DIGITALEUROPE

DIGITALEUROPE position on the proposed e-evidence package

Brussels, 2 August 2018

As the voice of the digital technology industry in Europe, DIGITALEUROPE represents many companies that provide a range of cloud-based services to enterprises and consumers across the EU. We consider the European Commission's proposals on improving cross-border access to electronic evidence in criminal matters (hereafter the 'e-evidence package') an important opportunity to provide legal certainty for both companies operating in this space and users – both citizens and businesses – who rely on our members' services to store and process some of their most sensitive and private information.

Our members take their responsibility to maintain the safety, security and privacy of millions of users in the EU seriously and invest heavily in technologies and processes designed to protect the security and confidentiality of data stored in the cloud. They also recognise that there are situations where they need to assist law enforcement agencies (LEAs) carrying out investigations into criminal activity. As stated in previous DIGITALEUROPE papers,[1] we believe that the legal framework governing cross-border requests should be clarified, and we are eager to continue to work with all relevant stakeholders on these important issues.

DIGITALEUROPE has supported the European Commission's effort to find workable solutions to improve cooperation with service providers within the existing framework. We believe the proposed package can establish a transparent and principled EU-wide framework that enables LEAs pursuing criminal investigations in one Member State to obtain digital evidence from a provider established in a different Member State, regardless of where that evidence is located.

The proposal also includes several critical safeguards to ensure that users' fundamental rights are respected and moves the EU closer to creating a more consistent and rules-bound international framework for lawful access to data in the cloud. The proposed forms to request data will also greatly enhance harmonisation and legal clarity. We also support the Commission's proposal for a Directive to establish a legal representative in the Union.

This legislation will set an important international precedent. It is essential for the EU to define its jurisdictional views in a way that would allow the Union to feel comfortable should its approach be replicated by other countries, which could have substantially different rule-of-law and fundamental rights safeguards. As they currently stand, the proposed jurisdictional rules are based on the 'offering of services in the Union' – both enabling legal or natural persons to use the service and with a substantial connection to the EU – but lack other international standards, such as 'possession and control.' EU legislation may be followed by other countries of varying rule-of-law standards; it is thus important that it improves and does not undermine the protection offered by the current system.

DIGITALEUROPE looks forward to engaging in a constructive discussion with policymakers and stakeholders on all key points in the proposals.

[1] See most recently our response to the European Commission's public consultation on improving cross-border access to electronic evidence in criminal matters, available at https://ec.europa.eu/info/sites/info/files/digitaleurope_2017_en.pdf

KEY MESSAGES

1. Scope (Articles 1, 3 and 23)

1.1 Material scope

The Commission is to be commended for elements of the proposal's material scope, which covers only stored data (not data in transit) and excludes real-time interception as well as 'direct access.' DIGITALEUROPE welcomes these suggestions, which should be preserved.

1.2 Only EPOs for cross-border situations

The proposal preserves the mechanisms that many Member State LEAs rely on today to obtain data on a cross-border basis, including through European Investigation Orders and Mutual Legal Assistance procedures. **It is important, therefore, that only the European Production and Preservation Orders are used when issued to a company whose main establishment is outside of the requesting authority's country.**

Article 1 states that the Regulation lays down rules under which a Member State authority may order a service provider offering services in the Union to produce electronic evidence. It clarifies, however, that this is without prejudice to authorities' powers to compel service providers established on their territories to comply with similar national measures. While we do not question the right of Member State laws to regulate purely domestic situations, that should not be the case where such national laws have cross-border impacts as this is the very essence of the problem the Regulation is trying to solve.

1.3 Jurisdiction

We are concerned that the Commission's proposal departs from the standard of jurisdiction established by the Budapest Convention. While that standard is composed of four elements,[2] of particular interest is the requirement that the service provider has possession and control over the requested information. **Companies should be able to maintain robust internal procedures that limit access and disclosure rights to users' communication data to those company personnel who are best placed to conduct the task.** Sales personnel in a store that sells hardware, for example, who may or may not be full-time employees and have no reason to access user information such as their emails, should not be punished for their inability to comply with the Order. Recognising the standard based on possession or control should not inhibit effective cooperation, as Production and Preservation Orders will help authorities address the relevant European entities. However, the standard is essential from an international and data protection perspective.

[2] (1) The authority's jurisdiction over the offence; (2) that the service provider has possession or control of the requested information; (3) that the service provider is either in the territory of the party or offers a service in the territory; and (4) that the information requested relates to a service of the provider offered in the territory of the party.

2. Strong protections for users' rights (Articles 4 and 5)

As we have called for previously, any solutions found at EU level need to respect the rule of law and fundamental rights, as confirmed by European Court of Human Rights (ECHR) and CJEU jurisprudence. Accordingly, requests for access to data must respect a number of procedural safeguards. Any request must: be 'reasoned,' based on law and subject to review and decision by a court or an independent administrative body; be limited to what is strictly necessary for the investigation in question; and target individuals implicated in the crime.

We welcome the safeguards in the proposed Regulation that aim to protect users' fundamental rights. We are encouraged by the fact that the Regulation makes it clear that orders for the production of digital data (hereafter referred to as 'EPOs') can only be issued by a judicial authority. We believe that prior judicial review by a judge or court should be required in all cases and not limited to content and transactional data. For EPOs seeking more sensitive data, i.e. the content of a communication or its source or destination, the underlying crime must be serious. EPOs must also be no broader than necessary, i.e. 'necessary and proportionate,' and are barred where the issuing LEA believes the data is protected by immunities or privileges in the Member State of the service provider or where disclosure would impact the national security, defence or other fundamental interests of that Member State. These protections are vital to protecting user rights and must be preserved during the legislative process.

There are additional safeguards we also would like to propose. While the EPO must include the grounds for necessity and proportionality of the measure, as currently drafted such justification need not be included in the communication to the service provider – the Production or Preservation Order's Certificate (EPOC or EPOC-PR). **The service provider should also receive such information in order to be able to properly assess the lawfulness of the request.**

The application of the necessity and proportionality principle should also ensure the EPO applies to data in a fixed time period and cannot be open-ended; we would welcome assurances that this is the case. It should be a further condition that the data could not be obtained by another, less intrusive method. In the context of a request to a service provider in relation to an enterprise customer, the requirements of 'necessary and proportionate' must include justification as to why the request must be addressed to the service provider and not to the customer directly. This must be built into the procedure for seeking judicial authorisation and should be confirmed to the service provider as part of the information provided to the service provider in order for them to properly assess the request. Finally, while Article 1(2) and Recital 12 confirm that the Regulation respects fundamental rights under the ECHR and the Charter, the recital should also explicitly mention the rights of freedom of expression and prohibition of torture. Beyond these procedural safeguards, we would encourage legislators to also consider 'thresholds of proof.'

The Regulation should make it explicit that there is **no requirement for a service provider to reverse engineer, provide back doors or any other technology mandates to weaken the security of its service**. Service providers must have the ability to continue to deploy the best possible encryption technologies to ensure the security, integrity and confidentiality of their services. According to Recital 19, data must be provided regardless of whether it is encrypted or not. Providing encrypted data is rendered useless without the applicable decryption keys; therefore, the reference to providing encrypted data in the recital should be removed from the proposal.

We would strongly discourage the consideration of any measures that would lead to a weakening of data security and privacy of the entire digital ecosystem.

3. Notice and transparency (Articles 11, 19 and 22)

The Regulation recognises that, in some scenarios, EPOCs must be kept confidential. We believe that such 'gag' orders should be the exception and not the rule; Article 11 should be rephrased in this light. When confidentiality of the order is required, it is important that the authority notify the person whose data is being sought without undue delay once notification would no longer obstruct the relevant criminal proceedings.

We welcome the fact that the authority must also provide information about available legal remedies and that the proposal explicitly recognises the ability for providers to notify their users and customers. These requirements not only ensure a degree of transparency around LEA demands for data, but also a guarantee the respect of users' right to effective remedy and due process.

Additional protection would be welcome. Specifically: EPOCs and EPOC-PRs should provide justification where confidentiality is demanded; addressees should be able to challenge compliance with an Order where they believe such confidentiality requirements are not justified; addressees should be informed when such confidentiality requirements have been lifted; and there should be a means to challenge the continued application of confidentiality requirements where no longer justified. We also believe that any such order should be subject to time limits and justification by the authority.

Further consideration should be given to situations where compliance with an EPO or EPO-PR could in itself undermine the confidentiality of the Order. In other words, where access by the service provider would be apparent to the company or person whose data is being sought. Such potential to jeopardise the investigation should serve as a potential justification for non-compliance with an Order.

The percentage of EPOCs and EPOC-PRs where confidentiality clauses are included should also be included in the statistics collected by Member States under Article 19. Such statistics should be published by the Commission, together with the other statistics it receives. The Regulation should prohibit Member States from limiting companies' ability to issue transparency reports on the number of EPO and EPO-PR requests they receive from each country.

We also welcome the fact that the Commission will make information publicly available on the competent issuing authorities, enforcing authorities and courts. The latter category should be expanded beyond the courts relating to third-country cases and include judicial authorities for appealing pecuniary sanctions.

4. Demands for enterprise data (Article 5)

Where the data sought is processed as part of an infrastructure provided by a service provider to a company or other entity, the Regulation requires the LEA to seek that data in the first instance from the company itself. While the Article and accompanying Recital 34 make it clear this includes hosting services, for the sake of clarity it would be good to clarify this covers all enterprise cloud services – including software as a service and platform as a service – not just infrastructure as a service.

LEAs can serve orders on service providers for enterprise data only where directing the order to the enterprise itself would not be appropriate, in particular because doing so might jeopardise the investigation. DIGITALEUROPE strongly supports these rules.

5. Necessity of immunity for good-faith compliance (Recital 46)

The Regulation and Directive require cloud providers to comply with EPOs and other legal processes or face substantial penalties; however, they do not clearly protect providers if their compliance violates other EU or Member State laws. Recital 46 of the Regulation states that providers should be immune from liability for their good-faith compliance with disclosure and preservation orders. **This immunity is critical and should be included in the Regulation's operative provisions.** This change should be a top priority as the proposals move through the legislative process.

6. Time limits for responses (Article 9)

The Regulation requires providers to transmit data to LEAs 'at the latest within 10 days upon receipt' of an EPO, and 'within 6 hours' in emergency cases. To adequately protect their users' interests, however, providers will need time to assess the legal validity of each order and to prepare their response. The time limits in Article 9 will often be too short for these purposes and **we call for the Regulation to be amended to give providers sufficient time to meaningfully evaluate, and respond appropriately to, each disclosure order they receive.**

Furthermore, for emergency cases the time limit should be aspirational as opposed to mandatory. With the best will in the world, it will not always be possible to react more quickly for emergency cases. Given the impact such time limits have on service providers' ability to conduct due diligence, the most important change legislators could make to speed up disclosures of such data in such cases is to provide protection from liability, in accordance with the points raised in the previous section.

Moreover, if all requests are urgent, providers will no longer be in the position to prioritise the true emergency cases. Such broad possibilities for authorities to depart from the already very tight deadlines should be deleted.

7. Clear rules on handling conflicts with foreign law (Articles 15 and 16)

To improve the efficiency and resilience of information systems, electronic data is nowadays often stored across national borders. This also means that when LEAs demand data, that data may be located in countries outside the Union and its disclosure might violate foreign law. Online service providers and cloud providers more often than not operate across national borders and may be subject to a range of legal requirements that will likely conflict. The Regulation establishes two separate procedures through which a provider can challenge an EPO on these grounds. It also contemplates in certain situations that an EU court can notify authorities in foreign countries of the demand and give them an opportunity to oppose it.

These safeguards provide important protections for both users and providers. They also ensure that LEA demands for data address potential conflicts in a responsible way that respects the sovereignty and other compelling interests of those foreign states that might be impacted by the disclosure. These procedures also provide an important template for a broader international framework for dealing with legal conflicts created by cross-border demands for data.

While we strongly support these safeguards, the proposed system can be further improved in order to prevent authorities in third countries from being bottlenecks to the correct application of applicable law. If the competent Member State court determines that there is a conflict of law under Article 15, they should automatically lift the Order as opposed to referring it to the third-country authority for possible objection.

There will likely be many instances where the court has enough information at its disposal – expert witnesses, previous submissions, testimony that was submitted in previous cases or other sources – to make this decision. It should be left to the court to decide whether intervention for the foreign authority is necessary. Instead, the review mechanism should be used to give third-country authorities the right to object and ask for further review if the Court decides to uphold the Order under Articles 15 or 16. These small nuances are important in light of the likely volume of requests that may trigger the process.

We welcome the recognition in the explanatory memorandum of the specific prohibitions within the US Electronic Communications Privacy Act that prevent the disclosure of content data except in very limited circumstances; the acknowledgement that MLAs should remain the main tool to access such data; and the recognition that an international agreement with the US is the potential route to tackle this conflict. Explicit acknowledgement of this clear conflict of law would ensure consistent interpretation across Member States.

8. Mechanism to address conflicts with Member State laws

While Articles 15 and 16 of the Regulation provide mechanisms for courts to address potential conflicts with third-country laws, there is no mechanism to guide providers when compliance with an order would violate the laws of a Member State other than that of the enforcing State, i.e. the Member State where the provider receives the order. Such conflicts could arise in any case where the data subject is a national of a Member State other than the issuing or enforcing State. **Providers should have the ability to challenge compliance with orders that create a risk of such conflicts.**

9. Provider participation in conflict-of-law evaluations

When a provider challenges an order on the basis that compliance would conflict with third-country laws, Articles 15 and 16 authorise the issuing Member State authorities to refer that decision to a Member State court for review. However, neither Article gives providers the right to intervene in these proceedings. Provider participation will be important, as providers will often have information relevant to a court's determinations. Lack of provider participation could lead courts to rule based on incomplete understandings of the law or facts. **Articles 15 and 16 should expressly authorise providers to intervene in these court proceedings.** It should be stressed, in this context, that the requirement for the court proceeding to take place in the issuing country, rather than the enforcing country and location of designated legal representative, will create an impediment for smaller companies that do not have capacity to challenge in all Member States.

10. Legal representatives (Article 7 of the Regulation and Articles 1, 2 and 3 of the Directive)

Our presumption is that the legal representatives are established in a separate legal instrument in order to ensure that they are the applicable addressee not only for EPOCs and EPOC-PRs but for a wider arrange of instruments available under domestic law. The intention for broader applicability of the representative is confirmed in Article 1(1) and Recital 8 of the Directive. Establishing the legal representative with a Directive, which requires transposition into national law, adds an unnecessary layer of confusion, however, and we would prefer either incorporation into the main Regulation or a separate Regulation as the appropriate legal instrument.

The clause allowing national authorities to address service providers established on their territory (Article 1 of the Directive and accompanying Recital 11) contradicts the stated goal to simplify and harmonise the point of contact. While we understand this may be appropriate where service providers are only established in that Member State, it does not make sense for international service providers and will only slow the time to respond to such requests.

Likewise, authorities should not be allowed to address any establishment of a service provider when the legal representative does not comply with an EPOC or EPOC-PR, as is currently possible under Article 7 of the Regulation. Authorities should not be permitted to go forum shopping for a more pliable or less knowledgeable branch of the same service provider simply because the representative did not comply; this possibility should only apply where the legal representative does not respond in the allotted time in emergency cases.

Finally, liability for non-compliance should be applied to the service provider or other legal entity. Given that the legal representative can be a natural person under the Directive, it should be clear that they cannot be held personally liable for pecuniary sanctions.

CONCLUSION

DIGITALEUROPE believes that any solution to improving criminal justice in cyberspace must consider the need for users of digital and online services such as cloud computing – whether individuals, governments or businesses – to be accorded the same protections for their e-evidence as for the information they commit to paper, including the right to be notified that their data is being accessed.

DIGITALEUROPE is acutely aware that customers often do not want to put their data in a cloud infrastructure outside their national borders in part due to the concern that law enforcement in another country could obtain their data. Any new framework must address this core concern and possible inhibitor to adoption of cloud technologies. Potential customers will naturally be reluctant to take advantage of cloud solutions if they perceive that their privacy protections will be reduced. These customers, as data controllers themselves, have direct legal obligations concerning the management of their data and they – not service providers – should be direct recipients of any law enforcement demands for data.

Any EU proposal should also take into account the international precedent it sets. It should honour international standards defining jurisdiction, as defined in the Budapest Convention. It should also strive to complement the EU rules with government-to-government solutions. Such solutions would limit the precedent-setting nature of the e-evidence proposals to countries with strong privacy protections and rule of law, thus limiting conflicts of law. This would allow the EU to raise, rather than undermine, the global rule-of-law and fundamental rights standard.

We hope that the e-evidence proposal will provide a strong platform for the Commission to negotiate agreements with third countries that provide similar rules-based protections for users and providers when LEAs seek access to stored data on a cross-border basis, including reciprocal arrangements between the EU and the US. We look forward to working with the Commission, the Council and the Parliament to further refine the Regulation and Directive along the lines indicated above.

--

For more information please contact:
Alberto Di Felice, DIGITALEUROPE's Senior Policy Manager for Infrastructure, Privacy and Security
alberto.difelice@digitaleurope.org or +32 2 609 53 10

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total over 35,000 ICT companies in Europe represented by 63 Corporate Members and 39 National Trade Associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK