EP and Council Reach Consensus on E-evidence Dossier

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2022, Vol. 17(2) eucrim p 124
ISSN: 1862-6947
https://eucrim.eu

On 28 June 2022, negotiators of the European Parliament (EP) and the Council reached a political agreement on the core elements of the Commission proposals on e-evidence (→ eucrim 1/2018, 35-36). As reported in previous eucrim issues, negotiations have been extremely controversial and cumbersome since positions between the EP and the Member States in the Council on finding the right balance between security and fundamental rights protection considerably differed. The major aim of the future EU legislation on e-evidence is to allow national authorities to request evidence directly from service providers in other Member States, or ask that data be preserved for future use. This will mean a major paradigm shift to the existing rules on judicial cooperation in criminal matters. The new rules would also mandate companies to appoint EU legal representatives to deal with electronic evidence requests in a centralised way.

The EP negotiators now announced that they were able to push through major safeguards for fundamental rights and data protection, including:

- If traffic and content data are sought from a service provider, the Member State where the service provider is located must be notified, except for situations where the suspect of the crime has its permanent residence in the issuing State and the crime was or is likely to have been committed exclusively in the issuing State;
- The notified authority may reject the order within ten days or, in emergency cases, within eight hours on the basis of a list of reasons. During this time, the service provider shall back up the data;
- The double criminality requirement is a refusal ground, i.e. if the crime under investigation is not a crime in the service provider's country, carrying out the request is to be denied;
- The violation of fundamental rights enshrined in the Charter and the EU Treaties would also constitute a refusal ground;
- Special provisions ensure that a refusal on the basis of an assumed violation of fundamental rights can be made if requests are issued by authorities of an EU Member State which is under an ongoing rule-of-law procedure pursuant to Art. 7 TEU (such as Poland and Hungary at the moment);
- Service providers may bring surrender orders not only to the attention of the issuing authority, but also to the authorities of the country in which they are located, for example if they restrict media freedom;
- The provisional provisions are better aligned to existing EU data protection rules; for example, orders have to be sent to data controllers, in principle, and can only be addressed to data processors under certain conditions.

The EP and the Council also found compromises on the reimbursement of costs and sanctions that could be imposed to the service providers in case of non-compliance. Lastly, they agreed that orders are sent through

a specific, secure IT system so that genuineness of the orders and confidentiality of data transmissions to investigating authorities are ensured.

The political agreement will now be further debated at the technical level. Moreover, the EP and Council have to agree on other outstanding aspects of the legislative dossier. It is expected that the final compromise can be submitted to the EP and Council for adoption later this year.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).


Co-funded by
the European Union