Statement on Inception Impact Assessment: Europol Regulation (Ref. Ares(2020)2555219)

Berlin, 2 July 2020

As digitalisation advances, new challenges are emerging for the field of policing. The gathering of evidence is increasingly taking place in the electronic field. Due to the global nature of digital services and the Internet, the acquisition of this data poses questions and problems for investigating authorities as well as for service providers and operators – issues that have been discussed in various arenas in the recent past and which have in some cases also been addressed from a regulatory perspective. The debate on e-Evidence provides one instance of this, as do the discussions on the Convention on Cybercrime. In this context, the European Commission would also like to redefine and potentially extend the role of Europol, the European investigation agency. The Commission has drawn up an Inception Impact Assessment (IIA) which outlines various scenarios for the further development of the agency.

I. Preliminary Remark

The debate referred to represents an immense challenge for the providers of digital services. The cross-border requests by foreign investigating authorities for the transfer of data – in particular personal, confidential or otherwise legally protected data – means that these companies are faced with questions concerning the extent to which the requests comply with their respective national laws, and whether the transfer of this information could result in criminal or civil law consequences for them. The transfer of data and information at the request of a law enforcement authority outside of its respective responsible national jurisdiction can thus raise issues of liability for the companies and create legal uncertainty.

In addition, the problem exists that such requests undermine the “double criminality” principle. What may be perceived as a minor problem in the case of drug offences may be regarded completely differently in the case of expression offences. The transfer of information and data from foreign jurisdictions is therefore always a critical problem that requires appropriate constitutional safeguards.

II. On the Inception Impact Assessment in Detail

- **On the “Context” Section**

As initially presented, digitalisation poses new challenges for policing. Especially in a European context, where sovereign Member States co-exist

in a relatively small area, both crime and law enforcement can often have a cross-border dimension. Accordingly, the Commission's proposal to strengthen Europol makes sense. It is also to be assumed that criminals will increasingly make use of digital technologies and exploit them for their own purposes, an escalation which is occurring in light of a general upsurge in the digitalisation of society and the economy. Against this background, strengthening Europol with the appropriate digital skills and capacities is a legitimate objective. At the same time, an important premise is being left out of the equation. Digitalisation, the use of encrypted messenger services, and the leap in the number of Internet users are developments mainly driven by private individuals with no criminal intent. In demanding access rights and the possibility to request data, investigating authorities often do not take this fact sufficiently into account. Appropriate regulations must be devised that protect the rights of citizens. This also applies to cross-border access to the corresponding information. The regulations being sought should thus give due consideration to this reality.

- **On the "Problem the Initiative Aims to Tackle" Section**

The fact that Europol cannot obtain data directly from private parties understandably poses a problem for the agency's work. This stems from the nature of law enforcement organisation in Europe, and must be addressed in this realm. In eco's view, presenting Europol with the challenge of an operational problem in this context would be misguided.

- **On the "Objectives and Policy Options" Section**

The strengthening of Europol's cooperation with private parties, as set out under Objective No. 1, offers the opportunity to create a legally compliant and uniform framework for the requests for certain data and information. However, it must be ensured in principle that the measures listed under Options No. 2 and No. 3 are transparent, proportionate and manageable for the companies concerned. The commitment to involve the Member States concerned in the transfer must be clarified in such a way that companies can rely on the legality of the request when transferring information, and that legal protection is achieved which is at least as high as that for existing judicial assistance.

For the options listed under Objective No. 2, eco would like to emphasise that, if rights of request to data for Europol were to be introduced, what should be provided as a matter of urgency is a legal clarification regarding the execution of requests and their legal framework are to be implemented. As part of this clarification, consideration should also be given to the extent to which expenses incurred by companies as a result of the possible transfer of information can be reimbursed.

III. Classification and Conclusion:

The reform of Europol's mandate offers the opportunity to make cross-border law enforcement within Europe more effective. From a provider's perspective, a European central authority for cross-border data transfers is conceivable and, if appropriately implemented, even desirable. If necessary, Europol could become a suitable agency for this purpose. However, a transparent, comprehensible and uniform legal framework for cross-border access to data is what is initially needed. This should be regulated on the basis of an EU law and not merely by extending the powers of investigating authorities. Finally, an agency such as Europol must also be held accountable and subject to control by EU institutions. The question also arises as to who would control the transfer of data to the USA or the United Kingdom.

In regulating cross-border access to data, the following aspects should be taken into account at all times:

- The transfer of data must comply with the law of the respective Member State concerned. In addition to a consistent involvement of the competent authorities of the Member State, it is important that transfers are only permitted for particular offences which all EU Member States have agreed upon. A common catalogue of offences in accordance with the principle of double criminality would make sense in this regard.
- The responsibility for protecting fundamental rights and the legality of criminal prosecution must remain with the state authorities. The provider cannot assess the legality or accept liability for it.
- Technical standards for secure data transfer are required.
- Provision should be made for appropriate compensation for private companies.

eco expresses the hope that the points raised here will be borne in mind in the further debate. The redefinition of Europol's role should not lead to service providers and operators being faced with greater legal uncertainty.

About eco

With more than 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust and ethically-oriented digitalisation. That is why eco advocates for a free, technology-neutral and high-performance Internet.