fairtrials.org

Fair Trials

Position Paper on the Proposed New Europol Regulation (COM(2026) 580 final)

November 2026

Fair Trials is a Brussels-based NGO that campaigns for fair and equal criminal justice systems. Our team of experts exposes threats to justice through original research and identifies practical changes to fix them. We campaign to change laws, support strategic litigation, reform policy and develop international standards and best practice. We do this by supporting local movements for reform and building partnerships with lawyers, activists, academics, experts by experience and other NGOs. We are the only NGO that campaigns exclusively on the right to a fair trial, giving us a comparative perspective on how to tackle failings within criminal justice systems.

Contact

Chryssa Mela
Director
chryssa.mela@fairtrials.net

Stephanie Classmann
Legal Consultant
stephanie.classmann@fairtrials.net

Acknowledgments
This paper was authored by Stephanie Classmann, Legal Consultant at Fair Trials.

Fair Trials would like to thank the following members of the Legal Experts Advisory Panel (LEAP) for sharing their expertise and insights, which form the basis of this paper: Valsamis Mitsilegas, Oliver Wallasch, Nicola Canestrini, Achille Campagna, Alexis Anagostakis, Athanasia Dionyssopoulou, Chara Chioni-Chotouman, Christina Koenig, Dominique Arvanitis, Dominique Tricaud, Gwennhaëlle Barral, Ioannis Pagonas, Javier Blay, Marine Braun, Ondrej Muka and Vitor Neves. We also thank Wannes Bellaert for his input.

Introduction

As part of this year's Criminal Justice Package, the Commission has published a proposal to repeal the current Europol Regulation (EU) 2016/794 and replace it with an enhanced and more structured mandate organised around three core functions: **Europol as "information hub", Europol as "operational hub", and Europol as "technology and innovation hub."** Our position paper makes an effort to unpack these functions, drawing attention to relevant provisions, the ways in which they can be expected to interact, and the concerns they create or amplify.

For reasons that will quickly become apparent, the analysis places particular emphasis on the envisioned new, centralised information infrastructure. Systematic data sharing, cross-checking and querying at scale; the involvement of private parties and third countries; and a lowering of data processing and retention standards, including with respect to data subject categories under Annex II, biometric data, data of persons under the age of 18, and information obtained through human rights violations, should prompt heightened scrutiny—and, on our recommendation, a series of decisive amendments. The provisions on operational support activities underscore this assessment. Equipped with criminal intelligence from across 27 Member States, Europol shall gain new powers to actively steer, and participate in, national investigations, including through deployments and dedicated support offices embedded within national units. A broad mandate for the agency to engage in the development, testing, validation, and integration of advanced capabilities, including AI-enabled applications and decryption tools, completes the picture.

Together, these changes mark **a significant departure from the current framework of law enforcement cooperation**. While this could come with equally significant efficiency gains, Fair Trials is taken aback by the **complete absence of procedural safeguards designed to protect the rights of suspects and accused persons**. Our analysis makes this absence visible; our recommendations provide the co-legislators with concrete advice on how to fill it.

A key objective should be that when Europol outputs and other activities materially influence national investigations and proceedings, they should do so in a way that is amenable to scrutiny by both courts and the defence. The safety of criminal convictions and, crucially, the effective exercise of national remedies will depend on **transparency and accountability**. Europol's lack of either of these qualities is not a new observation—it has been a structural feature for as long as the agency has been active. However, not without irony and certainly not without concern, it is the only feature that the Commission has chosen to leave untouched.

1. Europol as "information hub"

a. Systematic data sharing, cross-checking and querying at scale

The proposal seeks to transform Europol into a centralised intelligence agency. To this end, the Member States "shall provide Europol in a timely manner with the information necessary for it to carry out its tasks" under Art. 6(1) and, "where appropriate, enable the structured, automated and interoperable provision of [that] information" (Art. 29(1) and (2)). This is not a gentle request. The proposal envisions a **mandatory, real-time syncing of national case-management systems** with the Europol information infrastructure. Specifically, Member States shall equip their national units and competent authorities with "data loaders" designed to "systematically and without undue delay" upload any data that relates to crimes falling within Europol's competence, that is relevant for cross-border cooperation, or that contains **"factual indications of a possible link to other Member States or third countries" to a new Europol cross-checking service (Art. 38(1) and (3))**. According to Art. 38(2) and Art. 29(5), data may be withheld only where sharing it would be contrary to the essential security interests of the Member State concerned, jeopardise the success of an ongoing investigation or the safety of an individual, and/or disclose information relating to organisations or specific intelligence activities in the field of national security.

Every new upload to the cross-checking service shall be **automatically matched against the entire data holding (Art. 38(6))** "to identify links between persons, objects, criminal activities, and investigations conducted in one or more Member States or with third countries." A match triggers an alert and a notification of relevant authorities and the data provider, where access has been restricted (Art. 38(7), 34). Member States shall also be required to **"systematically query" the service, including by means of biometric data**, when conducting investigations of crimes falling within Europol's competence and **"where there are reasonable grounds to consider that the case has a cross-border or international dimension" (Art. 39(2) and (3))**. Europol, in turn, shall query the service to carry out its tasks (Art. 39(5)). Subject to prior authorisation (case-by-case or standing) by the data-owning Member State, it shall also be allowed to use the data provided to **query national databases through the existing Prüm II router** (**Art. 136(1) and (2),** which would amend Art. 49(5) and (5a) of Regulation (EU) 2024/982 accordingly).

A separate **Europol Analytical Environment** shall enable storage, processing, and analysis of data to support Europol's analytical activity and cooperation with Member States and partners, including the work on Joint Operational Analysis Cases (JOAC) in a new Police Shared Data Space (Art. 40, 42, 43-45). The data holding in this environment would be richer and more diverse than that of the cross-checking service. It would include **data received from Member States, third countries, international organisations, private parties, and "other sources in accordance with this Regulation" (Recital 50)—meaning, it would extend to information that Europol has retrieved from publicly available sources, such as the internet, under Art. 28(2).** Unlike for data stored in the cross-checking service (Art. 39(1)), Member States shall have no direct access to this environment, but they shall be able to **query it on a hit/no-hit basis, including by means of**

biometric data; **a hit would initiate a procedure for sharing the data subject to any provider restrictions (Art. 41(1) and (3))**. Europol shall query the service to carry out its tasks (Art. 41(2)).

Fair Trials recognises that the effective prevention and combatting of serious, organised and cross-border crime requires the swift and coordinated exchange of information between Europol and Member States. The scale and systematic character of the data sharing, cross-checking and querying envisioned by the proposal, however, gives rise to significant concerns. In its current form, the Regulation **risks normalising mass and largely invisible circulation of personal data**, transforming what should be targeted support and suspicion-led cooperation into a generalised infrastructure of surveillance, with profound consequences not just for data protection but for the **presumption of innocence** and the **rights of the defence**, which the proposal does not address.

The first and most fundamental concern is not new. Our network of criminal practitioners has long emphasised that when Europol-derived intelligence reaches national case files as evidence, it does so as a highly curated analytical product instead of the raw data, and without any of the information necessary—for either courts or the defence—to verify its provenance, accuracy, completeness or, crucially, chain of custody. While courts have shown a troubling tendency to assume that evidence obtained or channelled through Europol is reliable and reliably lawful, the defence is left to prove the opposite. The issue has reached the European Court of Justice in the context of encrypted communications. In its 2024 landmark ruling on the infiltration of **EncroChat** devices by French and Dutch authorities, and the subsequent transfer of data through Europol, the Court held that **the fairness of the proceedings requires that national courts disregard any evidence likely to have a preponderant influence on the findings of fact on which the defence has been unable to effectively comment (Case C-670/22, paras. 104-5, 130-31)**.[1] Yet, without meaningful access to the underlying data and the process by which it was generated, this ability and the national remedies designed to enforce it will remain largely theoretical.

The Commission's proposal makes no effort to alleviate these difficulties and instead chooses to institutionalise the problem: data from various sources and across various platforms is shared, cross-checked and queried on an ongoing basis without any accompanying requirements of **documentation** and **disclosure**. It does allocate certain responsibilities, but only for the original transmissions. According to Art. 29(4), Europol national units and competent authorities of the Member States shall ensure compliance with national law (see also Art. 107(4)) and, "to the extent possible", the completeness, accuracy and timeliness of information provided to Europol (see also Art. 107(2)); all providers, including third countries and private parties, shall assess and code information with respect to its reliability and accuracy (Art. 99(1), (2) and (5)); and data from a private party shall be received by Europol only where that party "declares it is legally allowed to transmit [the information] in accordance with the applicable law" (Art. 96(2)).

[1] There has been a series of cases before national and European courts in this area. Fair Trials has intervened before the European Court of Human Rights in *Silgir v. Germany* (App. no. 22234/25) (EncroChat) and *Raal and Reudolph v. Estonia* (App. nos. 14711/25, 14712/25) (ANOM) (joint filing with the European Criminal Bar Association).

Member States' diligence during the collection and upload of data does not guard against the **risks of continuous aggregation and cross-checking** by Europol; it does not mean that national courts and the defence will be able to **reconstruct a particular hit or evaluate the strength of a particular analytical product**; and a private party's **declaration of legality** has no evidentiary value whatsoever. The Commission seeks to drastically expand Europol's powers to collect, pool, and distribute information with so much as a "possible" cross-border or international link, so it must provide genuine safeguards that empower the defence to verify and challenge the upshot of those activities once it is presented to them as evidence in national proceedings. We urge the co-legislators to consider the following recommendations.

- Europol should be required to create **a complete and auditable record** for every data item received, including source and ownership; legal basis; data category; status; access and use restrictions; reliability and accuracy codes; date and time of upload and every subsequent processing event; a log of all cross-checks and queries (databases searched, matching parameters, thresholds, tools and model versions used, known error rates, etc.); an access log (who, when, for what purpose, etc.); and a log of reviews and decisions (on verification, status changes, deletion/retention, etc.). Where the data materially influences criminal proceedings, this record and the data should become **part of the case file**.
- Data received from **private parties and third countries** should not be exempt from this requirement, nor should data that Europol retrieves from **publicly available sources**.
- A **positive cross-check or hit** should never, on its own, justify a coercive measure—it is a link between data items requiring **verification before any operational use**.
- **Data items and corresponding analytical conclusions** (e.g., verified match, investigative lead, operational product, evidentiary output) **should remain distinguishable throughout the information chain**. In particular, the Regulation should specify that a match cannot through subsequent matching alone turn into a confirmed suspicion.

The last recommendation ties in closely with our second concern. According to **Art. 37(1)(b)**, the new Europol cross-checking service shall contain data on **"persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned [that is, the Member State who provides the data] to believe that they will commit criminal offences in respect of which Europol is competent."** While the inclusion of "prospective offenders" as a relevant data category for cross-checking purposes is **not new** (see Art. 18(2)(ii) of Regulation (EU) 2016/794, as currently in force), the information infrastructure in which it shall be uploaded, stored and processed operates at a **completely new scale**: every data item in this category would be automatically matched against the entire holding of the service (Art. 38(6)); it would be "systematically queried", including by means of biometric data (Art. 39(2) and (3)); it could be used for Prüm II searches (Art. 136(1) and (2)); and it could be further processed in the Europol Analytical Environment (Art. 40-41) and the Police Shared Data Space (Art. 42-45).

Even if Member States converged on an understanding of what constitutes "factual indications or reasonable grounds" that a person "will commit criminal offences", this would be an alarming expansion of investigative reach requiring strict safeguards to ensure the **effective protection of the presumption of innocence (Art. 48(1) of the Charter, Art. 6(2) of the ECHR)**—but there is no such understanding. A person who is a "prospective offender" in one Member State may well be no more than a "person of interest" (or less) in another. Yet, in its current form, the Regulation permits these assessments to travel across the Union as if they were one and the same; and if a cross-check or query produces a hit, the authorities who receive the notification have no means of confirming the factual and legal bases on which these assessments were made. Fair Trials, therefore, urges the co-legislators to consider the following recommendations.

- Data on "prospective offenders" should be **excluded from automated cross-checking**; it should be cross-checked on a targeted, case-by-case basis, for specific investigations and only following an individualised assessment of necessity and proportionality.
- In both cases, that is, including where Art. 37(1)(b) is retained, Member States should be required to provide the **meta-data on "prospective offender" assessments** (factual and legal basis, date of assessment, review/expiry date, etc.). This data should be part of the record recommended above, and it should be subject to periodic confirmation.

A third set of concerns in this area involves the **sharing of data by Europol** and specifically with private parties, third countries, and the European Public Prosecutor's Office (EPPO).

With respect to **private parties**, Art. 47(1) establishes an "information exchange mechanism" as part of the Analytical Environment. It is meant to facilitate cooperation among private parties, the Member States and Europol, and act as **"a crisis response platform in online crisis situations**" by facilitating communication, including with third countries, and by enabling Europol to **provide private parties "with the information necessary to identify relevant online content, services, accounts, infrastructures or digital activities" (Art. 47(2)(b))**. Similar provisions are included in **Art. 15(b)** and **Art. 18(a)** which state that Europol shall **refer online content to online service providers** to help address "online crisis situations" as well as the dissemination of terrorist and violent extremist content. The legal character of these referrals appears to be advisory only.

All exchanges of personal data with private parties are subject to the restrictions set out in **Art. 96(5)-(7) and (10)**, which means, notably, that they shall be "strictly necessary and proportionate", "not be systematic, massive or structural", and documented in "detailed records."

- These are **valuable safeguards** and should be retained.

However, especially the first requirement appears to stand in tension with the proposal's own **definition of an "online crisis situation" under Art. 4(9), which is "the dissemination of online content stemming from an ongoing or recent real world event which depicts harm to life or to**

physical integrity, or calls for imminent harm to life or to physical integrity." This definition, on the face of it, is broad enough to capture the reposting of ordinary, unrelenting news footage (floods, car accidents, violent protests, etc.) on social media and could become a flexible trigger for "exceptional" data sharing and processing at scale. Similarly, a **Europol referral** of online content to online service providers may not have the legal force of a formal removal order, but it would carry **authoritative weight**. It could cause a platform to take action against the person concerned, such as removing content or restricting an account, based on a piece of intelligence (possibly, unverified) that this person may never see, contest or have corrected—thus bypassing not just official mechanisms but procedural safeguards and accountability alike.

The same is true for **incidental data sharing**, which the Commission appears to deem both necessary and unproblematic. **Recital 39** explains that "[t]he effective gathering of information from publicly available sources for Europol includes notably the use of online search engines, including the input of personal data, which should not be regarded as a transmission or transfer of personal data to private parties." This is **a legal fiction**. The business model of every major search engine is to collect, retain and exploit the data entered into their systems, so queries using a person's name or professional association or any other identifying information are not neutral acts. They disclose a connection between the person concerned and Europol and may lead to their data being used for unauthorised purposes, including the training of AI models. In light of these risks, we urge the co-legislators to consider the following amendments.

- The definition of "online crisis situation" under **Art. 4(9) should be tightened**.
- Art. 15(b), 18(a) and 47(2)(b) should require **a documented reason, the preservation of referred content, a notification of the person concerned, and a route for review**.
- Recital 39 should be amended and **open-source searches regulated in the operative provisions** (privacy-preserving methods, purpose restrictions, query logs, etc.).

With respect to **third countries**, **Art. 43(5)(a) and (b) authorises the participation in JOACs, with access to the relevant data stored in the Police Shared Data Space**, where the opening Member State proposes it, Europol considers the participation relevant, and an agreement enabling the third country to exchange personal data with Europol is in force; an international agreement with Schengen associated countries may provide for **access to, and the ability to query, the Europol cross-matching service (Art. 93(3)(a))**; and the Management Board may, following authorisation by the European Data Protection Supervisor (EDPS), "authorise for a period not exceeding one year, which shall be renewable, **a set of transfers" of personal data (Art. 94(2), incorrectly numbered as (5) in the proposal)**. Fair Trials appreciates the practical need for cooperation with third countries, but these are significant and open-ended leaks in the information infrastructure protected by Union law and, in particular, the Charter. Persons whose data is being accessed or transferred may suffer changes to their legal status (entry bans, enhanced border checks, or the refusal of asylum; professional registration or security clearance issues; banking and financial

access restrictions, etc.), detention or prosecution abroad, and the loss of effective remedies. We therefore urge the co-legislators to consider the following recommendations.

- Third-country participation in **JOACs** should be clearly defined, prohibit the bulk export or onward transfer of data, ensure technical enforcement of provider restrictions, require continuous logging, and deletion or return of all data at closure. High-risk participation should be preceded by a fair trial and fundamental rights assessment.
- Third-country access to the new **cross-checking** service and **bulk transfers** should be **replaced by case-by-case exchanges for specific investigations**. High-risk cross-checks and transfers should be preceded by a fair trial and fundamental rights assessment.

Finally, with respect to **the EPPO**, **Art. 79(6) and Art. 81(4) and (5) depart from the principle of data ownership** laid down in Art. 33: the EPPO shall be granted indirect access to data related to offences that fall within its competence on the basis of a hit/no-hit automated system; in case of a hit, Europol shall be required to share the information that generated the hit "regardless of any restriction indicated pursuant to Articles 33(2) or (3);" the provider shall be notified. The rationale behind this exception is explained in Recital 87. Providing the EPPO with information regardless of restrictions is meant to reduce delays in access that the EPPO could request of its own accord, which in turn ensures the effective protection of the Union's financial interests.

We accept this rationale. It must be noted, however, that **the provider's restriction may exist precisely because the information is unreliable or may have been unlawfully obtained; it may be sensitive, subject to conditions from a third country, or otherwise unsuitable for onward use.** Removing the restriction without disclosing the reason for imposing it would deprive the EPPO, and later the court and the defence, of relevant context to assess the evidence. Fair Trials therefore urges the co-legislators to **amend Art. 79(6)** of the proposal.

- Where Europol shares data with the EPPO notwithstanding a provider restriction, the provider's **reasons for imposing the restriction should be shared as well.**

b. Data processing and retention

Europol may process information "[i]n so far as is necessary for fulfilling its tasks" (Art. 32(1)). It may process personal data for the purposes of cross-checking; strategic and thematic analyses; operational analyses; information exchange between Member States, Europol and other Union entities, third countries, international organisations and private parties; research and innovation projects; the issuing of public wanted notices (upon request); and the distinguishing between data subject categories under Annex II (Art. 32(2)(a)-(g)). The main and most concerning change in this area—the Explanatory Memorandum describes it as **"a fundamental shift" (p. 18)**—is the relaxation of the **requirement to distinguish between data subject categories** at all.

According to **Art. 32(6),** "Europol shall, **where applicable and as far as possible**, make a clear distinction" between data subject categories under Annex II; **Art. 32(7)** permits the processing of personal data on persons outside those categories **"where such processing is relevant and necessary" for the purposes set out in Art. 32(2)(a)-(g)**; and **Art. 32(10)** permits the temporary processing for up to 6 months **"for the purpose of determining whether processing is relevant and necessary."** The principal justification behind this shift is operational necessity: modern investigations generate vast amounts of unstructured data whose relevance and subject status are difficult or impossible to ascertain at the point of receipt; therefore, Europol needs to be able to process first and categorise "where applicable and as far as possible" (Recital 43). But the Commission is also candid about the fact that "[p]ersonal data that are initially not considered relevant for inclusion under a data subject category of Annex II may, upon further processing, **acquire operational significance or reveal connections** to ongoing investigations" (**Recital 44**). Europol, in short, should be able to process personal data in case it turns out to be useful.

That is a fundamental shift indeed. The data categorisation requirement is intended to ensure that Europol's processing powers can, in principle, extend only to personal data of persons with an established connection to crime: suspects and convicted persons, "prospective offenders" (as discussed in section 1.a. above), witnesses, victims, contacts and associates, and persons who can provide information (Annex II.B of Regulation (EU) 2016/794, as currently in force)—and that, in turn, is to ensure that personal data of persons who lack such a connection cannot circulate freely among 27 jurisdictions. The Commission now describes this system as "a key operational bottleneck" (Explanatory Memorandum, p. 18) and the processing of uncategorised information by Europol as a core operational task, effectively turning the exception into the principle. The proposed safeguards do little to alleviate these concerns. **Art. 32(8)** specifies that Europol "**shall inform" its Data Protection Officer** when processing or struggling to categorise data outside Annex II but does not mention any consequences attached to taking that step. **Art. 32(9)** requires that uncategorised personal data be **"kept functionally separate"**, but once again only **"where applicable and as far as possible."** And **Art. 32(7)** stipulates that uncategorised data **"shall be immediately deleted once the purpose of processing is fulfilled."** But of course, some purposes listed in Art. 32(2)(a)-(g), notably the automated cross-checking against the entire data holding, are open-ended by design, and so there really appears to be no clear time limit at all.

The **retention scheme in Art. 101** further compounds the problem. Personal data processed by Europol may be stored "for as long as is necessary and proportionate for the purposes for which the data is processed" (Art. 101(1)). Storage must be reviewed—by Europol—no later than 3 years after initial processing, with **continued storage renewable for successive 3-year periods,** and automatic deletion following only where no decision is taken **(Art. 101(2))**. There is no maximum time limit, and the agency who benefits from continued storage is in charge of deciding whether continued storage is "necessary and proportionate." The are two moments of external oversight. First, the EDPS "shall be informed" where data of victims, witnesses, or persons who can provide information (Art. 100(1)), or special categories of data, such as biometric data (Art. 100(2)), has been stored for more than 5 years (Art. 101(3)). And second, where a data provider has indicated

a restriction on deletion, or has deleted data from their own files, Europol may retain data only where it considers continued storage necessary on the basis of information more extensive than the provider's. In the former case, where the provider has indicated a restriction, Europol "shall request [their] authorisation" for continued storage; in the latter case, where the data has been deleted by the provider, Europol "shall inform the data provider" (Art. 101(4) and (5)).

Having consulted our network of criminal practitioners, we read these provisions as a startling **transition from suspect to data-led investigations at unprecedented scale**. Persons could enter the scope of criminal proceedings because they appear in a contact list, message, photograph, or seized dataset rather than because of an individualised suspicion. The Art. 32(10) temporary processing period could become a standing authorisation for profiling and relationship analysis. And personal data could sit on the Europol server, possibly without functional separation, ready to be cross-checked and queried, for an indefinite period of time. Fair Trials is taken aback by this vision and urges the co-legislators to make the following amendments.

- Processing of uncategorised data under **Art. 32(7)** should not be **"necessary and proportionate"** simply because "it might be useful", as suggested by **Recital 44**. Europol should be required to record a concrete investigative objective, the persons potentially affected, the access group, the expected duration, and the deletion trigger.
- **Art. 32(8)** should require **notification of the EDPS**, who should have **direct access to the records created under Art. 32(7) and the power to request correction.**
- Functional separation of uncategorized data under **Art. 32(9) should be mandatory**, not aspirational, and supported by data-level purpose tags that are visible to every user.
- The 6-month period in **Art. 32(10) should be the decisive outer limit** for the processing of uncategorised data—on expiry, any data item that has not been assigned an Annex II subject status should be automatically deleted from all servers.[2]
- Extensions of storage beyond the initial 3-year period laid down in **Art. 101(2) should require independent authorisation**. For data provided by Member States, Union entities, third countries or international organisations, authorisation should lie with the provider; for data originating from Europol's own analyses, private parties or publicly available sources, authorisation should lie with the EDPS.
- **Art. 101** should establish an **absolute maximum storage period, differentiated by data subject category**. The applicable period should **start on the date of receipt by Europol** to prevent late categorisation from resetting or extending the retention clock.

[2] This recommendation is consistent with EDPS, Decision of 3 January 2022 on the retention by Europol of datasets lacking data subject categorisation (Case 2019-0370).

- To facilitate the effective exercise of **remedies**, Europol should **notify** all persons whose data has been processed once notification no longer poses a material risk to an ongoing investigation and, in any case, once it has been deleted under **Art. 32(10)** or **Art. 101**.

While Art. 32 and Art. 101 give rise to the most structural concerns, there are other sections of the proposal where data processing standards have been subtly but significantly lowered.

As was already seen, the proposal normalises querying by means of **biometric data, including for the purpose of uniquely identifying a natural person**, across the new cross-checking service and the Europol Analytical Environment (Art. 39 and 41). The **safeguards in Art. 100(2)** mitigate this only partially: biometric identification "shall be allowed only where strictly necessary and proportionate", but—unlike other special categories of personal data—such processing **shall not have to supplement other personal data** held by Europol. That is, a biometric match may, in principle, be sought on the basis of the biometric template itself, rather than as corroboration of an existing investigative lead. **Recital 106** goes even further when it states that "[p]rocessing of biometric data for the purpose of uniquely identifying a natural person by Europol in the Europol Analytical Environment and where otherwise required under Union law **should be considered strictly necessary for preventing or combating crimes falling within the scope of Europol's competence."** A recital cannot establish a legal presumption, but the formulation is telling; read together with the operative provisions, it is clear that the proposal seeks to turn the processing of biometric data from an exceptional, individually justified measure into **a general investigative capability**. That is at odds with the case-law of the European Court of Justice. In C-205/21 (paras. 121-35), the Court held that national rules permitting the systematic collection of biometric and genetic data from any person accused of an intentional offence is **incompatible with Article 10 of Directive 2016/680**, unless competent authorities must first verify and establish that collection is in fact strictly necessary, that is, other measures "less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by **Articles 7 and 8 of the Charter**" (para. 126) would not suffice.

- The presumption of strict necessity for the processing of biometric data for the purpose of uniquely identifying a natural person in **Recital 106** should be deleted.
- Every query by means of biometric data under Art. 39 and 41 should require **a defined and documented purpose and a human, case-specific necessity assessment**. This log should be part of the auditable data record, as recommended above.

With respect to third countries, Europol shall not process **"[a]ny information which has clearly been obtained in obvious violation of human rights"** (**(Art. 91(8)**, see also **Art. 79(7)** with respect to other Union entities). The risks of third country access to the Europol information infrastructure have already been discussed; and it is hard to imagine a case where a threshold this high could act as an effective safeguard. Human rights violations are rarely both "clear" and "obvious" and, crucially, they do not have to be. Ruling on information obtained through torture or inhuman and

degrading treatment, for instance, the European Court of Human Rights has made clear that all that is required is **"a real risk"** (*El Haski v. Belgium* (App. no. 649/08), paras. 85-89).

- The threshold for human rights violations in **Art. 91(8) and Art. 79(7)** should be **aligned with the case-law of the European Court of Human Rights**.

Finally, the proposal removes the **explicit protection previously afforded to minors** (compare **Art. 100(1)** to Art. 30(1) of Regulation (EU) 2016/794, as currently in force), leaving children's data to be governed by general rules on necessity, proportionality and special categories. This is problematic because it eliminates child-specific safeguards precisely where Europol's expanded cross-checking, biometric matching and analytical powers materially increase the risk that data on child victims and victim-offenders (Recital 104 and Art. 14(d) acknowledge the issue of **child criminal exploitation**), witnesses, contacts , etc., will be collected, used and retained at scale. We therefore urge the co-legislators to consider the following recommendations.

- **Art. 100** should **include persons under the age of 18.** It should require a **documented best-interests assessment**, including a presumption in favour of safeguarding status where exploitation is plausible, **access controls** and **case-specific authorisation for biometric queries**, and a **mandatory notification of the Fundamental Rights Officer**.
- **Art. 101** should specify both a **shorter review period** and a **shorter maximum retention period**, as recommended above, for data on persons under the age of 18.

2. Europol as "operational hub"

The proposal formally stays within the limits of Art. 88 TFEU. Europol shall provide "operational support"—a term which remains undefined—to the Member States (Art. 6(1)(b), (2)(a)) and it "shall not apply coercive measures in carrying out any of its tasks" (Art. 6(3)). However, a number of provisions are clearly designed to **enhance Europol's ability to steer national investigations**.

Art. 11(1) and (2) permit Europol to request the competent authorities of the Member States, via their national units, to **initiate, conduct or coordinate criminal investigations** into crimes that fall within its competence (as is the case under Art. 6(1) of Regulation (EU) 2016/794, as currently in force) and into specific crimes which concern only one Member State but affect a common interest covered by a Union policy. These requests are to be treated "as a matter of priority" and require a reasoned decision within one month; reasons may be withheld only if their disclosure is contrary to essential security interests or jeopardises the success of an ongoing investigation or the safety of an individual (Art. 11(4) and (5)). Regardless of whether the Member State concerned accedes to the request, Europol shall "immediately inform" Eurojust and the EPPO for follow-up (Art. 11(6) and (7)). According to **Art. 20(6)**, the Executive Director shall propose to the competent

authorities of the Member States, via their national units, the **establishment of operational task forces** where such task forces "would provide added value"; **Art. 22(7)** authorises the same for **Europol deployments**. The ability to participate in **joint investigation teams** is retained **(Art. 21)**. **Art. 26** establishes **Europol support offices** within national units, staffed by seconded personnel under the joint responsibility of Europol and the Member State concerned (Art. 26(3)).

Viewed against the backdrop of the proposed information infrastructure, these changes mark a significant departure from Europol's role as a merely "supportive" agency. While requests and proposals are technically non-binding, they carry authoritative weight, especially if based on the ongoing, automated analysis of criminal intelligence from 27 Member States, and especially if the national units who receive and respond to them are stacked with Europol staff. Our network of practitioners has noted that **national authorities already feel pressure to treat requests for the initiation of criminal investigations as practically directive**. In many States, that is due to the principle of legality; an investigative lead from Europol is an investigative lead that competent authorities are obliged to pursue. We expect these patterns to proliferate, and purposely so. It is clear from the above provisions that the Commission seeks to convert the agency into an active participant in national investigations. **Art. 22** is the most striking example. Deployed Europol staff shall be provided with **"all relevant information without undue delay"** and, where possible, be granted direct access (Art. 22(6)(a)); they shall also be allowed to **be present during the execution of investigative measures** (Art. 22(6)(b)). In addition, and in tension with the principle of national procedural autonomy, as recognised by the European Court of Justice, Art. 22(6)(d) asks Member States to **ensure, in accordance with national law, that the outputs produced through Europol deployments "may be used as evidence in national investigative and judicial proceedings**."

For the defence, the problems that arise here are centred on **attribution and accountability**. It needs to be **visible** whether investigative acts were prompted by Europol and, if so, on the basis of which information; whether Europol was involved in their execution and, if so, to what extent, under whose supervision, etc; and whether Europol (co-)authored a particular output presented as evidence in the proceedings. These questions are difficult to answer—and, more importantly, the answers may be inconsequential—if Europol staff act under a **dual line of responsibility** but are **effectively captured by none**: they are not "authorities" under national codes of procedure, and they enjoy immunity from legal proceedings as Union staff (Art. 125(1)). Fair Trials urges the co-legislators to reflect on these issues and to consider the following recommendations.

- In tandem with our recommendations on data sharing/processing by Europol, **requests and proposals under Art. 11(1) and (2), 20(6) and 22(7) should be recorded and included in the case file** of any subsequent national proceedings.
- **Cooperation agreements under Art. 20, 21 and 22** should all require a **precise and documented allocation of tasks and responsibilities** between Europol and national law enforcement staff, including regarding the selection and use of analytical tools, the interpretation of results, and the production of outputs for use in national proceedings.

- **Art. 22(6)(d)** should require outputs produced through Europol deployments to identify the responsible unit and, where appropriate, **the responsible analyst**. The clause on evidentiary use should be deleted or, failing that, paired with a requirement that **outputs obtained in breach of fair trial and fundamental rights need to be excluded**.
- **Art. 125** should set out the procedure, competent authority and conditions for **waiver of immunity** where evidence of Europol staff is required in national proceedings.

3. Europol as "technology and innovation hub"

Chapter IV and specifically **Art. 57-64** of the proposal give Europol a comprehensive research and innovation mandate, authorising the agency to identify "immediate, emerging and longer-term **capability needs** at Union level" (Art. 57(2)); to assist the Commission in programming Union **funding programmes** for research, innovation and capability development, and to participate in activities funded through those programmes (Art. 58(1) and (2)); to **develop, operate, host and provide advanced capabilities** (e.g., "AI-enabled applications, secure information-processing environments, forensic capabilities, cloud-based collaborative environments, and capabilities supporting the processing and analysis of lawfully obtained encrypted data", see Explanatory Memorandum, p. 20) (Art. 59(1)); to **test and validate** algorithmic tools, AI systems and models in regulatory sandboxes (Art. 61(1)); and to **support the early deployment, scaling, and effective integration** of those capabilities into national investigations (Art. 62(1), 63(1), 64).

Having consulted our network of criminal practitioners, the principal concern here is not the envisioned research and innovation activities per se, but the absence of **procedural safeguards for the defence**. In its current form, the Regulation would enable advanced capabilities to shape investigative conclusions without enabling both courts and the defence to assess, test and/or challenge the method by which these conclusions were produced.

The protections that are being proposed primarily relate to data protection, and they come with significant omissions and exceptions. **Art. 61(1) and (2)** confine the development, modification, testing, validation and, where relevant, the training of algorithmic tools, AI systems and models to a "separate, isolated and protected processing environment" that must comply, for high-risk AI systems, with the requirements on regulatory sandboxes laid down in Regulation (EU) 2024/1689; and yet, **Art. 61(3)** permits Europol to grant access to this environment to private parties with whom it is cooperating. **Art. 102(2)(c)(iv)** specifies that personal data processed during research and innovation projects "shall not lead to measures or decisions affecting the data subjects"; but this restriction need not apply to the adjustment or modification of capabilities that are already in use **(Art. 102(4)). Art. 102(2)(d) and (6)** require Europol to keep a data processing log and, where applicable, a document detailing the process of, and rationale behind, the training, testing and validation of algorithms. The latter shall be made available to "interested parties" upon request, which, remarkably, does not seem to include the defence. And finally, **Art. 108(1)** requires prior

consultation of the EDPS for new types of processing in accordance with Art. 90(1) of Regulation (EU) 2018/1725 but permits Europol to start if the EDPS has not provided written advice within 8 weeks and, exceptionally, where doing so is "particularly urgent and necessary" **(Art. 108(2))**.

The Explanatory Memorandum (p. 11) concedes that capability and technology development under Chapter IV was **excluded from the impact assessment** on the ground that "broad support already existed." But of course, as our network is keen to point out, broad support among those who will benefit from a particular capability says virtually nothing about its impact on those who will be subjected to it. An adequate defence requires sharp, dedicated safeguards that apply to, but legally exceed, the project phase of Europol's research and innovation activities. Fair Trials urges the co-legislators to consider the following recommendations.

- **Art. 62** should require that advanced capabilities undergo **independent validation** prior to any operational use; defence experts should be consulted in this process.
- In tandem with our recommendations on data sharing/processing by Europol, **Art. 59** should require that where a Europol-developed, operated, hosted, or provided advanced capability is relied upon in national investigations and proceedings, Europol needs to **preserve and disclose**—or make available for controlled inspection—the tool and model version, input data, configuration, processing steps, validation report, error rates, known limitations, rejected alternatives, and a record of human reviews and interventions.
- With respect to access to documentation under **Art. 102(6)**, both the defence and court-appointed experts should be expressly recognised as **"interested parties"**.
- **Private party access to testing environments under Art. 61(3)** should be clearly defined, prohibit the export or onward transfer of data, and require continuous logging.
- The safeguard exception for existing capabilities in **Art. 102(4)** should be **deleted**.
- The **8-week fixed consultation period in Art. 108(1) should be deleted** to ensure the EDPS can claim the complexity-based extension for a total of up to 10 weeks under Art. 90(4) of Regulation (EU) 2018/1725.The exception in **Art. 108(2)** should be **deleted**.

Summary of key concerns

The Commission seeks to transform Europol into a centralised information, operational and technology and innovation "hub." If the co-legislators share this vision, they must also ensure the safeguards that make it compatible with the rights of the defence. To help them do so, we have drawn attention to the following key areas of concern:

- complete and auditable records for every data item received, for every operational support activity, and for every use of advanced capabilities by Europol;
- independent authorisation of continued storage of categorised data, and absolute maximum storage periods, differentiated by data subject category;
- temporary processing of uncategorised data for a strict, non-renewable period only, and mandatory functional separation from categorised data;
- documented and case-specific necessity and proportionality assessments for the processing of biometric data and data related to persons under the age of 18;
- increased safeguards for data sharing with private parties and third countries;
- possible waiver of immunity where evidence of Europol staff is required;
- independent validation of advanced capabilities before any operational use;
- effective oversight by the EDPS.

fairtrials.org

Fair Trials

Fairness, equality, justice