GIBSON DUNN

August 1, 2023

EU STRENGTHENS CROSS-BORDER ACCESS TO E-EVIDENCE IN CRIMINAL PROCEEDINGS

To Our Clients and Friends:

On July 28, 2023, a new EU regulation regarding the cross-border access to electronic evidence in criminal proceedings was announced in the Official Journal of the European Union (the "**Regulation**").[1] The Regulation, which will apply as of August 18, 2026, contains rules under which an authority of a EU Member State may issue a European Production Order or a European Preservation Order to request a service provider in another Member State to produce or to preserve electronic evidence *regardless of the location of the data*.[2] Failing to comply with such orders may involve severe sanctions for such service providers.

The Regulation is a considerable step forward for cross-border government investigations in the European Union. Currently, to obtain electronic evidence, EU Member State authorities must rely either on lengthy judicial cooperation procedures with the risk that data are moved or deleted or on the voluntary cooperation of service providers, a process which, according to the EU Commission, lacks reliability, transparency, accountability, and legal certainty.[3]

1. European Production Orders

Pursuant to the Regulation, a judicial authority of a Member State will be entitled to issue a European Production Order to request electronic evidence directly from a service provider located in another Member State. In the case of requesting traffic data[4] or content data,[5] a judge, a court or an investigating judge will be a proper issuing authority. If a Member State wanted to obtain subscriber data[6] or data for the sole purpose of identifying the user, a public prosecutor would also be entitled to issue a European Production Order. The Member States may define further competent issuing authorities, but in these case the Regulation requires a validation process.[7]

A European Production Order for obtaining traffic data or content data may be issued if these data are necessary and proportionate to the purpose of criminal proceedings relating to offenses punishable in the issuing State by a custodial sentence of a maximum of at least three years or to specific offenses[8] referenced in the Regulation. Further, a European Production Order requires that a similar order could have been issued under the same conditions in a domestic case. These data may also be requested for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings and imposed by a decision that was not rendered in absentia in cases where the person convicted absconded from justice.[9]

In the case of subscriber data or of data requested for the sole purpose of identifying the user, the same conditions apply, but in these cases European Production Orders may be issued for all offenses subject to a criminal investigation.[10]

A European Production Order will be addressed directly to the service provider,[11] but in certain cases of requesting traffic or content data the issuing authority must notify an enforcing authority based in the Member State where the service provider resides.[12] The enforcing authority will assess the case as soon as possible, but no later than ten days following the receipt of the notification, and decide whether it wants to invoke a ground for refusal, such as the protection of fundamental rights or of immunities and privileges.[13]

Upon receipt of a European Production Order, a service provider must expeditiously preserve the requested data and transmit them at the latest within ten days directly to the issuing authority or to the law enforcement authority designated on the order.[14]In cases of emergency, the service provider must transmit the data without undue delay and at the latest within eight hours following the receipt of the order.[15]

2. European Preservation Orders

By way of a European Preservation Order, a judge, a court, an investigating judge, a public prosecutor or – upon validation – another designated authority may order that a service provider located in another Member State preserve electronic evidence for the purposes of a subsequent request for production.[16]

Such an order may be issued for all criminal offenses if necessary for and proportionate to the purpose of preventing the removal, deletion or alteration of data with a view to issuing a subsequent request for production of those data and if it could have been issued under the same conditions in a similar domestic case. These orders may also serve for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice.[17]

In the case of a European Preservation Order, the service provider must preserve the requested data without undue delay. The obligation to preserve the data will cease after 60 days, unless the issuing authority confirms that a subsequent request for production has been issued. During that 60-day period, the issuing authority may extend the duration of the obligation to preserve the data by an additional 30-day period if necessary to allow for the issuing of a subsequent request for production.[18]

3. Notion of a Service Provider Offering Services in the Union

The Regulation applies to service providers which offer services in the European Union.[19] The Regulation defines a "service provider" as any natural or legal person that provides one or more of the following categories of services:

- Electronic communications services;[20]
- Internet domain name and IP numbering services, such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services;
- Other information society services[21] that enable their users to communicate with each other; or make it possible to store or otherwise process data on behalf of the users to whom the service is rendered, provided that the storage of data is a defining component of the service provided to the user.[22]

Financial services such as such as banking, credit, insurance and re-insurance, occupational or personal pensions, securities, investment funds, payment and investment advice are not covered by the Regulation.[23]

A service provider in that sense offers services within the European Union if it enables natural or legal persons in a Member State to use the services listed above and if it has a substantial connection, based on specific factual criteria, to that Member State.[24] Such a substantial connection is considered to exist where the service provider has an establishment in a Member State, where there is a significant number of users in one or more Member States or where the service provider targets its activities towards one or more Member States.[25]

Pursuant to a EU Directive announced on the same day as the Regulation in the Official Journal of the European Union (the "**Directive**"), Member States will have to ensure that all service providers offering services in the European Union designate a legal representative or a designated establishment to receive, comply with, and enforce requests to gather electronic evidence.[26]

4. Sanctions, Enforcement, Conflict of Laws

The Regulation sets forth that Member States must enact rules on pecuniary penalties for infringements of the execution of European Production Orders or European Preservation Orders. These pecuniary penalties must be effective, proportionate and dissuasive. In that respect, Member States must ensure that pecuniary penalties of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year can be imposed.[27] Pursuant to the Directive, Member States will have to ensure that that both the designated establishment or the legal representative and the service provider can be held jointly and severally liable for non-compliance so that each of them may be subject to penalties.[28]

Apart from pecuniary penalties, the Regulation contains detailed rules on the enforcement by the enforcing state.[29] However, a service provider must inform the issuing authority and the enforcing authority if it considered that the execution of a European Production Order or of a European Preservation Order could interfere with immunities or privileges, or with rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media, under the law of the enforcing State. In such cases, the issuing authority decides whether to withdraw, adapt or maintain the respective order. In addition, in the case of a European Production Order, the enforcing authority may raise a ground for refusal.[30]

A special review procedure applies, if a service provider invoked that complying with a European Production Order would conflict with an obligation under the law of a third country. Then, the service provider would have to file a "reasoned objection" within ten days after receipt of the European Production Order. If the issuing authority decided to uphold the order, a competent court of the issuing state would have to review the case. Importantly, if this court found that the law of the third country prohibits disclosure of the data concerned, the court would not automatically lift the European Production Order but rather balance relevant factors (some of which are set out in more detail in the Regulation[31]) to decide whether to uphold or lift the order.

---

[1] Eur-Lex, Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, available under https://eur-lex.europa.eu/eli/reg/2023/1543/oj (last visited [July 31, 2023]).

[2] Article 1(1) of the Regulation.

[3] EU Commission, press release of November 29, 2022, https://ec.europa.eu/commission/presscorner/detail/es/ip_22_7246 (last visited [July 31, 2023]).

[4] Article 3 no. 11 of the Regulation.

[5] Article 3 no. 12 of the Regulation.

[6] Article 3 no. 9 of the Regulation.

[7] Article 4(1) and (2) of the Regulation.

[8] Article 5(4) of the Regulation.

[9] Article 5(2) and (4) of the Regulation.

[10] Article 5(2) and (3) of the Regulation.

[11] Article 7 of the Regulation.

[12] Article 3 no. 16, 17 and Article 8 of the Regulation. No notification is necessary where the offense has been committed, is being committed or is likely to be committed in the issuing State and the person whose data are requested resides in the issuing State.

[13] Article 12 of the Regulation.

[14] Article 10 of the Regulation.

[15] Article 10(4) of the Regulation.

[16] Article 5(3) of the Regulation.

[17] Article 6(2) and (3) of the Regulation.

[18] Article 11(1) of the Regulation.

[19] Article 2(1) of the Regulation.

[20] Article 2 no. 4 of Directive (EU) 2018/1972 establishing the European Electronic Communications Code.

[21] As referred to in Article 1(1) (b) of Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

[22] Article 3 no. 3 of the Regulation.

[23] Article 3 no. 3 of the Regulation, see also Article 2(2) lit. b of the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[24] Article 3 no. 4 of the Regulation.

[25] Article 3 no. 4 of the Regulation.

[26] Eur-Lex, Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, available under https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0123 (last visited [July 31, 2023]).

[27] Article 15 of the Regulation.

[28] Article 3(5) of the Directive.

[29] Article 16 of the Regulation.

[30] Articles 10(5) and 11(4) of the Regulation.

[31] According to Article 17(6) of the Regulation, the assessment shall in particular be based on the following factors, while giving particular weight to the factors referred to in points (a) and (b): (a) the interest protected by the relevant law of the third country, including fundamental rights as well as other fundamental interests preventing disclosure of the data, in particular national security interests of the third country; (b) the degree of connection between the criminal case for which the European Production Order was issued and either of the two jurisdictions, as indicated inter alia by: (i) the location, nationality and place of residence of the person whose data are being requested or of the victim or victims of the criminal offense in question; (ii) the place where the criminal offense in question was committed; (c) the degree of connection between the service provider and the third country in question; in this context, the

data storage location alone shall not suffice for the purpose of establishing a substantial degree of connection; (d) the interests of the investigating State in obtaining the evidence concerned, based on the seriousness of the offence and the importance of obtaining evidence in an expeditious manner; (e) the possible consequences for the addressee or for the service provider of complying with the European Production Order, including the potential penalties.

The following Gibson Dunn attorneys assisted in preparing this update: Andreas Dürr, Kai Gesing, Katharina Humphrey, and Benno Schwarz.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. If you wish to discuss any of the matters set out above, please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following members of Gibson Dunn's White Collar Defense and Investigations or Anti-Corruption and FCPA practice groups in Germany:

Corporate Compliance / White Collar Matters
Andreas Dürr (+49 89 189 33 219, aduerr@gibsondunn.com)
Ferdinand Fromholzer (+49 89 189 33 270, ffromholzer@gibsondunn.com)
Kai Gesing (+49 89 189 33 285, kgesing@gibsondunn.com)
Katharina Humphrey (+49 89 189 33 217, khumphrey@gibsondunn.com)
Markus Nauheim (+49 89 189 33 222, mnauheim@gibsondunn.com)
Markus Rieder (+49 89 189 33 260, mrieder@gibsondunn.com)
Benno Schwarz (+49 89 189 33 210, bschwarz@gibsondunn.com)
Finn Zeidler (+49 69 247 411 530, fzeidler@gibsondunn.com)
Mark Zimmer (+49 89 189 33 230, mzimmer@gibsondunn.com)