DIGITALEUROPE

15 NOVEMBER 2019

Safeguards and Protections

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

EU legislation must always respect the rule of law and fundamental rights, requests for access to data must respect several procedural safeguards. Requests 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, the underlying crime must be serious. EPOs must also be no broader than necessary and should be barred where the issuing LEA believes the data is protected by immunities or privileges.

It is concerning that the Regulation does not require a sufficient threshold of proof for obtaining the content of one's communications. It is recommended 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.

Currently 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 will know when information requests are too broad should be able to object to these orders to prevent unlawful disclosures. To better assess orders that demand too much data, 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.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Any request related to enterprise customer, must be ‘necessary and proportionate’ and justified as to why the request is addressed to the service provider and not to the customer. 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 for providers to properly assess the request.

The Regulation states, 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 should be removed. It should be 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. It is strongly discouraged considerations 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)

In some scenarios, EPOCs must be kept confidential, however, providers should not, by default, be required to keep the orders secret. Council amendments 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. 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.

The issuing authority should provide a justification as to why giving notice would jeopardise an ongoing investigation and/or endanger public security. We urge the European Parliament to require LEAs to notify impacted individuals and remove any bar against service providers from being able to do so.

The percentage of EPOC(-PR)s where confidentiality clauses are included should also be collected by Member States. Statistics should be published by the Commission, together with the other statistics it receives. In addition, it is vitally important that companies maintain the ability to publish transparency reports on the number of orders received from each country. It is also equally important the proposal ensures all information is publicly available regarding competent issuing authorities, enforcing authorities, courts, appeal mechanisms and legal remedies.

We fully support the inclusion of additional protections such as an ability for addressees to challenge compliance with an Order where they believe confidentiality requirements are not justified.

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