Brussels, 22 November 2022

Political compromise on the e-evidence proposal European media and journalists, civil society groups and technology companies call on decision-makers to improve fundamental rights protections

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

We, a coalition of 24 civil society groups, associations of media and journalists and of internet service providers and professional associations, are urging you to revise the latest compromise text on the proposal for an e-Evidence Regulation. Without substantial improvements, the system of cross-border access to data in criminal matters foreseen by the political trilogue of 28 June risks to severely undermine fundamental rights, including press and media freedom, the rights of the defence, the right to privacy and medical patients' rights. It would also fail to provide legal certainty for all stakeholders involved in the process.

We regret that most of our previous recommendations were not taken into account, in particular:

- **Article 7a(2) – Notification and residence criterion**

The residence criterion introduced as an exemption from notification of the enforcing State is a major loophole in the rights protection framework of the e-Evidence Regulation. The assessment of where the person whose data is sought lives will be at the sole discretion of the issuing State which can have clear incentives to avoid the notification. The threshold is also too low and can be easily abused, as "reasonable grounds to believe" does not necessarily mean that the issuing State needs objective evidence or concrete indications. The issuing authority is not even required to justify its beliefs in the order, effectively preventing scrutiny of its assessment. **How will the Regulation ensure that the standards to carry out this assessment are harmonised, thus guaranteeing an equal level of protection to affected individuals?**

In case the issuing State makes a false assumption and fails to notify the enforcing State, it is unclear how the mistake can be reported and rectified: Article 9 does not provide the possibility for the service provider to raise this issue. The enforcing State cannot deny the enforcement of the order for this reason under Article 14(4) and the individual cannot necessarily exercise their right to effective remedies if the information is restricted or if this is not foreseen under the issuing State's national law (Article 17(1)).

The residence criterion will also weaken the possibility to raise the grounds for refusal foreseen in Article 7b(1)(c) and recital 11a when there is a risk of manifest breaches of fundamental rights in the issuing State, such as in Member States with systemic rule-of-law issues. Given that the risks entailed by this exemption that would apply to orders requesting very sensitive types of data (traffic and content) and that could possibly lead to serious fundamental rights violations, **it is essential that the residence criterion is not part of the final compromise text.**

- **Article 7a – Notification for subscriber and traffic data**

Besides the need for mandatory notification for content data and traffic data, the notification of the enforcing State should be mandatory when subscriber data and traffic data sought for the sole purpose of identifying the person are requested. Even though subscriber data overall is less sensitive than traffic data, there are notable exceptions, especially when privileges and immunities are involved (identity of a journalistic source, a whistleblower, etc.). In its draft Council Decision for authorising Member States to sign and ratify the Second Additional Protocol to the Cybercrime Convention, the European Commission clearly states that mandatory notification for access to subscriber data is necessary to ensure compatibility with Union law.

- **Article 4(1)(b) – Procedural involvement of a court for subscriber data**

We support the proposal from the Rapporteur that where execution of an EPOC for subscriber data (and traffic for the sole purpose of identifying the user) requires the procedural involvement of a court in a Member State, it should be possible to require the order to be issued by a court in the issuing State as well. **The provision should be strengthened** by deleting the requirement of a declaration from the concerned Member State(s), so that the provision applies solely by virtue of national law requiring procedural involvement of a court.

- **Article 9(2) and (3) – Execution of an EPOC and suspensive effects**

Notification of the authority in the enforcing state is a key safeguard to allow raising any grounds for refusal and provide legal certainty to the service provider before disclosing the requested user data. At the very least, a notification should thus always have a suspensive effect on the disclosure obligation of the service provider in all cases, including emergency requests. Under the current proposal, where a notification has taken place, the addressee must produce the data at the end of the 10-days or 8-hour time period, even in the absence of a validation by the enforcing authority. The risks are too great that the enforcing authority does not carry out a genuine review of the orders and simply let the waiting period lapse. This does not only undermine the efficiency of this critical safeguard but is also inefficient as with an active validation requirement, orders could be executed sooner where the validation has been given by the enforcing authority before the end of the deadline. **The suspensive effects of production orders should apply for all types of orders (urgent or not) until the enforcing authority proactively gives its green light.**

- **Article 12b – Speciality principle and purpose limitation**

The rules to re-use data obtained via an e-Evidence order in other proceedings or to transmit it to another Member State are too weak. The notification system enables a case-specific assessment of production orders that takes into account the specific circumstances of each investigation. Allowing the issuing authority to determine on its own whether data can be re-used in different proceedings is possibly undermining the notified State's assessment of the order. Even if the conditions for issuing a production order could be met , the exception to the purpose limitation principle should be limited to extraordinary circumstances where there is an imminent risk to the life or physical integrity of a person. It should not be possible to transfer the obtained data to another Member State as the reasons for raising a refusal ground may differ from one requesting Member State to another (e.g. manifest breach of fundamental rights).

In addition, we have identified several loopholes that need to be urgently addressed or clarified to ensure legal certainty:

- **Article 7b - Grounds for non-recognition or non-execution**

What are the consequences for individual effective remedies in case the enforcing authority has an obligation to raise grounds for refusal ("shall")? May the affected data subject complain against the enforcing authority if the latter failed to raise grounds for refusal?

Leaving the option to the enforcing authority whether to refuse an order or not ("may") would be extremely detrimental for the protection of fundamental rights, in cases where an order is manifestly abusive or where it violates press and media freedom, professional privileges or the principles of *ne bis in idem* or double criminality.

- **Article 5(5)(g) - Conditions for issuing a European Production Order in emergency**

The difference between an emergency order and a request for earlier disclosure is very unclear. Earlier disclosure would put in jeopardy the effectiveness of the notification process and the

grounds for refusal. **The risk of illegal disclosure of data should be avoided and therefore earlier disclosure should be deleted from the text.**

- **Article 5(6c) - Conditions for issuing a European Production Order and immunities and privileges**

The draft agreement introduces a set of conditions for the request of traffic and content data protected by professional privilege (doctor holding sensitive patient data, lawyer storing their client files, etc.) but it is unclear to which situations the specific condition "in cases where the data is stored or processed by a service provider *as part of an infrastructure*" applies and which services are excluded from the scope of this paragraph. To effectively protect immunities and privileges, we believe the paragraph should apply to all types of services offered to protected professions and that the three conditions listed should be cumulative and not alternative ("and" instead of "or").

- **Article 9(2b) – Execution of an EPOC and immunities and privileges**

Why should the possibility for the addressee to refuse to execute an order violating immunities or privileges or press and media freedom be "based solely on the information contained in the EPOC" and not also on information the addressee holds on the concerned individual?

We are looking forward to receiving your thoughts on the points we raise above and remain at your disposal should you wish to discuss this further.

Yours faithfully,

Bundesverband Digitalpublisher und Zeitungsverleger e.V. (BDZV)
Chaos Computer Club (CCC)
Committee to Protect Journalists (CPJ)
Digitalcourage
Digitale Gesellschaft e.V.
Državljan D / Citizen D
IT-Pol Denmark
eco, Association of the Internet Industry
EuroISPA
European Broadcasting Union (EBU)
European Digital Rights (EDRi)
European Federation of Journalists (EFJ)
European Magazine Media Association (EMMA)
European Newspaper Publishers' Association (ENPA)
Fair Trials
European Hospital and Healthcare Federation (HOPE)
Mailfence.com
Medienverband der freien Presse e.V. (MVFP)
Standing Committee of European Doctors (CPME)
News Media Europe
Tutanota – Tutao GmbH
Uni Global Union
Wikimedia Deutschland e. V.
Wikimedia France