EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European Lawyers
Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE Position Paper on the Proposal for Regulation amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

6/05/2021

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 45 countries, and through them more than 1 million European lawyers. The CCBE responds regularly on behalf of its members on policy issues which affect European citizens and lawyers.

In December 2020 the European Commission published a proposal for a regulation amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data in support of criminal investigations, and Europol's role on research and innovation.

The proposal sets out the new powers to be given to Europol to process personal data "*in support of a criminal investigation outside the categories of data subjects listed in Annex II*" (Article 18a), to transmit operational personal data to another Union institution, body, office or agency "*when deemed necessary for the performance of tasks of said bodies*" (Article 24), to receive personal data directly from private parties and process those personal data "*to prevent the dissemination of online content related to terrorism or violent extremism in crisis situations*" (Article 26a), and to process personal data for research and innovation purposes (Art. 33a).

It is the purpose of the present paper for the CCBE to set out its position in relation to a number of aspects of the proposal.

A. General comments

First, the CCBE observes the concepts of "national security", the "fight against terrorism", prevention of "violent extremism"; as well as the invocation of a claimed need to address crisis situations are often used by States and other authorities as a ground to justify a claimed necessity to obtain access to personal data. A major problem in this regard is the lack of any internationally accepted common definition of these terms ("national security", "terrorism", "extremism", etc) which makes it difficult for courts to effectively ensure that surveillance measures comply with a strict test of what is necessary and proportionate. This matter has already been addressed by the CCBE in its Recommendations on the protection of fundamental rights in the context of national security[1].

The CCBE believes that any direct or indirect access to personal data of citizens undertaken by a State should fall within the bounds of the rule of law and, given that it would constitute an interference with fundamental rights, it must be proportional and, in particular, be kept to a minimum as regards the scope of surveillance and period of data retention[2].

---

1 CCBE Recommendations on the protection of fundamental rights in the context of national security, pp. 2 and 22.

2 The Court of Justice of the EU has recently delivered judgments in cases La Quadrature du Net e.a. and Privacy International (C-511/18, 512/18, 520/18 and 623/17), confirming the importance given to data protection by the Court

In this respect, the CCBE points out that the European Court of Human Rights (hereinafter "**ECtHR**") has ruled that the mere storing of data relating to the private life of an individual, irrespective of their subsequent use, amounts to an interference within the meaning of Article 8 of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence[3]. For its part, the Court of Justice of the European Union (hereinafter "**CJEU**") considers that access to personal data with a view to its retention or use affects the fundamental right to respect for private life guaranteed in Article 7 of the Charter of the Fundamental Rights of the EU (hereinafter "the Charter"). Such processing of personal data also falls within the scope of Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article[4]. Moreover, both courts consider that access to personal data by a public authority constitutes a further interference[5]. **As a consequence, access, retention and further use of personal data by public authorities, such as law enforcement authorities, within the remit of surveillance measures must not exceed the limits of what is strictly necessary, assessed in the light of the Charter, in order to be justified within a democratic society.**

Such interference becomes particularly dangerous when there is accessed data and communications which have been granted special protection by law. This is clearly the case in relation to communications between lawyers and their clients, since, in all EU Member States, the law protects from disclosure information communicated in confidence between lawyers and their clients[6]. Furthermore, this protection is, in contentious matters, an essential component in guaranteeing the ECHR Article 6 right to a fair trial, which is an absolute right, and in all matters a foundational principle of the rule of law. **Consequently, the CCBE is especially concerned by the impact that any EU measure on Europol's access to personal data may have on the professional secrecy or legal professional privilege (hereinafter "PS/LPP").**

An additional problem in relation to any access to lawyers' data stored online, is the existing difficulty of identifying in advance whether data are covered by PS/LPP. The CCBE acknowledges that Internet service providers have not yet the means, or, if they do so, then only on a very limited basis, to recognise whether the data requested by law enforcement authorities is covered by professional secrecy[7]; it is, therefore, possible that access may be given to protected data, leading to breaches of PS/LPP.

On this issue, the CJEU recognised that "*the transmission of traffic data and location data to public authorities for security purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of means of electronic communication from exercising their freedom of expression, guaranteed in Article 11 of the Charter.* ***Such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy***"[8]**.**

---

and the strict interpretation of the possibility of derogating from the State's obligation to ensure the confidentiality of data on the grounds of national security. The Court confirmed that any derogation must always be limited to what it is strictly necessary and accompanied by effective safeguards. In particular, it was ruled that EU law precludes national legislation requiring a provider of electronic communications services to carry out a general and indiscriminate transmission or retention of data for the purpose of combating crime.
See also EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, para. 20-22.

3 ECtHR, 4 December 2008, S. and Marper v. the United Kingdom, applications 30562/04 and 30566/04, §67.

4 CJEU, 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18, §170.

5 CJEU, 8 April 2014, Digital Rights Ireland, Cases C-293/12 and C-594/12; ECtHR, 26 March 1987, Leander v. Sweden, Application 9248/81, §48.

6 CCBE Recommendations on the protection of client confidentiality within the context of surveillance activities, p. 9

7 Talks conducted between the CCBE and EURO-ISPA (European association of European Internet Services Providers Associations, https://www.euroispa.org/about/).

8 CJEU, 6 October 2020, Privacy International, Case C-623/17, §72.

In this regard, the CCBE stresses that Internet service providers and/or law enforcement authorities and Europol should be required to ensure that the technology used to collect, process and exchange personal data amongst them guarantees that there is no interference with any kind of data protected by professional secrecy. In any event, law enforcement authorities should be required to use all technological means available to leave material protected by PS/LPP out of the scope of surveillance operations or the collection, storage, processing and transfer of personal data. The development of such technology should be a top priority.

With a view to informing legislators and policy makers about standards that must be upheld in order to ensure that the essential principles of PS/LPP are not undermined, it is proposed to set out the following recommendations, based on the CCBE Recommendations on the protection of client confidentiality within the context of surveillance activities[9].

1. Need for legislative control

The CCBE considers that any surveillance activity undertaken by law enforcement authorities needs to be regulated with adequate specificity and transparency. This principle must apply to Europol. Therefore, any European measure on Europol's powers to access personal data must be subject to effective legislative control within a clear regulatory framework[10].

In this regard, the CCBE stresses that the concepts of national security/extremism/terrorism/crisis as justificatory elements in relation to the processing personal data should be laid down with adequate specificity and clarity. The proposal provides for Europol to exchange personal data with private parties related to crisis response according to the new Article 26a. The aim of this provision is to prevent the dissemination of content related to terrorism or violent extremism in crisis situations. However, the proposal does not define in particular what a crisis situation is, nor terrorism nor violent extremism. The CCBE considers that the proposal should lay down more clear and precise provisions with regard to the justifications for the collection, processing and exchange of personal data.

The power to access personal data needs to be regulated with the same specificity and transparency. **The CCBE considers that access to personal data should be permitted only when Europol, as the body wishing to undertake surveillance, can establish that there are compelling reasons giving rise to a sufficient degree of suspicion to justify the interception[11]. Such reasons should be clearly defined.**

In this regard, the CCBE refers to the most recent case-law of the CJEU which rules that "a*s regards the objective of preventing, investigating, detecting and prosecuting criminal offences, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be*

---

9 CCBE Recommendations on the protection of fundamental rights in the context of national security, pp. 2 and 22.

10 This is in line with the position of the EDPB, as outlined in the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (para. 26-31).

11 Similarly, the EDPB requires "necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated" (EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, para. 32-38).

justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general."[12]

Beyond the regulatory framework, the CCBE considers that effective legislative controls and democratic oversight should be in place to politically assess Europol's activity and the processing of personal data or data covered by LPP/PS. In this regard, the CCBE notes that, in accordance with Article 88 TFEU, Europol regulation provides for a Joint Parliamentary Scrutiny Group (Article 51, hereafter "**the JPSG**"), with members both from national parliaments and from the European Parliament. The proposal reinforces this scrutiny by laying down that Europol should provide the JPSG with annual information on the use of its additional tools and capabilities and the result thereof (Recital 40, modification of Article 51 §3).

However, the CCBE considers that the current legislative scrutiny and the proposed reinforcement provisions are not sufficient to ensure an effective democratic oversight of Europol's activities. Regarding the risks and threats to fundamental rights caused by the processing of personal data from law enforcement authorities and Europol, the powers of scrutiny conferred upon the JPSG should be enhanced so as to extend beyond the power to question or to be informed of Europol's activities. The regulation should provide for more concrete powers and responsibilities for the JPSG and effective sanctions and other appropriate consequences in the event of a finding of infringement of fundamental rights.

2. Prior judicial authorisation, independent control and effective remedies

According to the proposed new Articles 26 §6a, and 26a §5, Europol may request Member States to obtain personal data from private parties under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol. It is specified that "*Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives*".

In this regard, the CCBE observes that prior **authorisation given by a Court** must be required for any access to personal data by law enforcement authorities. **The ECtHR and the CJEU have specified on many occasions that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system[13].**

Legislation must ensure that personal data obtained without specific prior judicial authorisation is inadmissible in a court of law. Furthermore, any intercepted material ruled as having been unlawfully acquired, should be required to be destroyed. Furthermore, any lawfully intercepted personal data should be used solely for the purpose for which the authorisation was granted.

In this regard, the CCBE stresses that the proposal must not allow Europol to bypass neither the need for prior judicial authorisation nor the independent and impartial oversight system which are essential guarantees[14].

Furthermore, in order to provide effective legal protection against unlawful surveillance, it is necessary that **legal remedies**[15] are made available to citizens whose data have been processed. In particular, once it has been disclosed that surveillance measures have been undertaken, citizens must have the

[12] CJEU, 6 October 2020, La Quadrature du Net e.a., Cases C-511/18, C-512/18 and C-520/18, §140. See also CJEU, 2 March 2021, H.K. v Prokuratuur, Case C-746/18, §45.

[13] ECtHR, 1978, Klass and others v. Germany, Application 5029/71; CJEU, La Quadrature du Net, §189.

[14] European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.

[15] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, para. 43-47.

right to be informed of the data which have been collected and processed and must be able to challenge the legality of such measures before a judge. Further, appropriate sanctions should be imposed upon persons and agencies who have undertaken unlawful surveillance.

The CCBE notes that the Europol Regulation provides that affected data subjects can lodge a complaint with the EDPS in the case of an irregular processing of personal data by Europol (Article 47). Further, any individual, who has suffered damage from an unlawful data processing operation shall have the right to receive compensation from Europol, in accordance with Article 340 TFUE, and shall have the right to bring an action against Europol before the CJEU or before national courts against Member States.

However, the CCBE considers that such remedies should be reinforced, within Europol itself, in order to enable the persons affected to exercise their rights under Article 7 and 8 of the Charter to be informed of the processing of their data, to request access to their personal data which has been the subject of a processing and, where appropriate, to have the data rectified or erased, as well as to avail themselves of an effective remedy before a tribunal.

Respect for the Rule of law and PS/LPP must be an **overarching principle** in the context of any EU measure on surveillance and, in particular, on access to data for the purposes of security and law enforcement. Furthermore, the law needs to provide for **explicit protection of PS/LPP**, always affording it the highest level of protection.

In the event that access to data relating to lawyer-client communications is granted in exceptional circumstances, the CCBE stresses that there must be an independent judicial supervision[16] at all stages of the surveillance procedure, on a case-by-case basis. The judge supervising the implementation of the interception must be different from the judge who allowed it.

Furthermore, where data protected by LPP/PS are wrongly intercepted without authorisation, such data should be erased immediately, regardless of whether it relates to the concerned case or not. In case of doubt regarding the privileged nature of data, Europol should separate the concerned data and carry out the necessary controls before any processing.

3. Essential guarantees applying to the transfer of personal data to private parties

According to the proposed new Articles 26 §5 and 26 §6, Europol may transmit or transfer personal data to private parties, established within or outside the EU, on a case-by-case basis in several situations and in compliance with the requirements for absolute and strict necessity. A specific authorisation from the Executive director of Europol is requested if the private party concerned is not established within the Union and conditions are to be met in order to grant this authorisation. In particular, personal data shall not be transferred if the Executive Director determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer. Also, transfers shall not be systematic, massive or structural. The specific safeguards provided for in the proposal were welcomed by the EDPS[17].

The CCBE recalls that the data subject whose personal data are transferred to a third country must be afforded a level of protection essentially equivalent to that which is guaranteed within the European Union[18]. Therefore, any transfer of personal data to private parties made by Europol,

[16] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, para. 39.

[17] EDPS Opinion on the proposal for Amendment of the Europol Regulation, Opinion 4/2021, 8 March 2021, point 18.

[18] CJEU, 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18, point 96.

within or outside the EU, must respect the above-mentioned European essential guarantees recognised by the EU Data Protection Board:

- **The transfer should be based on clear, precise and accessible rules.**
- **Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.**
- **An independent judicial oversight should be ensured.**
- **Effective remedies should be available to the data subject.**

Moreover, the CCBE considers that additional safeguards must be included in the proposal regarding the transfer or transmission of personal data to private parties by Europol, beyond the ones provided by the proposed regulation and the EU data protection law. The CCBE stresses that any transfer of personal data to private parties must take due account of the rights of the defence and the right to a fair trial. In any event, Europol shall ensure that personal data protected by LPP/PS are not transferred.

Furthermore, before any transmission of personal data to private parties, Europol must ensure that the data are adequate, relevant and up to date. This is of significant importance when, for instance, the data concern information related to a criminal offence for which the data subject has been acquitted.

As recommended by the EDPS in its opinion on the proposal, such safeguards must apply to transmissions to private parties within or without the EU[19].

B. Europol's new research and innovation powers

The CCBE considers that the proposed research and innovation power should be linked to strong safeguards, in particular on transparency and monitoring, especially by the EDPS.

1. Development of AI-based technologies for law enforcement authorities

According to Recital (38), "*Europol should play a key role in assisting Member States to develop new technological solutions based on artificial intelligence, which would benefit national law enforcement authorities throughout the Union*".

The CCBE considers that Europol should not lead in the development of new technological solutions based on AI for law enforcement authorities. Indeed, the CCBE stresses that much debate is still needed to critically assess what role, if any, AI tools should play in the field of law enforcement and criminal justice. Whilst it may be possible that the use of AI could contribute to the prevention or solving of crimes, the risks of bias and discrimination against particular groups in society are high, and the threat of mass surveillance by AI systems poses a risk to open and pluralistic societies.

Therefore, AI-based tools for law enforcement should be introduced only when there are sufficient safeguards against any form of bias or discrimination. All measures of increased surveillance should be carefully balanced against the impact that they may have on an open and pluralistic society. In this regard, it is not upon Europol, as the law enforcement European Agency, to play a key role in promoting ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety and fundamental rights. If any AI-based technologies have to be developed for justice and law enforcement systems at the European level,

[19] EDPS Opinion on the proposal for Amendment of the Europol Regulation, Opinion 4/2021, 8 March 2021, point 18.

it should be upon the European legislator first to build the above-mentioned safeguards in an open and transparent manner.

2. Scope of Europol research and innovation activities

According to the proposed **Article 18 §2 (e)**, Europol could process personal data for the purpose of "*research and innovation regarding matters covered by this Regulation for the development, training, testing and validation of algorithms for the development of tools*".

The CCBE notes that the EDPS in its Opinion on the proposal for amending the Europol regulation concluded that the scope of the new research and innovation processing purpose is too broadly defined in the new Article 18 §2 (e)[20]. The CCBE agrees with this conclusion.

Given the high risks of bias and the threats of mass surveillance, the scope of Europol research and innovation activities should be clearly defined in the proposal by providing, in particular, the objectives pursued, the targeted activities of law enforcement authorities, the tools to be developed and their foreseen uses.

3. Safeguards and control upon Europol research and innovation activities (New article 33a)

The CCBE notes that additional safeguards have been provided for in a new Article 33a regarding the processing of personal data by Europol in the context of research and innovation. Furthermore, Europol is required to keep a complete and detailed description of the processing and rationale behind the training, testing and validation of algorithms to ensure transparency and for verification of the accuracy of the results.

Regarding the monitoring of Europol research and innovation activities, the proposal states that any project shall be subject to prior authorisation by the Executive Director of Europol based on a description of the envisaged processing activity setting out the necessity of the processing; a description of the retention period; conditions for accessing data; a **data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome, and the measures envisaged to address those risks.** Also, prior to the launch of a project processing personal data for research and innovation, the EDPS is to be informed.

The CCBE considers that the safeguards laid down in the proposal are necessary. However, such safeguards are not sufficient and only constitute no more than a minimum. Regarding the prior authorisation of research and innovation projects, the CCBE considers that such authorisation should come from an independent authority. The Executive Director of Europol should not be the one to decide whether a project should be launched or not, nor the only person performing a data protection impact assessment of the risks to the rights and freedoms of data subjects, including, but not limited to, the risks of bias.

This task could be given to the EDPS. The CCBE notes that the Europol regulation already provides by Article 43(f) for the EDPS to impose a temporary or definitive ban on processing operations by Europol which are in breach of the provisions governing the processing of personal data. However, in view of the risks and threats posed to rights and freedoms, such assessment should not be subsequent to the launch of a new research and innovation project by Europol.

Furthermore, the CCBE stresses that, for the reasons explained above, the JPSG should be informed on a case-by-case basis prior to the launch of any project of research and innovation. Such projects should also be conducted in a transparent manner, not only with regards to the results of the research but also with regard to the whole process. Stakeholders, including the legal

[20] EDPS Opinion on the proposal for Amendment of the Europol Regulation, Opinion 4/2021, 8 March 2021, point 33.

profession, who are concerned by the use of the tools for law enforcement authorities should be informed of each intended project and be consulted on it.

C. Final remarks

Finally, the CCBE draws attention to the European Data Protection Supervisor (EDPS) Report dated 17 September 2020, which resulted in a formal "admonishment" against Europol, based on the potentially unlawful processing of personal data of vast numbers of innocent people.

According to the report, Europol receives vast quantities of data from national law enforcement agencies and elsewhere, and in order to use that data for criminal investigations, has adopted means and methods that do not comply with the legislation governing the agency.

The result, says the EDPS, is:

"…a situation where large amounts of personal data for which it is uncertain that they comply with the requirements set up by… the Europol Regulation, are stored on Europol systems for several years. As such, the continued storage of personal data that might go beyond the limits contained in these articles undermines the principle of data minimisation…"

The report underlines that Europol most likely is unlawfully processing personal data of a vast – in fact, unknowable – number of people: *"…there is a high likelihood that Europol continually processes personal data on individuals for whom it is not allowed to do so and retain categories of personal data that go beyond the restrictive list provided in… the Europol Regulation. While the exact amount cannot be quantified, the increase in the use of the [...] observed for the last years clearly shows that the amount of large datasets shared by MS with Europol is rapidly growing."*

The report goes on to set out what this means for individuals: *"The processing of data about individuals in an EU law enforcement database can have deep consequences on those involved. Without a proper implementation of the data minimisation principle and the specific safeguards contained in the Europol Regulation, data subjects run the risk of wrongfully being linked to a criminal activity across the EU, with all of the potential damage for their personal and family life, freedom of movement and occupation that this entails."*

The CCBE urges Europol and the competent European Institutions, before any further legislative process or enaction, to address the above concerns by providing an adequate response, especially by laying down the necessary measures and policies they plan to undertake in order to tackle the issue of the unlawful processing of personal data that has arisen.

Further, the CCBE notes that the Europol regulation requires to be evaluated by the European Commission, by 1 May 2022. Article 68 lays down that this evaluation should assess, in particular, the impact, effectiveness and efficiency of Europol and of its working practices. This evaluation is the best occasion to undertake a deep assessment of the regulation regarding the compatibility of Europol's activities with fundamental rights. Therefore, the CCBE considers that the adoption of the proposal to strengthen Europol's mandate, following the EPDS admonishment, is premature and hasty.