EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPEENS
AVOCATS EUROPEENS

Le Président
The President

Olivier Onidi
Deputy Director General Directorate-General for Migration and Home Affairs
European Commission

Carlo Van Heuckelom
Justice and Home Affairs Counsellor
Permanent Representation of Belgium to the European Union

Cc:
Anu Talus, Chair of the European Data Protection Board (EDPB)
Isabelle Vereecken, Head of the EDPB Secretariat

Wojciech Wiewiórowski, European Data Protection Supervisor (EDPS)
Anna Buchta, Head of Policy and Consultation Unit, EDPS
Plamen Angelov, Head of Activity for Justice and Home Affairs
at Policy and Consultation Unit, EDPS

Brussels, 15 April 2024

CCBE letter on the protection of confidentiality of lawyer-client communications in the context of the activities of the High-Level Group (HLG) on access to data for effective law enforcement

Dear Mr Onidi,
Dear Mr Van Heuckelom,

I am writing on behalf of the Council of Bars and Law Societies of Europe (CCBE) which represents the Bars and Law Societies of 46 countries, and through them more than 1 million European lawyers. The CCBE is recognised as the voice of European lawyers, representing European Bars and Law Societies in their common interests before European and other international institutions. Defending human rights and the rule of law are central values of the CCBE.

The CCBE welcomes the opportunity to submit its written observations relating to the work of the high-level group on access to data by law enforcement authorities. The CCBE would like to convey that the regulation of such activities, and especially the appropriate safeguards and respect for the confidential nature of lawyer-client information, are of core interest to the CCBE.

The protection of confidentiality is one of the fundamental obligations of the legal profession and the foundation of the proper administration of justice and the right to a fair trial. It has been extensively recognised in the case law of the European Court of Human Rights (ECtHR) and the

Court of Justice of the EU (CJEU) which we would like to draw your attention to (see the list at the end of the letter). In particular, the ECtHR states in *Michaud* that:

> '*[...] while Article 8 protects the confidentiality of all "correspondence" between individuals**, it affords strengthened protection to exchanges between lawyers and their clients**. This is justified by the fact that **lawyers are assigned a fundamental role in a democratic society, that of defending litigants**. Yet lawyers cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential. It is the relationship of trust between them, essential to the accomplishment of that mission, that is at stake. **Indirectly but necessarily dependent thereupon is the right of everyone to a fair trial, including the right of accused persons not to incriminate themselves.**'* (own emphasis added)

We have examined multiple legislative and policy initiatives which pertain to access to data through that lens (list available at the end of this letter).

We understand that the law enforcement authorities need to find new ways to effectively investigate crime given the technological advancements. We also fully support the objectives to combat crime and the adoption of specific measures to prevent and fight it. At the same time, **we are concerned by potential threats regarding law enforcement access to data which can interfere with the confidentiality of lawyer-client communications**, and more broadly, to fundamental rights (including the right privacy and the right to a fair trial).

We believe that any system providing for direct or indirect access to personal data of citizens undertaken by a State should fall within the bounds of the rule of law and must respect the legal requirements set out in EU law and the settled and well-established case law of the CJEU and the ECtHR. Given the risk that any access may constitute an interference with fundamental rights, it must be proportionate and, in particular, be kept to a minimum as regards the scope of surveillance and period of data retention. **Crucially, such systems must guarantee the inviolability of data and other evidence falling under the principle of legal professional privilege or professional secrecy.** To that end, any system which provides access to data should include the following provisions:

- **provisions ensuring the protection of confidentiality of lawyer-client communications**;

In this regard, we would like to stress that any system which regulates access to data must not prevent lawyers from adequately protecting the confidentiality of their communications through encryption methods. Moreover, the mechanism would have to provide the possibility to challenge production orders/warrants on the grounds of the protection of confidentiality of lawyer-client communications. Finally, the law enforcement authorities should be required to use any means to exclude material protected by professional secrecy and legal professional privilege from the scope of the production orders/warrants.

- **provisions setting out clear and foreseeable conditions for issuing production orders/warrants, such as proper justification, reasonable suspicion and judicial oversight;**

To this end, the concepts of national security, extremism, terrorism, or crisis as justificatory elements in relation to the processing of personal data should be laid down with adequate specificity and clarity. Moreover, any access to personal data by law enforcement authorities must be subject to prior authorisation provided by a Court.

- **provisions ensuring there are appropriate remedies to provide effective legal protection against unlawful production orders/warrants;**

It is necessary that legal remedies 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 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. Furthermore, there should exist appropriate sanctions on persons and agencies who have undertaken unlawful surveillance.

- **provisions ensuring notification to data subjects;**

We stress that the imposition of confidentiality restrictions on production orders/warrants must be subject to the approval of an independent judicial authority and in each case be duly motivated and justified by the issuing authority on the basis of meaningful and documented assessments. In case of lawyers or law firms, there should also be clear procedures for notification of the relevant professional bodies of production order/warrant issued to the member of legal profession.

- **provisions ensuring equality of arms between the prosecution and defence.**

Equality of arms is an inherent principle to the right to a fair trial, as guaranteed by Article 47 of the EU Charter of Fundamental Rights and Article 6 of the European Convention on Human Rights. The CCBE would like to stress that, with the deployment of new technologies in the justice system and law enforcement, there are numerous areas where the principle of equality of arms is affected, for example with regard to access to the case file or access to tools to analyse data and evidence.

We have elaborated extensively on the above points in our 'Recommendations on the protection of client confidentiality within the context of surveillance activities.'

In addition, we urge the Commission and the Presidency to ensure that its planned recommendations, and any future actions based thereon, comply with the principles of good governance and better regulation. In particular, they should be supported by a comprehensive evidence-based impact assessment and broad and meaningful stakeholder consultations. This, in our view, will allow for an appropriate evaluation of potential risks to fundamental rights and for ensuring that adequate safeguards are in place.

We trust these remarks will assist you in your work. We would welcome an opportunity to discuss the issues raised in this letter during a meeting with you or a member of your office and we are happy to elaborate on any issue raised in this letter. Please do not hesitate to contact us if you have any questions or require further information on the above or related issues.

Yours sincerely,

Pierre-Dominique Schupp
CCBE President

List of relevant CCBE positions that pertain to law enforcement access to data

- 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)
- CCBE position on the proposal for a regulation laying down rules to prevent and combat child sexual abuse (25/11/2022)
- CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (19/10/2018)
- Recommendations on the protection of fundamental rights in the context of national security (29/03/2019)
- CCBE statement on defence issues and procedural rights in EPPO proceedings (10/12/2021)

List of the selected ECtHR and CJEU judgments on the protection of lawyer-client communications

- C-694/20, Ordre van Vlaamse Balies (...) v. Vlaamse Regering, ECLI:EU:C:2022:963
- C-155/79, AM & S v. Commission, ECLI:EU:C:1982:157 (paras 16 and 18)
- Michaud v France, Application no. 12323/11: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-115377%22]
- S. v. Switzerland, Application No 12629/87, para 48: https://hudoc.echr.coe.int/eng?i=001-57709#{%22itemid%22:[%22001-57709%22]}
- Niemietz v Germany, Application No 13710/88: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57887%22]}
- Petri Sallinen and Ors v Finland, Application No 50882/99: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-70283%22]}
- Iliya Stefanov v Bulgaria, Application No 65755/01: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-86449%22]}
- ECtHR, Pruteanu v. Romania, Application No 30181/05, para 49: https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-150776%22]}
- Kopp v. Switzerland, Application No 23224/94, paras 73-74: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58144%22]}

List of selected CJEU judgments on data retention

- C-203/15, Tele2 Sverige AB, ECLI:EU:C:2016:970
- Joined cases C-793/19 and C-794/19, SpaceNet AG / Telekom Deutschland GmbH, ECLI:EU:C:2022:702
- Joined Cases C-511/18, C-512/18 and C-520/18, Quadrature du Net, ECLI:EU:C:2020:791
- C-623/17, Privacy International, ECLI:EU:C:2020:790