4 May 2022

Dear Member of the European Parliament,

The undersigned organisations would like to raise your attention about the ongoing trilogue negotiations on the "e-evidence package" (Regulation and Directive). The e-evidence proposals have been subject to intense debates with all stakeholders as well as lengthy and difficult negotiations between legislators.

Following the impasse in the trilogue negotiations, the Rapporteur, Ms Sippel, presented a few months ago a compromise package to the Council in an attempt to pave the way towards an agreement. While we welcomed the rapporteur's efforts to find a balanced compromise guaranteeing fundamental rights, we expressed reservations regarding some proposals of the package, notably on the notification procedure for subscriber data and other identifiers.

Having seen the Council's reaction to the European Parliament's compromise proposals of 17 March 2022, we regret to note that the Council Presidency and Member States are far from making the same efforts as the Rapporteur to work jointly towards a balanced compromise. We are therefore all the more concerned about the continuation of the negotiations.

The Council refuses to make any useful concessions on key issues such as the notification procedure, the residence criterion, grounds for refusal or legal remedies. **You will find below comments elaborated by a coalition of professional associations, media and journalists' organisations and civil society groups.**

Thus, we urge the European Parliament to maintain its original approach and not to cede to pressure from the Council. The rapporteur has already yielded on some key points of the report. More concessions would lead to disproportionate impact on the work of journalists, the protection of sensitive health data, the freedom to protest and the right to a fair trial (see our compendium of scenarios) and would confront the providers with various legal uncertainties. The protection of fundamental rights should not take a backseat to efficiency in cross-border investigations.

We thank you for taking into consideration our attached comments.

Sincerely,

- ARTICLE 19: Global Campaign for Free Expression
- Deutscher Anwaltverein
- Digital Rights Ireland
- Digitale Gesellschaft (Germany)
- EBU – European Broadcasting Union
- eco
- EDRi
- EFJ – European Federation of Journalists
- EuroISPA
- EMMA
- ENPA
- Fair Trials
- Homo Digitalis
- IT-Pol Denmark
- News Media Europe
- Tutanota
- UNI Global Union

*****

Comments on the Council's reaction to the European Parliament's proposals for compromise

In December 2021, the European Parliament's rapporteur, Birgit Sippel (S&D), proposed to the Council a compromise package on the proposed Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. The Council responded in a letter dated 17 March 2022 (7106/22).

Below are detailed comments on the 5 main lines of the Council's response to the Parliament package (notification, scope, individual rights, enforcement and handling of evidence gathered). These comments were prepared by a coalition of professional associations, media and journalists' organisations and civil society groups.

A balanced notification:

- **The Council fails to make one step in the direction of the Parliament's position on the issue of mandatory notification.** The "residence criterion" is unacceptable as it would severely limit the rights safeguards offered by the notification regime and therefore must be abandoned by Council members. The assessment of where the person concerned lives is made by the issuing State which may have clear incentives to avoid the notification mechanism. There is a risk of abuse, especially since this assessment is not regulated by clearly defined criteria in the Regulation. For example, whereas for cyber-assisted crimes the issuing authority could sometimes determine the residence of a suspect based on other evidence, it would often have to rely on information provided by the service provider for cyber-enabled and cyber-depended crimes, which itself already constitutes sensitive traffic data. From a technical perspective it is not always possible to locate a user in a certain country, for example, because of the use of VPNs or signals from a user moving between countries. Mandatory notification is critical for protecting fundamental rights of individuals, including those residing in Member States with rule-of-law issues. It provides legal certainty for service providers which will follow the decision of the authorities in their Member State, in accordance with domestic law.
- **The Council doggedly sticks to its original position on the list of grounds for refusal.** However, we imperatively need a substantive list of grounds for refusal similar to Article 11 of the EIO Directive to respect important principles such as ne bis in idem, double criminality as well as the respect of higher protections granted by national constitutions in the executing State. Limiting the list of grounds for refusal would risk depriving the notification regime of its purpose.
- **We call on both legislators to require a mandatory notification of the executing State when subscriber data is requested.** Even though subscriber data overall is less sensitive than traffic data, there are notable exceptions, especially when privileges and immunities are involved. 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.

The precise definition of the scope of the instruments:

- Not all data transferred under the e-evidence Regulation will be used as evidence in courts: from this perspective, it is more accurate to talk about "electronic information".
- On the nature of the issuing authorities depending on data categories, we recall that **production orders for any data category should be reviewed by a court or an independent administrative authority prior to their issuance**, in line with the CJEU case law (especially for IP addresses, and even in cases where such data and other access numbers are solely sought to identify a person).

Guarantees for individual rights:

- **We welcome the Council's decision to accept the notification to the affected person by the issuing authority as the rule by default.** However, this requirement could very easily be bypassed by authorities if exceptions are too widely applied (e.g. they could pretend it jeopardises the investigation). Proper justification needs to be given, otherwise individual rights such as the right to a fair trial could be impaired and threatened. Any gag order should be validated by a court or an independent administrative authority on a case-by-case basis. Competent authorities need to provide duly motivated confidentiality restrictions on the disclosure of an order to the individual concerned as soon as possible.
- **The Council must show more flexibility on legal remedies.** They should be available to affected persons outside of criminal proceedings and include the right to contest the executing State's decision to validate or reject an order and/or its failure to fulfil its obligations under the Regulation.
- Under the case law of the CJEU, limitations on the exercise of fundamental rights must be provided for by law and impose minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. The Council's preference of **relying on safeguards in Member States' national law will not generally be sufficient in light of the CJEU's requirement that minimum safeguards must be established in EU law.**

Effective enforcement procedures:

- We would like to stress that **an 8-hour deadline to comply with an order in emergency cases is not realistic for many small providers in the EU**, as they do not have the resources to operate a legal service on a 24/7 basis. We invite the co-legislators to consider applying the same extenuating circumstances as in Article 3 (7) of Regulation 2021/784. We recall that an ex-post judicial validation should be sought by the competent authorities, notably by exposing the reasonable grounds for emergency and the executing State should allocated sufficient resources to review and process emergency orders.
- Given the 24 months-period set by the Council in its general approach to implement the Regulation, **there should be sufficient time for the European Commission to build and run a common European exchange system before the application of the Regulation.**
- **The Council needs to make a step towards the Parliament on the issue of reimbursement of costs.** We see the harmonisation of costs reimbursement at EU level as an effective

accountability mechanism to ensure orders are issued with moderation and proportionality.

- **We call on the Council to consider the preservation of EU's good international relations when addressing the issue of conflicts of laws.** The EU should not let Member States' authorities resolve conflict of law situations unilaterally. The involvement of competent authorities in third countries should be provided for. We recall that GDPR Article 48 ensures that controllers in the EU cannot disclose personal data directly to law enforcement authorities in third countries without an international agreement with the EU, such as a mutual legal assistance treaty. The same principles should be reflected in EU legislation covering service providers in third countries, especially when the legislation in question could affect persons residing in those countries and possibly deprive them of protections in their domestic legal framework.

Compliant processing of the evidence gathered:

- **The Council is not making any effort on the issue of data retention limits.** Preservation orders should contain fixed limits to ensure they respect the necessity and proportionality principles.

*****