Brussels, 12 June 2023

Plenary vote on the "e-evidence package"
Regulation and Directive on "European production and preservation orders for electronic evidence in criminal matters" and "legal representatives"

Dear Members of the European Parliament,

On 13 June, you will vote on the so-called "e-evidence" Regulation and Directive which establish "European production and preservation orders for electronic evidence in criminal matters" and "legal representatives".

We, the undersigned associations of digital rights, media, journalists, internet service providers and professional associations, are recommending to vote against the adoption of the proposals.

We are gravely concerned that the proposed system of cross-border access to data in criminal matters as concluded by the trilogues of December 2022 risks to **severely undermine fundamental rights**, including press and media freedoms, the right to privacy, the right to a fair trial and the duties of professional secrecy and confidentiality. It would also fail to provide legal certainty for all stakeholders involved in the process.

Since 2018, our coalition has been providing regular input to the European Union (EU) legislature to improve the text.[1] In this regard, we would like to highlight the European Parliament's considerable work to close the many loopholes of the European Commission's dangerous legislative proposals. However, despite these attempts, **the negotiations with the Council have**

1 See the following documents:
(1) https://edri.org/wp-content/uploads/2021/10/EDRI_eEvidence.pdf;
(2) https://edri.org/wp-content/uploads/2022/05/2022-05-03-Comments-on-Councils-reply-to-EP-package-deal_COUNCIL.pdf;
(3) https://edri.org/wp-content/uploads/2021/05/20210518_EevidenceJointLetter_18May2021.pdf
(4) https://edri.org/wp-content/uploads/2020/09/Joint-e-evidence-coalition-letter-14-09-2020.pdf

seriously weakened essential safeguards in the proposed Regulation, leaving only a few that will remain almost meaningless in practice.

Equally important to stress are the **wider repercussions** this Regulation will have: **it sets a precedent for the level of protection** when law enforcement authorities across the world order access to people's personal data from private entities in the EU. It indeed serves as the baseline for the Commission in its **current negotiations with the United States** to conclude an agreement to "facilitate access to electronic evidence in criminal investigations" but also in all future negotiations with other third countries. As recently as 11 May 2023, **the European Parliament confirmed in a resolution its concerns over U.S. surveillance and the lack of appropriate safeguards for EU citizens** in the context of cross-border commercial data transfers. With the "e-evidence" Regulation as a yardstick, the future agreement risks suffering from the same shortcomings.

The following elements of the proposed Regulation are of particular concern and lead us to caution the Members of the European Parliament with the adoption of the "e-evidence" Regulation as it currently stands[2]:

- The **notification system** has been **reduced to a trickle** and **is basically toothless**, although it has been advocated for by many stakeholders as a **key solution to provide for the necessary safeguards in the procedure**, notably by ensuring the respect of the principles of legality, necessity and proportionality, accountability of the competent authorities involved and the rights of the defence. In the daily practice of law enforcement and judicial authorities, the notification mechanism will likely be the **exception rather than the rule.** As a result, the instrument **fails to fulfil its promise to bring legal certainty** to internet service providers and **risks being abused to target journalists, human rights defenders, activists, political opponents and lawyers.**

- The proposed Regulation **fails to account for national contexts with weakened rule of law** and heightened risks of political repression. The provisions addressing these issues are clearly not enough, treating them as "exceptional circumstances". This approach is at odds with the findings of the European Parliament's PEGA Committee on the **systemic abuse of state surveillance powers**.

- Likewise, regarding **professional secrecy and confidentiality,** the Regulation provides **poorly designed safeguards** that, in practice, will not prevent **illegitimate access to the communications and data of doctors, social workers and lawyers**, in breach of their legal obligations towards their patients and clients. In the majority of cases, the service providers will remain the sole defence against law enforcement overreach. Unfortunately, even their power to halt the execution of orders is limited and clearly disincentivised.

- The **right to effective remedies is limited** by insufficiently regulated "gag orders", weak rules for onward transfers and unaddressed multiple barriers for individuals who defend themselves in front of a court.

We urge the European Parliament to reconsider this proposal, as it poses serious threats to fundamental rights, fails to provide legal certainty and acts as a poor benchmark for future

2 More detailed analysis of the final text can be found here: https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

international agreements with third countries.

We remain at your disposal if you have any questions.

Sincerely,

Committee to Protect Journalists (CPJ)
Council of Bars and Law Societies of Europe (CCBE)
Digitalcourage
eco, Association of the Internet Industry
European Digital Rights (EDRi)
European Federation of Journalists (EFJ)
Homo Digitalis
IT-Pol Denmark
Mailfence.com
Standing Committee of European Doctors (CPME)
Tutanota – Tutao GmbH
Vrijschrift.org