European Commission

SECURITY UNION

FACILITATING ACCESS TO ELECTRONIC EVIDENCE

April 2018

The European Commission has proposed legislation to facilitate and accelerate law enforcement and judicial authorities' access to electronic evidence to better fight crime and terrorism. This will give authorities the right tools to investigate and prosecute crimes in the digital age.

WHAT IS ELECTRONIC EVIDENCE?

Electronic evidence is data stored in electronic form – such as IP addresses, e-mails, photographs, or user names – that is relevant in criminal proceedings. Often, this data is stored by service providers, and law enforcement and judicial authorities have to turn to them to obtain it.

WHAT ARE THE PROBLEMS ADDRESSED TODAY?

Today, much of the useful information needed for criminal investigations and prosecutions is stored in the cloud, on a server in another country and/or held by service providers that are located in other countries. Even where all other elements of a case are located in the investigating country, the location of the data or of the service provider can create a cross-border situation.

To obtain such electronic evidence stored abroad and/or by a service provider located in another country, EU national authorities rely on either traditional existing judicial cooperation tools or voluntary cooperation with service providers. For requests within the EU, judicial authorities normally use the **European Investigation Order** to obtain evidence. **Mutual Legal Assistance agreements (MLA)** are used by EU Member States' authorities to obtain evidence from outside the EU. While these procedures work well for traditional investigative measures, they are often too slow for obtaining electronic evidence which can be transferred or deleted at the click of a mouse. As a result, **voluntary cooperation** between law enforcement and service providers based in the United States has developed as an alternative way of obtaining non-content data. This form of cooperation is generally faster than judicial cooperation, but it lacks reliability, transparency, accountability and legal certainty.

THREE MAIN PROBLEMS:

Inefficient public-private cooperation
Inefficiencies in cooperation between service providers and public authorities hamper effective investigations and prosecutions.

Slow procedures
It takes too long to access electronic evidence across borders under existing judicial cooperation procedures, rendering investigations and prosecutions less effective.

No legal certainty
Limitations in how authorities can use investigative measures in cross-border situations can hinder effective investigations and prosecutions. Also, there is no clear framework for cooperation with service providers who voluntarily accept direct requests for non-content data as permitted by their domestic law.

WHAT WILL THE NEW PROPOSALS BRING?

Speed for fighting crime

Law enforcement and judicial authorities will be able to get hold of electronic evidence e.g. photographs and messages much more **easily** and **rapidly**.

The new proposal will require service providers to respond within **10 days**, and **up to 6 hours for emergencies**. This will allow authorities to **investigate crimes and terrorism** more quickly and efficiently.

Harmonised, clear rules for service providers

The new rules are binding for service providers and will bring clarity and legal certainty to both service providers and law enforcement authorities. **They will provide a clear** procedure in case of **conflicting obligations** with the law of a non-EU country.

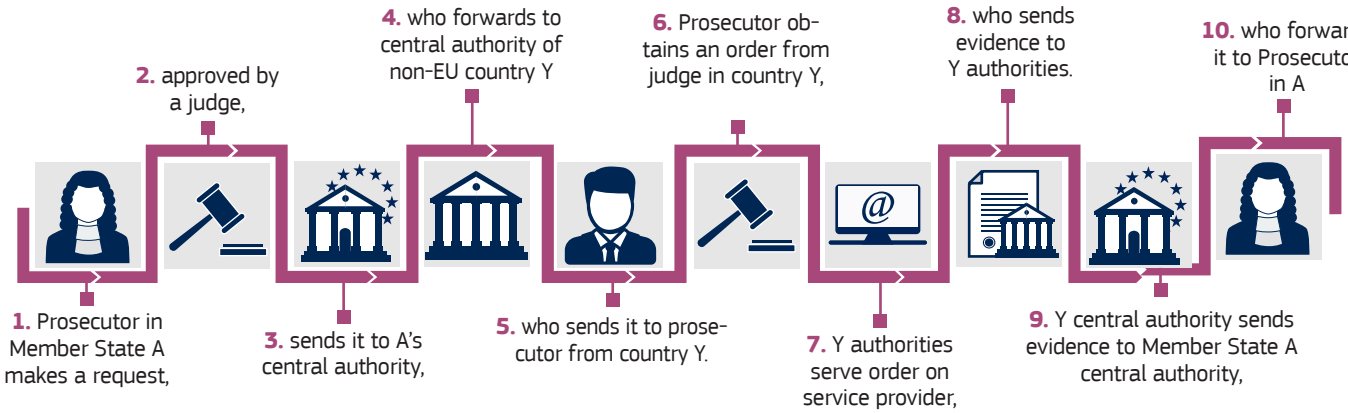
Respect of Fundamental rights

The new rules also introduce conditions and safeguards that aim to ensure **fundamental rights are fully protected**, including safeguards for the right to personal data protection, ensuring effective remedies and safeguards for the subjects of requests.

EXAMPLES OF HOW IT WORKS NOW

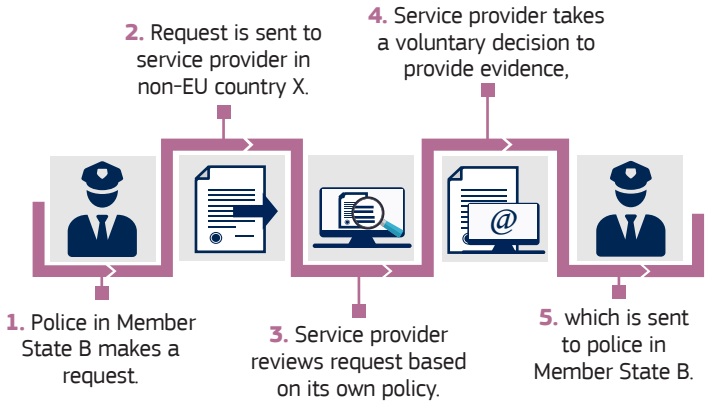
On Terrorism

After a terrorist attack in Member State A, the police connects the suspect to a terrorist cell that has been involved in other attacks in other Member States. The police has indications that the terrorist cell communicates through e-mail messages using a cloud-based e-mail service. The police would like to obtain transactional data regarding e-mails sent by the suspect to identify other members of the terrorist cell.



As the service provider hosting the cloud-based e-mail service is based in the Third Country Y, Member State A authorities have to send a Mutual Legal Assistance (MLA) request to the Third Country Y authorities who assess the request and transform it into a domestic order to obtain the transactional data from the service provider. Subsequently, the Third Country Y authorities transmit the data to the Member State A authorities. As MLA procedures can take several months to be completed, the investigation may be delayed significantly. New leads that emerge from the data obtained are often no longer useful.

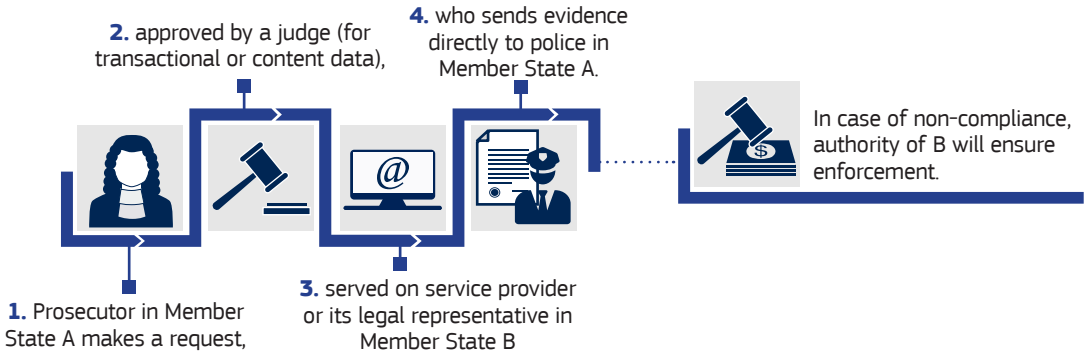
On Child Sexual Abuse



Having infiltrated an online forum for exchanging child sexual abuse material on the Darknet for over a year, the Third Country Z police gathers information on more than one million users globally, which they then share with law enforcement authorities around the world. Some of the child victims and suspects appear to be in Member State B, which receives information from Z authorities. The information and subsequent investigation in B lead to the discovery of the suspect's social media profile. B authorities need information about who is behind the profile to allow for identification. The social media company is based in the Third Country X, whose legislation allows B police to request the company to disclose subscriber information voluntarily.

The above process is dependent on the goodwill of the service provider. There are no standardised procedures across service providers, and the process can be non-transparent and unreliable.

HOW IT WILL WORK WITH THE PROPOSED RULES



This procedure also applies if the electronic evidence is stored in a non-EU country.

Safeguards:

- must be approved by judicial authority
- for transactional and content data, the European Production Order is limited to serious crimes
- individuals will be notified that their data was requested
- individuals will be notified of their rights
- criminal law procedural rights apply

HOW WILL THE ELECTRONIC EVIDENCE RULES WORK IN PRACTICE?

The proposed new rules would **provide a faster tool** for obtaining electronic evidence.
The European Investigation Order (EIO) and the Mutual Legal Assistance (MLA) will continue to exist, but there would be a fast track alternative for the specific case of electronic evidence: **the European Production Order**.

Under current procedures, the judicial authorities in both countries are involved. The new EU rules will allow the judicial authority to go **directly** to the legal representative of the service provider in another EU country. Also, the evidence will no longer travel back through many hands, but go directly from the legal representative to the authority requesting the data. The authorities of the host country will only be involved in cases where there are specific legal concerns or where the Order needs to be enforced.
The proposed new rules also include a **European Preservation Order** which may be issued to avoid deletion of electronic evidence.