieuwe regels moesten worden ingevoerd voor het toezicht door de **functionaris voor gegevensbescherming** (data protection officer — DPO) en de **Europese Toezichthouder voor gegevensbescherming** (European Data Protection Supervisor — EDPS). Zo moet nu voor elke nieuwe soort verwerking systematisch een gegevensbeschermingseffectbeoordeling worden uitgevoerd en moet vooraf de EDPS worden geraadpleegd. Bij Verordening (EU) 2022/991 is ook een nieuwe bevoegdheid van Europol voor verzoeken om toegangsrechten ingevoerd. Voorheen waren de nationale bevoegde autoriteiten voor de behandeling van verzoeken om toegangsrechten verantwoordelijk indien de lidstaten de gegevensverstrekkers waren.

Bij Verordening (EU) 2022/991 is ook de **nieuwe functie van grondrechtenfunctionaris** (fundamental rights officer — FRO) bij Europol ingesteld. De grondrechtenfunctionaris heeft

---

[34] Verordening (EU) 2021/784 (PB L 172 van 17.5.2021, blz. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj).

[35] Verordening (EU) 2022/2065 (PB L 277 van 27.10.2022, blz. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

[36] Zie ProtectEU: een Europese strategie voor interne veiligheid, blz. 2.

onder meer tot taak de uitvoerend directeur van Europol te informeren over mogelijke schendingen van grondrechten tijdens de uitvoering van de activiteiten van het agentschap.

Daarnaast zijn **het democratische toezicht en de verantwoordingsplicht versterkt** via de politieke controle op de activiteiten van Europol door het **Europees Parlement en de nationale parlementen**, zoals voorzien in artikel 88, lid 2, tweede alinea, van het Verdrag betreffende de werking van de Europese Unie (VWEU). Verordening (EU) 2022/991 heeft het toezicht door de **Gezamenlijke Parlementaire Controlegroep** (GPC) versterkt[37]. Zo voorziet deze verordening in een verplichte raadpleging van de GPC over het ontwerp van de meerjarenprogrammering en het jaarlijkse werkprogramma van Europol, de mogelijkheid voor de GPC om niet-bindende specifieke aanbevelingen aan Europol te doen en deze bij het Europees Parlement en de nationale parlementen in te dienen, en de oprichting van een adviesforum dat de GPC desgevraagd bijstaat met onafhankelijk advies op het gebied van grondrechten.

3. Belangrijkste bevindingen van de evaluatie

3.1. Stand van zaken bij de operationele uitvoering van de nieuwe taken en bevoegdheden van Europol op het gebied van de verwerking van persoonsgegevens

Verordening (EU) 2022/991 is **op 28 juni 2022 in werking getreden**. De operationele toepassing ervan was echter afhankelijk van verschillende technische, administratieve en governancemaatregelen, alsook van operationele vereisten zoals het opzetten van nieuwe ICT-structuren in sommige gevallen.

Drie jaar later **zijn bijna alle** in artikel 68, lid 3, van Verordening (EU) 2022/991 genoemde **bepalingen operationeel geworden**. De bepalingen met betrekking tot de analyse van grote en complexe datasets (artikel 18, lid 6 bis, en artikel 18 bis van de Europol-verordening) en samenwerking met particuliere partijen (artikelen 26, 26 bis en 26 ter van de Europol-verordening) zijn van toepassing geworden op 28 juni 2022, of kort daarna. De verwerking van persoonsgegevens voor onderzoeks- en innovatieprojecten (artikel 18, lid 2, punt e), van de Europol-verordening) is in 2023 begonnen nadat de testomgeving, genaamd ODIN, was opgezet om te voldoen aan de specifieke gegevensbeschermingsvoorschriften van artikel 33 bis van de Europol-verordening. Op 29 juni 2025 was de mogelijkheid voor Europol om **SIS-informatiesignaleringen** aan de lidstaten voor te stellen overeenkomstig artikel 4, lid 1, punt t), van de Europol-verordening nog niet operationeel geworden, aangezien de technische uitvoering van het nieuwe type signalering nog aan de gang is. De inwerkingtreding wordt **verwacht in 2026**.

3.2. Evaluatie van de operationele impact van de nieuwe taken en bevoegdheden van Europol op het gebied van de verwerking van persoonsgegevens op de doelstellingen van het agentschap als bedoeld in artikel 3 van de Europol-verordening

Wat de operationele impact van de nieuwe taken en bevoegdheden van Europol op het gebied van de verwerking van persoonsgegevens betreft, is uit de raadpleging gebleken dat **de lidstaten over het algemeen positief staan** tegenover de relevantie, effectiviteit en meerwaarde ervan en tegenover de ondersteuning door Europol van hun bevoegde autoriteiten op de betrokken gebieden[38].

---

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

38 Zie de bijdragen in punt 5 van het bij dit verslag gevoegde werkdocument van de diensten van de Commissie, en met name de opmerkingen van Europol en de antwoorden van de lidstaten op de vragen 2, 4 en 5 van de korte vragenlijst van 2 juni 2025, in bijlage III bij het werkdocument van de diensten van de Commissie.

De onderzoeksbevoegdheden waarop deze evaluatie betrekking heeft, worden niet voortdurend of systematisch gebruikt om gegevens te verwerken voor controledoeleinden; sommige bevoegdheden zijn zelfs uitzonderlijk van aard, terwijl andere vaker bij onderzoeken worden gebruikt op basis van behoeften. De **operationele toepassing van de nieuwe bepalingen** in de referentieperiode **verschilde aanzienlijk** in **kwantitatief opzicht,** afhankelijk van de verschillende technische kenmerken en wettelijke voorwaarden in verband met de nieuwe bepalingen.

Europol heeft een **niet-verwaarloosbaar** aantal **nieuwe bijdragen zonder categorisering** van de lidstaten ontvangen op grond van artikel 18, lid 6 bis, van de Europol-verordening, namelijk 653 in 2023 en 597 in 2024. Er was geen toename op korte termijn van de bijdragen zonder categorisering, en het aantal gevallen waarin artikel 18, lid 6 bis, werd toegepast, bleef **stabiel** vergeleken met gelijkwaardige gevallen in de periode vóór 28 juni 2022. De nieuwe bepalingen hadden evenmin een negatieve impact op de betrokkenheid van de lidstaten bij de uitvoering van de categorisering[39]. Tussen 2023 en 2024 bedroeg het aandeel van de bijdragen zonder categorisering **minder dan 1 % van alle** door Europol van de lidstaten aanvaarde **bijdragen** (0,85 % in 2023 en 0,71 % in 2024). Sinds juni 2022 heeft Europol de categorisering steeds binnen 18 maanden afgerond, zonder gebruik te maken van de verlengde termijn van 36 maanden. Europol en zes lidstaten benadrukten dat, ondanks de verbeterde rechtszekerheid, de **administratieve lasten aanzienlijk bleven** voor zowel Europol als de bevoegde autoriteiten, vanwege de inspanningen die nodig waren om te voldoen aan de categorisering van persoonsgegevens naar betrokkenheid van de individuele personen bij het strafbare feit. Dit vereiste wordt door Europol zeer strikt toegepast[40].

Europol meldde dat de uitwisseling van informatie met **particuliere partijen** in 2023 nog steeds verwaarloosbaar was, aangezien slechts 26 gevallen van toepassing van artikel 26 van de Europol-verordening werden geregistreerd (naast de gevallen die onder de digitaledienstenverordening vallen)[41]. In **2024** lieten de statistieken echter een **sterke stijging tot 284** (bijna +1 000 %) gevallen zien waarin met particuliere partijen werd samengewerkt op grond van artikel 26 van de Europol-verordening. Dit was met name het geval voor gegevens van particuliere ondernemingen voor het onderzoek naar **financiële en economische criminaliteit**. Europol heeft ook in aanzienlijke mate gebruikgemaakt van artikel 26 ter van de Europol-verordening bij de bestrijding van seksuele uitbuiting van kinderen, waarbij de samenwerking met particuliere partijen voorheen reeds zeer substantieel was. In beide gevallen omvatten de gegevens ook samenwerking die mogelijk was uit hoofde van het vorige rechtskader. Uit de beschikbare gegevens blijkt niet in welke mate deze nieuwe gevallen onder de nieuwe bepalingen vallen, noch dat er meer gebruik is gemaakt van de bestaande mogelijkheden.

In **2025** heeft Europol een **nieuwe strategie** vastgesteld om de samenwerking met particuliere partijen verder te versterken. Daarnaast zijn er maatregelen genomen om de ICT-infrastructuur van Europol die de bevoegde autoriteiten ter beschikking staat voor de uitwisseling van informatie met particuliere partijen, te verbeteren. In **2023** heeft Europol het Plateforme Européenne de Retraits de Contenus Illégaux sur Internet (**PERCI**) gelanceerd om de uitvoering van de TCO-verordening en, in de toekomst, mogelijk ook artikel 18 van de DSA,

---

39 Zoals door een lidstaat tijdens de raadpleging werd benadrukt, "zijn [de lidstaten] goed in staat te bepalen met welk soort gegevens [zij] te maken hebben, wat in het onderzoek zelf zeer belangrijk kan zijn".

40 Zie punt 7.1.3 van het bij dit verslag gevoegde werkdocument van de diensten van de Commissie en de antwoorden van de lidstaten op vraag 9 van de korte vragenlijst van 2 juni 2025, in bijlage III bij het werkdocument van de diensten van de Commissie.

41 Europol, verslag 2023 overeenkomstig artikel 16, lid 11, van de Europol-verordening.

alsook de EU Child Abuse Referral Service **(EU CARES)** te vergemakkelijken. PERCI maakt geen deel uit van het Europol-informatiesysteem (EIS)[42].

Andere bepalingen zijn in het geheel **niet toegepast** (artikel 26 bis van de Europol-verordening), hoewel ze wel operationeel waren, **of** zijn **slechts bij uitzondering** toegepast (één geval waarin artikel 18 bis van de Europol-verordening werd toegepast in 2024 en één project dat met de verwerking van persoonsgegevens krachtens artikel 18, lid 1, punt t), van de Europol-verordening werd verwezenlijkt in 2025, met drie nieuwe projecten reeds in de pijplijn).

Gezien de beperkte periode van operationele uitvoering van de bij Verordening (EU) 2022/991 ingevoerde bepalingen en de lange duur van strafrechtelijke onderzoeken en gerechtelijke procedures, konden de lidstaten geen kwantitatieve gegevens verstrekken over het effect van die bepalingen in operationeel opzicht. Zij hebben wel enkele voorbeelden van succesvolle onderzoeken gegeven die de **tastbare voordelen van de nieuwe onderzoeksmogelijkheden in reële situaties** aantonen voor de bepalingen die reeds worden toegepast, zoals EncroChat, Sky ECC, criminele netwerken afkomstig uit de Balkan die betrokken zijn bij cocaïnesmokkel, of Lumma Stealer.

Europol en acht lidstaten hebben ook een aantal **verbeterpunten** aangegeven om het efficiënte en coherente gebruik van het nieuwe rechtskader te maximaliseren en de rol van Europol in de toekomst te versterken. Er heerst bezorgdheid, met name bij Europol, dat de buitensporige complexiteit, versnippering en duur van de wettelijke bepalingen professionals of particuliere partijen kunnen ontmoedigen om de nieuwe beschikbare instrumenten te gebruiken. De opmerkingen van de lidstaten hebben veeleer betrekking op de manier waarop Europol waarborgen inzake gegevensbescherming restrictief toepast onder toezicht van de EDPS, waardoor de effectiviteit en de toegevoegde waarde van sommige bepalingen dreigen te worden ondermijnd.

3.3. Beoordeling van de impact van de nieuwe taken en bevoegdheden van Europol op het gebied van de verwerking van persoonsgegevens op de grondrechten

Op basis van het beperkte gebruik dat tot dusver van de nieuwe bevoegdheden op het gebied van de verwerking van persoonsgegevens is gemaakt, heeft de Commissie **geen** bewijs gevonden voor een **negatieve impact op de grondrechten** als gevolg van het operationele gebruik van deze nieuwe bevoegdheden.

Naast de uitvoering van de specifieke gegevensbeschermingsvoorschriften in verband met de nieuwe bevoegdheden op het gebied van de verwerking van persoonsgegevens heeft Europol geleidelijk alle nodige maatregelen genomen om de nieuwe horizontale toezichtmechanismen met betrekking tot de grondrechten toe te passen.

In 2024 heeft de raad van bestuur van Europol de herziene uitvoeringsregels met betrekking tot de DPO vastgesteld als een van de laatste uitvoeringshandelingen die nodig zijn in verband met de nieuwe regeling voor gegevensbescherming. Uit het verzamelde bewijsmateriaal blijkt dat Europol en zijn raad van bestuur, in samenwerking met de DPO van Europol en de EDPS, hebben gezorgd voor een **strikte toepassing van de** in 2022 ingevoerde **nieuwe waarborgen inzake gegevensbescherming**. Deze aanpak heeft op het eerste gezicht een eventuele negatieve impact van het eerste gebruik van de nieuwe bevoegdheden op het gebied van de verwerking van persoonsgegevens op, of een interferentie daarvan met, het recht van personen op privacy en bescherming van hun persoonsgegevens voorkomen. Volgens de lidstaten

[42] Verordening (EU) 2019/818 (PB L 135 van 22.5.2019, blz. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj).

beschikt Europol momenteel over een **robuust rechtskader voor gegevensbescherming**, dat voldoende waarborgen biedt voor het potentiële grotere gebruik van zijn nieuwe bevoegdheden. Zeven lidstaten benadrukten tevens dat dit kader **de informatiestroom vergemakkelijkt** door het vertrouwen te vergroten, hoewel er nog ruimte is voor verbetering. Slechts één lidstaat heeft zich negatief uitgelaten[43].

Naast de specifieke **uitdagingen** in verband met de categorisering noemden Europol en vier lidstaten als verbeterpunten de tijd en kosten die gemoeid zijn met de **gegevensbeschermingseffectbeoordeling** en de **voorafgaande raadpleging van** de EDPS, die in de praktijk standaard worden uitgevoerd. Een andere uitdaging die door zes lidstaten aan de orde werd gesteld, is de behandeling door Europol van **verzoeken van betrokkenen om toegang tot hun gegevens**, waarvoor het nu ook bevoegd is indien een lidstaat de eigenaar van de gegevens is.

De **eerste grondrechtenfunctionaris** werd in december **2022** benoemd. In de eerste twee jaar van zijn mandaat heeft hij **geen klachten** ontvangen van, noch ingediend bij de uitvoerend directeur. Sinds het van kracht worden van de nieuwe bepalingen is de GPC de activiteiten van Europol nauwlettend blijven volgen en heeft zij geen aanbevelingen gedaan. Het Europees Parlement heeft in februari **2024** het **adviesforum van de GPC voor de grondrechten** opgericht.

3.4. Kosten-batenanalyse van de nieuwe taken en bevoegdheden van Europol op het gebied van de verwerking van persoonsgegevens

Gezien het vroege stadium van uitvoering van de bij Verordening (EU) 2022/991 ingevoerde bepalingen en de beperkte ervaring daarmee, is het voor de Commissie nog **te vroeg** om uit een **kosten-batenanalyse** zinvolle conclusies over de nieuwe bepalingen te trekken.

De diensten van de Commissie hebben informatie van Europol verzameld over de kosten die in verband met de operationele uitvoering van Verordening (EU) 2022/991 tot op heden zijn gemaakt voor de onderzochte bepalingen. Deze kosten bedroegen tussen 2022 en 2025 ongeveer **25 miljoen EUR** (circa 5 % van de totale toewijzing aan Europol[44]) en bestonden voornamelijk uit eenmalige kosten. De lidstaten hebben tot op heden geen relevante nieuwe kosten gemaakt die specifiek verband houden met Verordening (EU) 2022/991.

Het grootste deel van de kosten (bijna 17 miljoen EUR) bestond uit significante investeringen in de **ontwikkeling van nieuwe ICT-structuren,** ter uitvoering van de bepalingen over onderzoek en innovatie (de testomgeving ODIN), en voor informatiesystemen voor de uitwisseling van persoonsgegevens met particuliere partijen (PERCI en EU CARES). De kosten voor **personele middelen** (human resources – HR), zowel met betrekking tot ICT als uitgevoerde werkzaamheden, maakten ongeveer een derde van de totale uitgaven uit (ongeveer 8 miljoen EUR). HR zal **op lange termijn de belangrijkste terugkerende kostenpost** vormen.

Er zij op gewezen dat in het bovengenoemde bedrag van 8 miljoen EUR de HR-kosten voor de eenheid Informatiebeheer (IMU) en de middelen in verband met (vorige en nieuwe) toezichtmaatregelen met een horizontaal karakter, waarvoor een uitsplitsing op het niveau van de uitvoering van specifieke bepalingen niet mogelijk is, niet zijn opgenomen. De kosten voor deze middelen zijn niet verwaarloosbaar. Zo waren in 2023 naar schatting

---

[43] Zie antwoorden van de lidstaten op vraag 9 van de korte vragenlijst van 2 juni 2025, in bijlage III bij het begeleidende werkdocument van de diensten van de Commissie.

[44] In dezelfde periode bedroeg het aan Europol toegewezen budget in totaal ongeveer **860 miljoen EUR** (geleidelijk verhoogd van 192 miljoen EUR in 2022 tot 241 miljoen EUR in 2025). Zie voor meer details het begeleidende werkdocument van de diensten van de Commissie.

60 voltijdequivalenten (vte's) (bijna **5 %** van het personeel van Europol) betrokken bij activiteiten in **waarborg-/toezichtorganen en controle-/adviesinstanties**. Europol heeft 25 vte's toegewezen aan inspanningen in reactie op maatregelen in verband met het toezicht op gegevensbescherming en de bijbehorende waarborgingsmaatregelen. Dit omvat follow-up van de aanbevelingen van de EDPS, alsook werkzaamheden in het kader van voorafgaande raadplegingen voor operationele gegevensverwerking. Van deze 25 vte's zijn er 16 specifiek betrokken bij activiteiten in verband met de voorschriften van de EDPS. Vanaf juni 2025 beschikt Europol over een speciaal team van acht voltijdse personeelsleden op het gebied van gegevensbescherming, waaronder de DPO.

Volgens Europol en vijftien lidstaten zullen de **voordelen** van de nieuwe taken en bevoegdheden op het gebied van de verwerking van persoonsgegevens, met name het analyseren van grote en complexe datasets, alsook het samenwerken met particuliere partijen, naar verwachting aanzienlijk zijn, en **groter dan de daarmee verband houdende kosten**. Geen van de lidstaten nam een ander standpunt in. Sommige efficiëntievoordelen worden redelijkerwijs op lange termijn verwacht, dankzij schaalvoordelen en afnemende marginale kosten. Een lidstaat benadrukte dat "het belangrijk is dat Europol de noodzakelijke ICT-middelen verschaft om de instrumenten voor de toepassing van de nieuwe mogelijkheden van Verordening (EU) 2022/991 te verstrekken en verder te ontwikkelen", hetgeen ook werd ondersteund door twee andere lidstaten en andere belanghebbenden[45].

Naar de mening van Europol en vijf lidstaten moeten mogelijke **inefficiënties** bij de toepassing ook binnen het **bestaande governance-, administratie- en gegevensbeschermingskader** worden aangepakt om ondermijning van de operationele impact van de nieuwe taken op het gebied van de verwerking van persoonsgegevens door opschorting of beperking van het gebruik ervan te voorkomen. Vijf lidstaten vroegen zich af of bij de uitvoering van de gegevensbeschermingsvoorschriften door Europol en zijn raad van bestuur, onder leiding van de EDPS, niet te voorzichtig te werk wordt gegaan. Zij wijzen erop dat de door de medewetgevers geboden flexibiliteit op passende wijze moet worden benut om de effectiviteit en efficiëntie van de taken van Europol te maximaliseren en de relevantie en het rendement op lange termijn ervan te waarborgen.

Een evaluatie van de werkmethoden van Europol en mogelijke gebieden voor vereenvoudiging valt buiten de reikwijdte van het verslag als bedoeld in artikel 68, lid 3, van de Europol-verordening en zal worden uitgevoerd binnen het kader van de evaluatie als bedoeld in artikel 68, lid 1, van de Europol-verordening.

4. Conclusies en vooruitzichten

Al met al zijn de voorlopige belangrijkste bevindingen van de Commissie dat de lidstaten **hun steun voor de rol van Europol** handhaven op de belangrijkste gebieden waarop het momenteel de lidstaten bijstaat met zijn **nieuwe taken op het gebied van de verwerking van persoonsgegevens**. Om **de voordelen** van de nieuwe bevoegdheden op het gebied van de verwerking van persoonsgegevens te **maximaliseren**, moeten naar de mening van sommige belanghebbenden echter **mogelijke inefficiënties** worden **aangepakt**, met name binnen het bestaande governance-, administratie- en gegevensbeschermingskader. Het zou ook nuttig zijn

[45] Zie de bijdragen in punt 5 van het bij dit verslag gevoegde werkdocument van de diensten van de Commissie, en met name de opmerkingen van Europol en de antwoorden van de lidstaten op de vragen 2, 4 en 5 van de korte vragenlijst van 2 juni 2025, in bijlage III bij het werkdocument van de diensten van de Commissie, en de gezamenlijke verklaring van de Europese hoofden van politie over de toekomst van Europol.

om de **complexiteit en versnippering** van het rechtskader, waardoor professionals kunnen worden ontmoedigd om gebruik te maken van de nieuwe mogelijkheden, te verminderen.

In het algemeen heeft de Commissie geen bewijs gevonden dat de nieuwe regels een **negatieve impact op de grondrechten** hadden, met name dankzij robuuste waarborgen inzake gegevensbescherming, die ook de informatiestroom vergemakkelijken door het vertrouwen van de partners te vergroten. Voor sommige lidstaten heeft het agentschap gekozen voor een conservatieve aanpak, terwijl **passend gebruik moet worden gemaakt van de door de medewetgevers geboden flexibiliteit** wat betreft de indeling van de betrokkenen in categorieën, de gegevensbeschermingseffectbeoordeling, de voorafgaande raadpleging van de toezichthouder voor gegevensbescherming van Europol, en de behandeling van verzoeken om toegangsrechten.

Gezien de in het algemeen korte periode voor de uitvoering van de nieuwe regels voor de bescherming van persoonsgegevens waarin Verordening (EU) 2022/991 voorziet, is het verzamelde bewijsmateriaal echter niet op alle punten overtuigend.

In haar Europese strategie voor interne veiligheid[46], **ProtectEU**, heeft de Commissie aangekondigd dat zij een ambitieuze herziening van het mandaat van Europol zal voorstellen om de steeds grotere veiligheidsuitdagingen aan te pakken. In overeenstemming met haar richtsnoeren voor betere regelgeving[47] is de Commissie begonnen met de voorbereidingen voor de evaluatie van de Europol-verordening en de werkmethoden van Europol, waarmee de weg wordt vrijgemaakt voor een **voorstel van de Commissie in 2026 om het agentschap operationeler te maken, zoals uiteengezet in de politieke beleidslijnen**[48]. In juli 2025 heeft de Commissie het verzoek om input gepubliceerd[49] en een externe studie laten uitvoeren om de evaluatie van de Europol-verordening en de effectbeoordeling voor het nieuwe voorstel te ondersteunen. De evaluatie van de Europol-verordening met het oog op het opstellen van dit verslag is bedoeld om aan die evaluatie bij te dragen.

---

46 ProtectEU: een Europese strategie voor interne veiligheid, blz. 10.

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

48 Ursula von der Leyen, Political Guidelines for the next European Commission 2024-2029 (Politieke beleidslijnen voor de volgende Europese Commissie 2024-2029) e6cd4328-673c-4e7a-8683-f63ffb2cf648_en.

49 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Samenwerking-op-het-gebied-van-rechtshandhaving-nieuwe-Europol-verordening-voorstel-_nl.