18-05-2021

Trilogue negotiations on the e-evidence proposal
European media and journalists, civil society groups, professional organisations and technology companies call on decision makers to protect fundamental rights

Dear European Parliament's Rapporteur and Shadow Rapporteurs,
Dear Members of the Working Party on Cooperation in Criminal Matters (COPEN),

We, the undersigned organisations, are writing to you to underline how fundamental rights protection in the E-Evidence Regulation must continue to remain a priority during the ongoing trilogues negotiations. Whereas we recognise the importance of enabling targeted access to data by law enforcement authorities for the purposes of criminal investigations, we believe stronger safeguards need to be included in the operational part of the draft Regulation.

We regret that none of the negotiating positions has fully taken into account our concerns, as outlined in our previous joint statement.[1] In particular, we believe the following issues deserve further discussion and revision from a fundamental rights and media freedom perspective:

- **Articles 7, 8a, 9, 10, 10a: Need to ensure a legal, systematic and meaningful involvement of the executing Member State**

It is our view that "direct cooperation" with private companies poses serious risks of violating human rights law by undermining key fundamental rights principles, including media freedom. In particular, when it does not require the notification and confirmation of the country where the company is located and/or where the data subject resides. Direct cooperation in a cross-border

collection of personal data risks infringing data protection laws and criminal procedure laws as well as contradicting the sovereignty of the targeted countries.

This is why **we fully support the European Data Protection Supervisor's opinion of 6 November 2019, calling for a "greater involvement of judicial authorities in the executing Member State" and the requirements that "they should be *systematically* involved as early as possible in this process**, have the possibility to review compliance of orders with the Charter and *have the obligation* to raise grounds for refusal on that basis."

The notification and validation of the executing Member State would ensure that:

- immunities and privileges designed in domestic legal systems to protect medical and legal professions, confidential communications between lawyers and clients, freedom of the media and freedom of expression are respected;
- traditional judicial cooperation principles like the non bis in idem and dual criminality principles are observed;
- legal certainty is given to individuals and service providers as both cannot be reasonably expected to know criminal law provisions of all 27 Member States;

From this perspective, we encourage the Council to take into account the Parliament's approach to these issues, which we consider an absolute prerequisite for the protection of media freedom and fundamental rights. Furthermore, the notification and active confirmation should apply to the production of all data categories and provide for strict deadlines for the executing Member State. To ensure that evidence is swiftly secured, the suspensive effect of a notification mechanism should not apply to preservation orders – thus allowing to freeze the data as soon as possible until the compliance review is over.

- **Article 10a: Protect lawyers, doctors and journalists**

The confidentiality of lawyer-client communications and special protections persons may have in their capacity as doctor or journalist should be duly taken into account when reviewing the legality of an order. Likewise, the issuing State should consider the national security interests of the affected Member State – where it is distinct from the issuing and executing States and the person's residence is known. This is especially relevant if the other Member States' rules are different or even incompatible with the rules of the investigating authorities' own domestic investigation.

Moreover, the recognition of rules related to "freedom of the press and freedom of expression in other media" should be recognised as a ground for refusal for the enforcement of an order. In addition, it should be clarified in recital 35 that all journalistic activities are covered by immunities and privileges.

- **Article 4: Ensure that orders are subject to judicial authorisation**

In *Tele2 Sverige and Watson and Others,* the Court of Justice of the European Union (CJEU) ruled that "it is essential that access of the competent national authorities to retained data should, as a general rule, be subject to a prior review carried out by a court or independent administrative body, except in cases of validly established urgency." Also, the European Court of Human Rights has repeatedly pointed out the importance of an ex-ante review by a court or another independent authority and expressed a clear preference for a judge.[2]Thus, to set the proposed Regulation in line with both the CJEU[3] and the European Court of Human Rights case law, we believe that the issuance of a production or preservation order for any type of data should require a judicial review and validation only by a court or an independent administrative authority.

- **Article 11: Inform the affected person as soon as possible that the interference occurred**

The person whose data is sought should be informed without undue delay and restriction that their personal data has been subject to an order. It is a fundamental element supporting the rights to a fair trial and to access effective remedies recognised by the jurisprudence of the CJEU that should not be restricted, even in the absence of ensuing criminal proceedings and unless otherwise decided by a court.

- **Article 7a: Ensure the authenticity, security and efficiency of data exchanges**

We recommend that the E-evidence proposal is accompanied by a secure central data exchange system between service providers and authorities in order to guarantee the security and integrity of data transfers and allow the service provider to verify the authenticity of an order. This would minimise the risk of severe data breaches of highly sensitive information, such as by exploitation of the cross-border data disclosure framework by cybercriminals who could commit identity theft (by impersonating competent authorities) or other cybercrime.[4] Considering that several Member States have already successfully implemented such a data exchange system, it is indispensable to ensure interoperability of these systems in order to avoid that service providers would have to simultaneously implement parallel data exchange systems. Otherwise, it would create substantial burdens especially for small and medium-sized enterprises and service providers would find it extremely challenging to comply with the short deadlines established in the Regulation. Where service providers already have a secure system for data transmission in place, such a system could be used instead as long as their systems enable the identification and authentication of sender and receivers and ensure data integrity.

To conclude, we call on the negotiators to build a predictable, accountable legal structure for access to personal data across borders that does not undermine existing fundamental rights protection standards.

We look forward to cooperating with you in the subsequent steps of the negotiations and remain at your disposal should you have any questions.

Sincerely,

Association for Proper Internet Governance (APIG)
Association of European Radios (AER)
Bundesverband Digitalpublisher und Zeitungsverleger e. V. (BDZV)
Committee to Protect Journalists (CPJ)
Council of Bars and Law Societies of Europe (CCBE)
Deutscher Anwaltverein
Digitale Gesellschaft e.V.
eco – Verband der Internetwirtschaft
European Broadcasting Union (EBU)
European Digital Rights (EDRi)
European Federation of Journalists (EFJ)
European Internet Services Providers Association (EuroISPA)
European Magazine Media Association (EMMA)
European Newspaper Publishers' Association (ENPA)
European Publishers Council (EPC)
IT-Pol Denmark
Internet Service Providers Austria (ISPA)
Iuridicium Remedium, z.s.

Mailfence – ContactOffice Group sa
News Media Europe
Nextcloud GmbH
Tutanota – Tutao GmbH
Statewatch
Verband Deutscher Zeitschriftenverleger (VDZ)
Wikimedia (Free Knowledge Advocacy Group EU)

1 https://edri.org/wp-content/uploads/2020/09/Joint-e-evidence-coalition-letter-14-09-2020.pdf
2 *Benedik v Slovenia* App no. 62357/14 (ECtHR 24. April 2018), *Szabo v Hungary* App no 37138/14 (ECtHR 12 January 2016)
3 In "La Quadrature du Net and Others" cases and its opinion on the EU-Canada PNR agreement, the CJEU recalls that access to any retained data, including subscriber identity and IP addresses, constitutes an interference with the fundamental right to the protection of personal data. Therefore, the CJEU requires "substantive and procedural conditions" for the access to retained data, notably that it must be subject to prior review by a court or an independent administrative body.
4 The risks of cybercriminals impersonating competent authorities in other countries are genuine, as illustrated by this recent case of a forged court order sent to a domain registrar from an email return address very similar to that of the real German court: https://www.vice.com/en/article/qj8833/dark-fail-fake-court-order-dark-web-markets