Frequently Asked Questions: New EU rules to obtain electronic evidence

Brussels, 17 April 2018

The Commission is proposing new rules to make it easier and faster for police and judicial authorities to obtain the electronic evidence, such as e-mails or documents located on the cloud, they need to investigate, prosecute and convict criminals and terrorists.

E-evidence

What is electronic evidence?

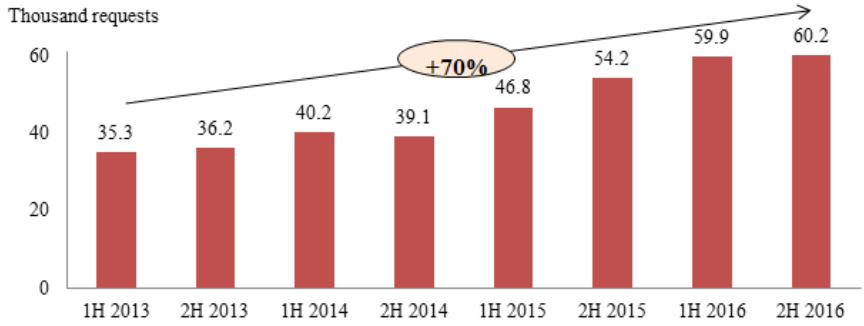
Electronic evidence refers to various types of data in electronic form that are relevant in investigating and prosecuting criminal offences — including 'content data' such as e-mails, text messages, photographs and videos – often stored on the servers of online service providers, as well as other categories of data, such as subscriber data or traffic information regarding an online account. These types of data are often essential in criminal investigations to identify a person or to obtain information about their activities.

Why improve the access to electronic evidence?

In the off-line world, authorities can request and obtain documents necessary to investigate a crime within their own country, but electronic evidence is stored online by service providers often based in a different country than the investigator. Some data may even be stored in multiple locations.

More than half of all investigations today involve a cross-border request to access electronic evidence. Electronic evidence is needed in around 85% of criminal investigations, and in two-thirds of these investigations there is a need to request evidence from online service providers based in another jurisdiction. The number of requests to the main online service providers grew by 70% in the period between 2013 and 2016 (see graph).

Evolution of number of Member States' requests to the main service providers *(based on transparency reports of Facebook, Google, Microsoft, Twitter and Apple)*



The current procedures for cooperation between judicial authorities to obtain e-evidence in cross-border situations are too slow compared to the speed at which electronic data can be changed or deleted. In addition, judicial authorities are struggling to cope with the growing number of cases involving a cross-border request to electronic evidence. These long procedures make it difficult for authorities to conclude their investigations and punish criminals or terrorists. As a result, victims feel less protected and citizens feel less safe.

What will the new rules change?

The proposed Regulation on **European Preservation Order** and on **European Production Order** introduces new rules to help authorities secure and obtain electronic evidence stored by service providers, irrespective of where the evidence is stored. The rules will build on existing principles of mutual recognition between Member States.

The European Production Order will allow a judicial authority in one Member State to request access to electronic evidence (such as emails, text or messages in apps) directly from a service provider's legal representative in another Member State, which will be obliged to respond within **10 days**, and within **6 hours** in cases of emergency (as compared to 120 days for the existing European Investigation Order or 10 months for a Mutual Legal Assistance procedure).

The **European Preservation Order** will allow judicial authorities in one Member State to oblige a service provider or its legal representative in another EU country to prevent electronic evidence from being deleted before their production request is completed.

The orders will apply only to stored data. Real-time interception of telecommunications is not covered by this proposal.

The proposed Directive on Legal Representatives will oblige service providers to designate a legal representative in the Unionto ensure that all providers that offer services in the European Union are subject to the same obligations, even if their headquarters are in a third country. The legal representative in the Union is responsible for the receipt of and compliance with of decisions and orders.

What types of data are covered by the proposal?

The categories of data that can be obtained with a European Production Order include subscriber data, access data, transactional data (the three categories commonly referred to jointly as 'non-content data') and content data.

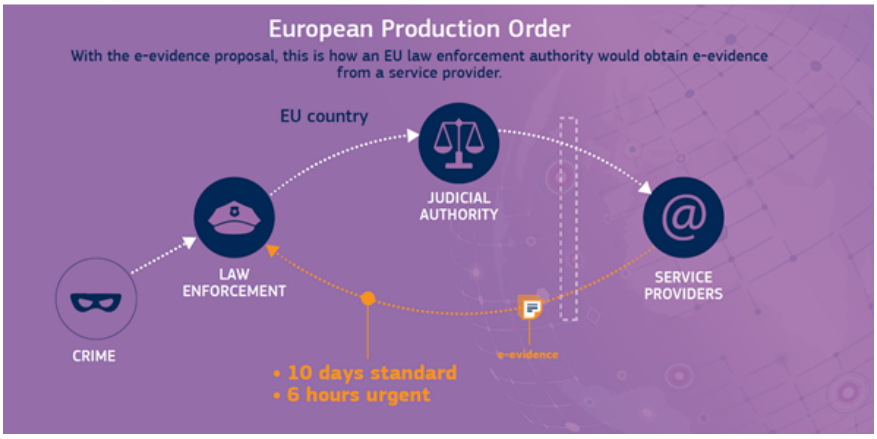
Type of data	Definition	Access rules
Subscriber data	Elements that serve to identify a subscriber or customer such as the name, date of birth, postal address, billing and payment data, telephone number, or email address.	Prosecutor/judge in country A can directly ask the service provider or its legal representative in country B to provide the electronic evidence. If request comes from police, they have to ask a prosecutor or judge in country A to approve the order before transmitting it to the service provider or its legal representative.
Access data	Data elements which in and of themselves cannot identify the user but are strictly necessary as a first step towards identification. This includes data on a user's access to a service, such as the date and time of use or the log-in to and log-off from the service or the IP address allocated by the service provider.	Prosecutor/judge in country A can directly ask the service provider or its legal representative in country B to provide the electronic evidence. If request comes from police, they have to ask a prosecutor or judge in country A to approve the order before transmitting it to the service provider or its legal representative.
Transactional data	Relates to the provision of a service, such as the source and destination of a message, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression.	Judge in country A can directly ask the service provider or its legal representative in country B to provide the electronic evidence. If request comes from police or prosecutor, they have to ask a judge in country A to approve the order before transmitting it to the service provider or its legal representative
Content data	Any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data.	Judge in country A can directly ask the service provider or its legal representative in country B to provide the electronic

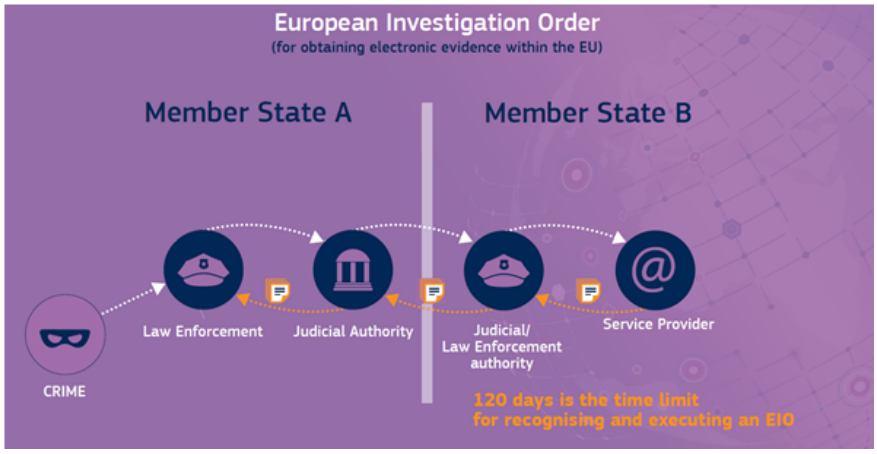
		evidence. If request comes from police or prosecutor, they have to ask a judge in country A to approve the order before transmitting it to the service provider or its legal representative

What are the current procedures to access e-evidence in cross-border situations?

Currently, law enforcement and judicial authorities cooperate to obtain electronic evidence by using mutual legal assistance procedures outside the European Union or the European Investigation Order inside the European Union. However, these judicial cooperation tools are often too slow and cumbersome for obtaining electronic evidence, which can be transferred or deleted at the click of a mouse.

Voluntary cooperation between law enforcement and service providers based in the United States has developed as an alternative way of obtaining electronic evidence. This form of cooperation is generally faster than judicial cooperation, but service providers have different ways of handling requests for disclosing electronic evidence, and the process lacks transparency, accountability and legal certainty.





What safeguards will be put in place to protect fundamental rights and freedoms?

The proposal contains strong safeguards to guarantee privacy, data protection and the right to judicial redress.

Issuing of European Production or Preservation Orders will only be possible in the context of criminal proceedings. All existing criminal law procedural rights will apply, including relevant legislation at EU level such as the right of access to a lawyer and the right of access to the case file. The proposal establishes an obligation for authorities to obtain approval of all orders from a judicial authority, to ensure that their legality, necessity and proportionality have been checked.

Production orders to produce transactional (source and destination of a message, data on the location of the device) or content data (text, voice, videos or images) may only be issued for criminal offences punishable in the issuing State by a maximum sentence of at least three years, or for specific cybercrimes and terrorism-related crimes defined in the proposal.

Personal data covered by this proposal is protected and may only be processed in accordance with the General Data Protection Regulation and the Police Directive, both of which enter into application as of May 2018.

Will it be mandatory for service providers to produce electronic evidence?

Yes, the European Preservation Order and the European Production Order are legally binding.

This will improve legal certainty compared to the existing voluntary cooperation, which creates challenges for service providers seeking to comply with law enforcement requests. It will also give law enforcement and judicial authorities more certainty to obtain the e-evidence they need.

The proposal allows service providers to seek clarifications from issuing authorities where necessary and to oppose the execution of orders in certain situations. In addition, a specific procedure has been put in place for situations where the obligation to produce data conflicts with a competing obligation arising from a third-country law. Service providers can raise an objection based on such conflicting obligations, triggering a judicial review.

Where the law of the third country protects fundamental rights or fundamental interests of the third country, the judge should normally lift the Order after consultation of the third country's authorities. Where the law of the third country protects other interests, the judge will have to balance the interests at stake. In both situations, the data should be preserved by the service provider.

What is the proposal on legal representatives about?

Currently, there are different approaches across Member States regarding obligations imposed on service providers, especially in criminal proceedings and for service providers which do not have an establishment in the Union. This fragmentation creates legal uncertainty for those involved and can place service providers under different — sometimes conflicting — obligations.

The proposal obliges service providers to designate legal representatives in the EU ti facilitate the receipt of , compliance with enforcement orders to gather electronic evidence on behalf of these service providers.

This will remove the need for individualised national approaches and provides legal certainty at EU level. In addition, a uniform approach creates a level playing field for all companies offering the same type of services in the EU, regardless of where they are established. Moreover, it does not affect companies' freedom to store the data where they choose to.

Which service providers will be covered by the proposals?

The legislative proposals include obligations for providers of services that are used for communication purposes (including providers of telecommunications services and other electronic communications services, including interpersonal communications services). In addition, the proposals will also apply to providers of information society services that facilitate interactions between users and that are used for the storage of data (including online marketplaces that facilitate peer-to-peer transactions and providers of cloud computing services) and for providers of internet infrastructure services (including registries that assign domain names and IP addresses important for the functioning of the internet).

The Commission proposal would apply to these providers when they are offering services in the European Union. According to the proposals, a provider is offering services in the European Union when he enables users in one or more Member States to use its services and where he has a substantial connection to the Union, for instance when it has an establishment in a Member State or because he provides services to a large number of users in that Member State.

What will happen if the data is stored in a non-EU country?

There is a difference between where the data is stored and where the service provider is based. The service provider might be based in a third country, but the data might be stored in the EU, even in the

country of the investigating State. Still, under the current system the judicial authorities have to address a request via mutual legal assistance to the service provider in the third country. This would change under the proposal.

The Regulation departs from data storage as the determining factor for jurisdiction, and rather requires that the requested data is (1) needed for a criminal proceeding for which the issuing authority is competent and (2) related to services of a provider offering services in the Union. If this is the case, the data must be preserved and produced, irrespective of the place of data storage

In case a service provider is confronted with conflicting obligations deriving from the law of a non-EU country when evidence is requested, the proposal foresees a review procedure to clarify such a situation. Ultimately the decision whether to uphold the request will be up to the competent national court.

A service provider who stores data relating to its European users outside of the EU, e.g. in the US, will thus have to provide data to European authorities if addressed with a European Production Order, unless there is a conflict with a third-country law.

For More Information

Press release

Factsheet

MEMO/18/3345

Press contacts:

Christian WIGAND (+32 2 296 22 53)
Natasha BERTAUD (+32 2 296 74 56)
Tove ERNST (+32 2 298 67 64)
Melanie VOIN (+ 32 2 295 86 59)
Kasia KOLANKO (+ 32 2 296 34 44)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

Attachments

Factsheet E-evidence.pdf