DIGITALEUROPE

15 OCTOBER 2019

The proposed e-evidence package in light of the Council's General Approach

Executive Summary

As the voice of the digital technology industry in Europe, DIGITALEUROPE represents many companies that provide a range of digital services to enterprises and consumers across the EU. The European Commission's proposal on cross-border access to electronic evidence in criminal matters (hereafter the 'e-evidence package') presents an important opportunity to rectify legal uncertainty and establish harmonised substantive and procedural safeguards for both citizens and businesses who rely on our members' services to store and process some of their most sensitive and private information. A more robust and rights-protecting e-evidence framework in Europe will also better position Europe to improve international cooperation with the US and other third countries that better meets the needs of all stakeholders.

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 stored data. In light of this, we have reservations about the General Approach issued by the Council of the European Union in December 2018 (E-evidence Regulation) and again in March 2019 (E-evidence Directive), which would scale back several important safeguards in the Commission's original proposal and erode protections for users of digital services across Europe.

We urge the European Parliament not only to improve the Commission's original proposal but also to remove changes introduced by Council. In this paper, we summarise the changes we believe are necessary to improve the e-evidence package to better reflect European values and meet the needs of citizens and business.

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

DIGITALEUROPE

Table of Contents

- Executive Summary 1
- Table of Contents 3
- Scope (Arts 1, 3 and 23) 4

Material scope 4

Exclusive use of Union instruments for cross-border situations 4

Jurisdiction 5

- Strong protections for users' rights (Arts 4 and 5) 6
- Notice to the user and transparency (Arts 11, 19 and 22) 8
- Member State notification (Art. 7a) 9
- Demands for enterprise data (Art. 5) 10
- Necessity of immunity for good-faith compliance (Recital 46) ... 11
- Time limits for responses (Art. 9) 11
- Ability for service providers to intervene with orders (Art. 9) 12
- Sanctions (Art. 13) 12
- Clear rules on handling conflicts with foreign law (Art. 15 and 16) 13
- Provider participation in conflict-of-law evaluations 15
- Mechanism to address conflicts with Member State laws 15
- Legal representative (Art. 7 of the Regulation and Arts 1, 2 and 3 of the Directive) 16
- GDPR main establishment analysis 17
- Double criminality 18
- Conclusion 18

Scope (Arts 1, 3 and 23)

Material scope

DIGITALEUROPE agrees with both the Commission and the Council positions which restrict the scope of the e-evidence package to stored data, excluding real-time interception and 'direct access.' DIGITALEUROPE urges the European Parliament to do the same.

Exclusive use of Union instruments for cross-border situations

When law enforcement authorities seek data from a company whose main establishment is located outside of the requesting authority's country, the e-evidence package preserves mechanisms that many law enforcement authorities (LEAs) rely on today to obtain data on a cross-border basis, including through European Investigation Orders (EIOs) and orders obtained through Mutual Legal Assistance (MLA) ('Union measures'). The e-evidence package also preserves the use of national orders for purely domestic scenarios.

Art. 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.

It is unfortunate that the Council's General Approach does not impose any obligation on an issuing authority to use a European Production Order (EPO) or European Preservation Order (EPO-PR) over a domestic instrument in cross-border cases – a shortcoming it shares with the European Commission text. As a result, the Council's text allows LEAs to bypass the safeguards set out in the proposed package and other Union measures and instead use a purely domestic legal process to obtain data about users located in a different Member State.

Such domestic procedures might offer fewer safeguards and result in weaker protections for fundamental rights across the EU. This approach also runs

counter to the proposal's fundamental harmonisation goal, as service providers will be required to examine, and process orders based on different legal bases.

We urge the European Parliament to require LEAs to use EPO(-PR)s or other Union instruments over domestic procedures unless those instruments are applicable. Revising the proposals in this way will strengthen safeguards for fundamental rights and reduce the risk that LEAs, using domestic procedures, will impose demands on service providers that can circumvent these safeguards.

Jurisdiction

We are concerned that both the Commission's proposal and the Council's General Approach depart from the standard of jurisdiction established by the Budapest Convention. That standard is composed of four elements, including the requirement that the service provider has possession and control over the requested information, which is missing from the e-evidence package.[1]

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 sell 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 EPO(-PR)s will help authorities address the relevant European entities. However, the standard is essential from an international and data protection perspective.[2]

1 See pages 13-14 of the study Commissioned by the LIBE Committee 'an assessment of the Commission's proposal on electronic evidence' (http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604989)

2 It is also important that this standard is also preserved in the context of the 2nd Additional Protocol to the Budapest Convention.

Strong protections for users' rights (Arts 4 and 5)

As we have called for previously, any solutions found at EU level must respect the rule of law and fundamental rights, as confirmed by European Court of Human Rights (ECHR) and Court of Justice of the European Union (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.

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 should be barred where the issuing LEA believes the data is protected by immunities or privileges in the Member State of the service provider, where the user is located, 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.

Furthermore, DIGITALEUROPE is concerned that the Regulation does not require a sufficient threshold of proof for obtaining the content of one's communications. One solution could be that the legislation requires that when requesting data from a provider established in another Member State, the issuing authority must present specific facts to the judge demonstrating that the requested information is relevant and material to an ongoing criminal investigation. When requesting the content of the communication, the issuing authority should also be required to demonstrate that the evidence is likely to be present in the specific place to be searched.

As pointed out by the European Parliament in its working documents, as it stands, LEAs would be able to demand too much data, which in the aggregate could reveal more information than was intended about the target(s), thereby conflicting with the requirement of necessity and proportionality. Moreover, the issuing authority should also be required to demand data only for a fixed time period. ***Demands must not be open-ended.***

Companies should be able to object to demands that are clearly too broad in order to prevent unlawful disclosures. In many cases, only the service provider will know that the information sought is overbroad. In order to better assess orders that demand too much data, whether unwittingly or not, the issuing authority should be required to communicate the grounds for necessity and proportionality in the Production or Preservation Order's Certificate (EPOC(-PR)). The issuing authority must also certify in the EPOC(-PR) that the data could not be obtained by another, less intrusive method.

We strongly believe that not only the Member State authority but also the service provider should receive such information in order to properly assess the lawfulness of the request.

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 should be built into the procedure for seeking judicial authorisation and should be confirmed to the service provider as part of the information provided in order for providers to properly assess the request.

Finally, while Art. 1(2) and Recital 12 confirm that the Regulation respects fundamental rights under the ECHR and the Charter for Fundamental Rights, 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 and other security 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, we would argue that 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.

Notice to the user and transparency (Arts 11, 19 and 22)

The Commission's original proposal recognises that, in some scenarios, EPOCs must be kept confidential. However, the proposal also recognised that providers should not, by default, be required to keep the orders secret.

DIGITALEUROPE strongly rejects amendments made by the Council to Art. 11 which would prohibit service providers from notifying persons or entities that their data is being sought unless the issuing authority explicitly requests the provider to do so. Moreover, the Council's text imposes no obligation on LEAs to justify the need for secrecy to an independent authority, or to establish that these restrictions on notice are no broader than necessary and respect the fundamental rights of all affected parties.

Secrecy should only be required when the circumstances necessitate it. Any requirement for secrecy should be narrowly tailored to the circumstances and last only as long as necessary (i.e. one year or less barring exceptional circumstances). Moreover, the issuing authority should provide a justification as to why giving notice would jeopardise an ongoing investigation and/or endanger public security. In this regard, DIGITALEUROPE agrees with the European Parliament working documents that 'prior notification of the suspect or accused is key.'[3]

DIGITALEUROPE urges the European Parliament to require LEAs to notify impacted individuals and remove any bar against service providers from being able to do so, unless the circumstances of the specific investigation justify secrecy for a limited period of time. Moreover, if secrecy is justified, LEAs should be required to notify the affected individuals as soon as notification would no longer obstruct the criminal investigation.

DIGITALEUROPE supports the Commission's proposal that the LEAs must provide information about available legal remedies. This requirement not only ensures a degree of transparency around LEA demands for data, but also guarantees the respect of users' right to effective remedy and due process. DIGITALEUROPE fully supports the inclusion of additional protections such as

[3] See page 2 of the '6th Working Document (A) on the proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Safeguards and remedies.' (http://www.europarl.europa.eu/doceo/document/LIBE-DT-637466_EN.pdf?redirect)

an ability for addressees to challenge compliance with an Order where they believe confidentiality requirements are not justified.

The percentage of EPOC(-PR)s where confidentiality clauses are included should also be included in the statistics collected by Member States under Art. 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(-PR) requests they receive from each country. We are encouraged to see that the Member States explicitly granted the service providers the right to 'collect, maintain, and publish statistics' on the Orders received.

Finally, DIGITALEUROPE supports the Commission's proposal which would make information publicly available regarding 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.

Member State notification (Art. 7a)

One of the most significant changes the Council made to the Commission proposal is the introduction of the additional notification procedure to another Member State. The Council text states that, in cases where the issuing LEA has reasonable grounds to believe that an EPO seeks data (content) of a person who is not residing on its own territory, it must send a copy of the EPOC to the enforcing Member State.

DIGITALEUROPE recognises the merit of involving the enforcing Member State in the process. However, in instances where the issuing authority has reasons to believe that the requested content data may be protected by immunities and privileges of the enforcing Member State, there is no obligation under Art. 7a(2) for the enforcing authority to clarify the issue within 10 days. Furthermore, Art. 7a(4) notes that the notification procedure shall have no suspensive effect on the obligations of the EPOC addressee. This may lead to a situation where a service provider responds, in good faith, within 10 days of receiving an EPOC, only to find out that after 10 days the enforcing authority confirms the disclosed content data was protected by an immunities or privilege ground. Such a situation would lead to legal liability for service providers.

Furthermore, DIGITALEUROPE believes that there should be a requirement to notify the Member State where the user whose information is sought resides (i.e.

the 'affected' Member State). Relevant procedural protections and remedies often arise under the laws of the Member State where a person resides, which often will not be the enforcing Member State. For example, under the Council proposal, Ireland may be inundated with notices since many service providers have established their law enforcement compliance team in Ireland. This will create a difficult situation for the Irish authorities to evaluate all orders.

Failing to give notice to affected Member States risks abrogating the fundamental rights of individuals whose data is targeted. It also means that providers will be compelled to disclose a person's data in situations where doing so would conflict with the law of the Member State where the person resides. Resolving those conflicts will be difficult if not impossible. This could be circumvented if the affected Member State is unaware of an issued order.

DIGITALEUROPE urges the European Parliament to require the issuing authority to notify the Member State of the EPO where the person targeted by the order resides. The 10-day timeline for compliance with the EPO by the service provider should be suspended until the enforcing authority is able to verify whether the requested data is protected by immunities or privilege grounds. This Member State will be in the best position to identify any applicable protections and will have the strongest interest in defending these protections. This solution should not be unduly burdensome given that, according to the Commission, around 92% of LEA demands for user data involve targets located in the same Member State.

Demands for enterprise data (Art. 5)

We are pleased to see that the Council text preserved the Commission's proposals that where LEAs seek data stored on behalf of an enterprise, they must seek the data from the enterprise itself, unless doing so would jeopardise the investigation. Again, 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.

We are also pleased that the Council draft has opted to add a clause protecting the confidentiality of public authorities' data stored in the cloud by limiting the reach of the EPO seeking such data to the issuing State.

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

The Regulation and Directive require service 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 priority as the proposals move through the legislative process.

Time limits for responses (Art. 9)

The Commission's proposal 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 Art. 9 will often be too short for these purposes and it is unfortunate that the Council has decided to uphold such tight deadlines for response.

The Regulation should 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. Even with the best intentions, it will not always be possible to react in a matter of hours, even 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. It is important that only an imminent threat to life or physical harm should be treated as emergency. The proposed broad possibilities for authorities to depart from the already very tight deadlines should be deleted.

Ability for service providers to intervene with orders (Art. 9)

Art. 9(5) of the Commission text authorises service providers to object to an EPO where it is apparent that the order manifestly violates the Charter of Fundamental Rights or is manifestly abusive. We share the Member States' view that this provision should not be focused on concerns that arise under the Charter but should instead give service providers the right to raise concerns whenever an order for user data is unlawful, overbroad or otherwise abusive.

DIGITALEUROPE members also see requests that may have impact on some basic rights, such as the right to freedom of expression. Therefore, a fundamental rights ground for refusal should be maintained. We welcome the Parliament's working document[4] that recognises the important role service providers can play in this regard.

Empowering service providers to raise such concerns is critical. In some cases, only service providers will have the ability to identify demands that are overly broad or inappropriate for other reasons. The Council's compromise text unfortunately does not give service providers any right or mechanism by which to raise concerns about the legality of orders they receive, and we strongly urge the European Parliament to reinstate such a possibility.

Sanctions (Art. 13)

Art. 13 of the Council text would require Member States to administer fines of up to 2% of a service provider's total worldwide annual turnover for failure to comply

[4] See pages 3-5 of the '3rd Working Document (A) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Execution of EPOC(-PR)s and the role of service providers.' (http://www.europarl.europa.eu/doceo/document/LIBE-DT-634849_EN.pdf?redirect)

with an EPO, an amount that could run into the hundreds of millions of euros, or even billions for some providers.

Such fines will ultimately encourage compliance at all costs and penalise providers who take their responsibilities to protect their users' data seriously. Skewing incentives in this way compounds the problem of diminished protections for fundamental rights that runs throughout the Council text.

In addition, sanctions at this level also exacerbate the lack of protections against conflicts of laws in the Council text in cases where compliance with an EPO would violate a third-country law. For example, service providers will face the impossible choice of refusing to comply with the order and facing massive fines or complying with the order and violating their legal obligations, potentially triggering criminal sanctions in a third country.

We urge the European Parliament to maintain the original sanctions provisions set out in Art. 13 of the Commission's proposal. This would require Member States to provide for sanctions that are 'effective, proportionate and dissuasive.'

Clear rules on handling conflicts with foreign law (Art. 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. Service providers more often than not operate across national borders and may be subject to a range of conflicting legal requirements. The Commission's proposal established two separate procedures through which a provider can challenge an EPO on these grounds. It also contemplated 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. By removing Art. 15 from the Council draft, these safeguards intended to provide protection for users and providers have been substantially weakened.

The Council text has made the requirements for courts to communicate with third-country authorities to resolve identified conflicts of laws optional rather than

mandatory. At the same time, the Council text also prohibits service providers from disclosing that they have received an Order, which means that third countries – including countries that work closely with the EU on important public security and law enforcement matters – might never know that EU authorities have forced the provider to violate their laws. In addition, this will make it almost impossible for service providers to object or defend the underlying fundamental rights of the Order.

DIGITALEUROPE is also concerned that even where a court determines that enforcement of the Order would violate third-country laws protecting fundamental rights, the Council text authorises the court to uphold the Order. Lastly, the Council text gives providers only 10 days to file a reasoned objection setting out 'all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation.' This very short period for service providers to assess the Order is far too insufficient for providers to prepare such a complex analysis.

We encourage the European Parliament to reinstate the Commission's original proposal for Art. 15. However, we believe that the proposed system can be improved upon further. If the competent Member State court determines that there is a conflict of law under Art. 15, they should automatically lift the Order. This should not depend on the third country's authority and its ability to intervene, especially if the court has the information necessary to decide the case.

There will indeed likely be many instances where the court has enough information at its disposal to make a well-informed decision, such as expert witnesses, previous submissions or testimony that was submitted in previous cases. Moreover, the proposal should require courts, where they have identified a conflict with third-country laws protecting fundamental rights, to lift the Order unless the competent authorities of the third country attest that there is no conflict. In addition, competent authorities should provide opportunities for service providers to submit arguments and evidence directly to such courts as to the existence or nature of such a conflict. 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. We continue to believe that explicit acknowledgement of this clear conflict of law would ensure consistent interpretation across Member States.

Provider participation in conflict-of-law evaluations

When a provider challenges an Order on the basis that compliance would conflict with third-country laws, Arts 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.

Arts 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 proceedings to take place in 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. It is positive to see that these issues and concerns have been picked up through the European Parliament's published working documents.

Mechanism to address conflicts with Member State laws

While Arts 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.

Legal representative (Art. 7 of the Regulation and Arts 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 EPOC(-PR)s, but also for other instruments available under domestic law. The intention for broader applicability of the representative is confirmed in Art. 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 and we continue to advocate converting the Directive to a Regulation or a separate Regulation as a more appropriate legal instrument.

The clause allowing national authorities to address service providers established on their territory (Art. 1 and accompanying Recital 11 of the Directive) 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.

DIGITALEUROPE strongly believes that EPOC(-PR)s or other Union-level instruments should be the only instruments used in a cross-border context.

Likewise, authorities should not be allowed to address any establishment of a service provider when the legal representative does not comply with an EPOC(-PR), as is currently possible under Art. 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 apply, if at all, only where the legal representative does not respond in the allotted time in emergency cases. Entities that do not have possession and control over the information sought should only be responsible for forwarding the request to the establishment of the provider that does have possession and control over the sought information.

Finally, liability for non-compliance should be applied to the service provider or other legal entity and not the identified legal representative. 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.

GDPR main establishment analysis

The GDPR's 'lead supervisory authority' mechanism ensures that in cases of cross-border data processing, a single Member State's data protection authority (DPA) – in the controller's or processor's Member State of 'main establishment' – has primary oversight of that processing. The main establishment mechanism enhances coordination among DPAs and streamlines regulatory compliance for service providers. Perhaps inadvertently, however, the Directive could impact and create confusion around this important measure.

Under the Directive, legal representatives must have the authority to receive, comply with and enforce Member State decisions and orders issued for the purpose of gathering evidence in criminal proceedings (Arts 3(1) and (5)e). Recital 18 states that legal representatives 'should be able to comply' with decisions and orders addressed to them and Art. 3(7) of the Directive states that legal representatives must have the 'necessary powers and resources to comply.'

It is unclear what this obligation requires in practice or how it intersects with the GDPR's main establishment test. Must the legal representative have the power not only to accept demands and disclose data in response, but also to decide whether or not to disclose data? If so, does that suggest that the organisation's main establishment is, at least for purposes of that processing, located wherever the legal representative is located? Or could compliance with these requirements effectively turn the legal representative into a co- or joint controller with the main establishment?

This issue will be particularly acute for service providers whose current main establishment is in Ireland, because those providers will be required to locate at least one legal representative outside of Ireland, as long as Ireland continues not to participate in the EIO Directive.

To avoid this unnecessary complexity, we propose adding language to the Directive to clarify that the Art. 3(7) requirement for the legal representative to have 'powers and resources' is satisfied so long as the legal representative can accept and process orders served under EU instruments and can disclose data in response to those orders, but need not be the locus of decision-making authority as to whether an order is lawful, and/or should be complied with.

The Council's text amends Recital 15 to state: 'The sole designation of a legal representative should not be considered to constitute an establishment of the service provider.' This is helpful – if there is no establishment, there cannot be a 'main establishment' – and it arguably follows that the 'sole designation' of a legal representative likewise should not be seen as indicative of a main establishment under the GDPR. At the same time, it could be interpreted to mean that the mere act of designating a legal representative does not create an establishment,

without bearing on the question of whether an establishment exists after that representative is vested with the 'powers and resources' required by Art. 3. Moreover, the recital language is non-binding, hence it remains possible under the Directive that a court would hold that the powers vested in a legal representative does constitute an 'establishment' in relation to the relevant processing.

Double criminality

DIGITALEUROPE support harmonisation in this field, which will be particularly helpful for our SME members. The EIO contains a list of crimes to which an EIO can be submitted. We agree with the European Parliament that this list could be also included in the E-evidence Regulation and the EPO(-PR) should be submitted only for these.

However, from a legal certainty perspective it would be beneficial to include a reference as to what some of these crimes mean, in particular when they contain a definition at EU level. For example, the EIO list contains 'computer-related crimes': the EU has a Directive on attacks against information systems, so the definitions should be aligned across the legal instruments.

Conclusion

DIGITALEUROPE believes that any solution to improving criminal justice in cyberspace must consider the need for users of digital and online services – 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 the 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

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

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 Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, Visa, VMware, Xerox.

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
Norway: Abelia
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