DIGITALEUROPE

15 NOVEMBER 2019

Conflicts with Member State and Foreign Law

Clear rules on conflicts with foreign law (Arts. 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 located in countries outside the Union and its disclosure might violate foreign law. The Commission's proposal established two separate procedures through which a provider can challenge an EPO on these grounds.

These safeguards provide protections for both users and providers. Ensuring that LEA demands for data address potential conflicts in a responsible way. Therefore, the protections provided for users and providers have been 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, alongside prohibits service providers from disclosing that they have received an Order. This means that third countries may never know that EU authorities have forced the provider to violate their laws. Ultimately making it impossible for service providers to object or defend the underlying fundamental rights of the Order.

We are concerned that 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. The Council text gives providers only 10 days to file a reasoned objection. This short period for service providers to assess the Order is far too short for providers to prepare such analysis.

There should also be a mechanism to guide providers when compliance with an order would violate the laws of a Member State other than that of the enforcing State.

We encourage the European Parliament to not only reinstate the Commission's original proposal for Art. 15 but improve by allowing Member State courts to lift an Order if any conflict. Also, service providers should be allowed to intervene in court proceedings. Providers should have the ability to challenge compliance with orders that create a risk of such conflicts.

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

We welcome the recognition in the explanatory memorandum of the prohibitions within the US Electronic Communications Privacy Act, limiting the disclosure of content data; acknowledging that MLAs should remain the main tool to access such data. Recognising 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.

Member State notification (Art. 7a)

The Council introduced the additional notification procedure to another Member State. Stating 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.

Issues may arise where the issuing authority believes that the requested content data may be protected by immunities and privileges of the enforcing Member State, there is no obligation for the enforcing authority to clarify the issue within 10 days. In addition, the notification procedure shall have no suspensive effect on the obligations of the EPOC addressee. Situations may arise where a service provider responds, within 10 days, only to find out that the enforcing authority confirms the disclosed content data was protected by an immunities or privilege. This could lead to legal liability for service providers.

Furthermore, there should be a requirement to notify the Member State where the user whose information is sought resides. 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, 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.

By not informing the affected Member States risks abrogating the fundamental rights of individuals whose data is targeted. In addition, 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. This could be circumvented if the affected Member State is unaware of an issued order.

We urge 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.

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