WT Client Alert

E-Evidence Regulation on the verge of becoming a reality

New rules will facilitate cross-border access to stored data in criminal proceedings

15 June 2023

Securing e-evidence and establishing efficient procedures is key

The E-Evidence Regulation (Council document 5448/23) will enable relevant authorities to address judicial orders for electronic evidence directly to service providers in other member states. Those who fail to respond to these orders within 10 days, or even within 8 hours in urgent cases, will face fines of up to 2% of the service provider's global turnover.

Summary of key points:

- The aim of the envisaged E-Evidence Regulation, which will be directly applicable in EU member states, is to preserve e-evidence and establish a quick and easy procedure for sharing said evidence among member states.
- Law enforcement will be able to access data directly from service providers offering their services in the EU, regardless of where the data is stored.
- Service providers must respond within 10 days and within 8 hours in emergency cases, or risk financial penalties.

Easier access to e-evidence for law enforcement

In recent years, life has increasingly moved into the digital space and crime is no exception. Law enforcement has become more and more dependent on electronic evidence ('e-evidence') to investigate and prosecute criminal offences. However, getting access to e-evidence can be a lengthy and complicated process for authorities as online service providers often store data on servers located in several countries, both in and outside the EU. Thus, the E-Evidence Regulation aims to facilitate access to e-evidence from a service provider, (e.g. online platform or mobile phone provider), that offers its services within the EU and established or represented in another member state.

The regulation on production and preservation orders for e-evidence will enable authorities to access stored data, no matter where it is located

The E-Evidence Regulation introduces an alternative mechanism to existing international cooperation and mutual legal assistance tools. The goal is to preserve important evidence and make the cooperation process more efficient overall. The Regulation creates two instruments, the European Production Order and the European Preservation Order. The Preservation Order will prevent e-evidence from being deleted by a service provider while the Production Order is still being processed.

National law enforcement authorities can issue these orders to obtain or preserve e-evidence regardless of the location of the data. E-evidence is a very broad term and covers any category of digital data, including subscriber data, content data (text, voice, videos, images or sound), and traffic data (e.g. source and destination of a message or the location of a device). While subscriber data and data needed to identify a perpetrator can be requested for any criminal offence, the disclosure of other traffic data and content data requires that the offences in question be of a certain severity. These data can only be requested for crimes punishable in the issuing country by a maximum custodial sentence of at least three years, or for specific offences relating to cybercrime, child pornography, counterfeiting of non-cash means of payment or terrorism.

The competent authorities will be able to address the orders directly to any service provider offering their services in the EU. Those providers that do not have a registered office in the EU must appoint a legal representative pursuant to the Directive on legal representatives, which is still pending publication (see below). The designated establishment and legal representative at issue should serve as an addressee for decisions and orders for the purpose of gathering electronic evidence. Where the data is located does not matter. However, the authorities will only be able to obtain stored data. Real-time interception of telecommunications is not covered by the proposed new rules.

Service providers must respond within 10 days or even 8 hours in emergency cases

The E-Evidence Regulation provides that the service providers concerned must respond within a mandatory deadline of 10 days from receipt of the request for electronic evidence, in emergency cases, the mandatory response timeframe is reduced to within 8 hours. Emergency cases are defined as situations where there is an imminent threat to life, physical integrity or the safety of a person or to critical infrastructure that would result in a threat to people's lives, physical integrity or safety. These tight deadlines are meant to significantly speed up investigation procedures.

According to the proposed wording, service providers shall have the right to inform the issuing authority if an order is incomplete, contains manifest errors, does not contain sufficient information for its proper execution, or if the service provider cannot comply with its obligations due to de facto impossibility.

> For service providers, the E-Evidence Regulation entails new challenges and compliance risks.

However, refusal to comply is a major risk for service providers. The E-Evidence Regulation provides for pecuniary sanctions applicable to infringements of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year.

Directive on legal representatives to supplement new rules

In addition to the E-Evidence-Regulation, the Directive on legal representatives (Council document 5449/23) lays down harmonised rules on the appointment of legal representatives for the purposes of gathering evidence in criminal proceedings. The Directive will compel all service providers not established, but offering services in the EU, to appoint a legal representative. There is currently no legal requirement for non-EU service providers to be physically present in the EU.

The representative can be a natural or legal person and will be responsible for receiving, complying with and enforcing decisions and orders. Service providers shall provide them with the necessary powers and resources to comply with decisions and orders received from any member state, so that they may fully cooperate with the competent authorities when receiving said decisions and orders. Member states shall ensure that each service provider established, or offering services within their territory, provides written notification of where their designated establishment is located, or where their legal representative resides and provide the respective contact details.

In cases of non-compliance with obligations stipulated by the E-Evidence Regulation, both the designated establishment or the legal representative and the service provider shall be held jointly and severally liable, with the effect that both the designated establishment or the legal representative and the service provider may be sanctioned for non-compliance.

In sum, the E-Evidence Regulation entails new challenges and compliance risks for service providers. Its publication is expected within a few months and it will enter into force three years later.

About Wolf Theiss

Wolf Theiss is one of the leading European law firms in Central, Eastern and South-Eastern Europe with a focus on international business law. With more than 360 lawyers in 13 countries, over 80% of the firm's work involves cross-border representation of international clients. Combining expertise in law and business, Wolf Theiss develops innovative solutions that integrate legal, financial and business know-how.

For more information, please contact:

Georg Kresbach
Partner

E georg.kresbach@wolftheiss.com
T +43 1 51510 5090

Angelika Zotter
Associate

E angelika.zotter@wolftheiss.com
T +43 1 51510 5472