FEDIL

Positionen - 16/11/2018

POSITION OF FEDIL – E-EVIDENCE

This position paper constitutes FEDIL's contribution to the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters ("e-evidence").

On 17 April 2018, the European Commission proposed a set of measures to make it easier for law enforcement and Judicial Authorities to obtain electronic evidence. Firstly, the proposed regulation will enable a Judicial Authority in one Member State to obtain electronic evidence directly from a service provider or its legal representative in another Member State. Secondly, it will allow to ask a service provider or its legal representative in another Member State to preserve specific data in view of a subsequent request to produce this data.

Context

On European level as well as international, many investigations involve a cross-border request to access electronic evidence. Currently, judicial cooperation in criminal matters within the European Union ("EU") is based on the "*European Investigation Order*" ("EIO"). Precisely, it consists of "*a judicial decision which has been issued or validated by a judicial authority of a Member State to have one or several specific investigative measures carried out in another Member State to obtain evidence*"[1] and the authorities from the service provider's jurisdiction are obliged to carry out the request for data from the issuing Member State.

Cooperation between the EU and third countries for the purpose of gathering information in criminal proceedings is based on "*Mutual Legal Assistance*" agreements[2] ("MLAT"). On 23 March 2018, the United-States federal law enacted the Cloud Act, amending the Stored Communications Act ("SCA") of 1986, and thereby allows federal law enforcement to compel US-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the US or on foreign soil, while at the same time creating the authority and framework for the US to establish a new generation of international agreements in the area of law enforcement, that, on a reciprocal basis, should enable law enforcement agencies to access data in each other's countries to investigate and prosecute crimes. Following the adoption of the Cloud Act and given both the uncertainties[3] and

opportunities that it brings, there is a need to adopt a common EU approach for concluding an executive agreement with the US.

The Commission's proposal will establish European Production and Preservation Orders ("Orders") and, similar to the US Cloud Act, allow competent authorities to collect data from service providers offering services in the EU, even though the company's headquarters may be in a third country or the data stored in another Member State.

General Comments

Effective mechanisms to obtain evidence are paramount in criminal investigations and for an adequate prosecution of criminals. Digital traces become increasingly important to solve or prevent crimes. Our members acknowledge their responsibility in assisting law enforcement and Judicial Authorities by providing or preserving electronic evidence.

Luxembourg's industry has always been in favour of an integrated, borderless internal market, also with respect to effective and efficient cooperation between Judicial Authorities to best protect European citizens and businesses from international crime and terrorism.

The Commission's proposal to make it easier and faster for law enforcement authorities to obtain electronic evidence is an opportunity to increase legal certainty for service providers and users who store and process data. With the right finetuning, this proposal can ensure that users' fundamental rights are respected and is a first step towards a more consistent framework for lawful cross-border access to data. In this respect, FEDIL welcomes that the proposal will apply the same rules to all the service providers *"offering services in the Union"* and thus, enhance harmonisation.

The EU should define its jurisdictional approach and put the rule-of-law and fundamental rights at its core. In view of the need for an EU wide executive agreement with the US on the Cloud Act, it is also important to note that the principles that will be included in the e-evidence proposal, are likely to form the basis for such agreement with the US. EU Member States and authorities thus have an interest in assessing from the start whether the principles that will be enshrined in the e-evidence proposal are equally acceptable in a broader, international context.

Withal, the regulation shouldn't undermine the protection offered by the current system and provide clarity in terms of responsibility (I). Especially, article 13 foresees effective, proportionate and dissuasive pecuniary sanctions against service providers who do not comply with their obligation to preserve or provide electronic evidence (article 9 and 10), as well as those who don't respect the confidentiality clause (article 11). Yet, there is no further protection for service providers who would violate European or national laws and obligations to comply with the proposed Regulation.

To achieve its objective, we believe the regulation also needs further improvements in terms of viability (II).

Specific Comments

I. A COHERENT AND IMPROVED LEGAL CERTAINTY

In the short time frame at disposal, our member companies consider it wise that the Commission's proposal limits its material scope to stored data and excludes direct access to data, real-time interception or data stored at a future point in time. However, more clarity on conflicts of obligations (A) and a legitimate allocation of responsibilities (B) is necessary.

A. The lack of clarity on conflict of obligations

While article 15 and 16 of the proposal lay down a mechanism to address conflicts with third-country laws and article 14 establishes limited grounds for opposing the execution of an order, nothing provides for an eventual conflict with national legal requirements. **The risk of breaching other obligations, and notably** immunities, privileges, obligations to confidentiality that may exist under Member State or Union law**, should allow service providers to contest Orders**.

For example, the Luxembourgish "*Commission de Surveillance du Secteur Financier*" (CSSF) imposes notification rules to financial entities who were asked to provide data. Likewise, a Luxembourgish law on electronic archiving[4] lays down rules on how PSDC[5] certified organisations must provide data to ensure confidentiality – digital signature, encryption – and guarantee a secure transmission. These national laws set out different, stricter rules of data transmission and would conflict with the proposed regulation.

Moreover, the obligation to provide data often contradicts with contractual engagements. There are cases where contracts clauses don't allow service providers to disclose any information about their clients. Therefore, we insist on the importance to maintain the principle that, unless it hampers the investigation, Orders should be directly addressed to the client.

In recital 46, the Commission's proposal states that "*notwithstanding their data protection obligations, service providers should not be held liable in Member States for prejudice to their users or third parties exclusively resulting from good faith compliance with an EPOC or an EPOC-PR*". While we appreciate this mentioning, it is critical to **include an operational provision stating that service providers and their employees wouldn't be liable for their good faith cooperation**.

Still, by executing Orders, breaches of obligations under GDPR[6] could be forthcoming. Indeed, to respect the deadlines but also for technical reasons, data provided or preserved by service providers would often be inextricably linked to personal data that was not subject of the request. To unbundle the dataset properly, companies would have to deploy considerable efforts and invest a lot in the identification of non-requested personal data within the requested dataset. Mostly, if GDPR primes, companies should have more time to apply GDPR and avoid self-incrimination.

Altogether, the final regulation should **include clear procedures on the rules to follow in case of conflict with other European and national obligations**. Ideally, if there is an uncertainty of conflict, the addressee should have the possibility to refer to the national authority and, if need be, submit his arguments to EU courts.

B. The need for a legitimate allocation of responsibilities

According to article 7 of the proposal, Orders "*shall be addressed directly to a legal representative designated by the service provider for the purpose of gathering evidence in criminal proceedings*" or failing this, "*to any establishment of the service provider in the Union*". By doing so, service

providers and not the national authorities will have to verify if requests for electronic evidence from other Member States are valid, authentic, necessary and proportional.

Particularly, we regret that the full reasoning with the grounds for necessity and proportionality isn't communicated to the addressee from the very beginning. This will add to the difficult execution of the Orders.

FEDIL believes that **Judicial Authorities of the Member State of the service provider should have a key responsibility to assess and as the case may be, enforce the request for electronic evidence while leaving service providers the right to make a first assessment and if relevant address local authorities when they doubt on the completion of the conditions under article 5 and 6**. Judicial Authorities have the necessary knowledge and expertise to quickly verify if conditions are met and judge the authenticity as well as the validity of the law enforcement's request.

Additionally, we strongly recommend the implementation of an **EU level platform. It would** offer many advantages, including the possibility of an easy authentication of the request and a secure transmission of the data. FEDIL encourages decision makers to consider the expansion of eIDAS, the eCodex and SIRIUS platforms for the purposes of the proposed regulation. Orders should be digitally signed to be valid and only competent authorities should be able to submit requests on the platform. This would testify the authenticity of the Orders and of the authority in the issuing State. Not only would it improve legal certainty, but also reduce administrative burdens and costs for verification by the service provider. An EU level platform would facilitate the execution of Orders and support more swiftness and efficiency for justice. For example, an exchange platform called TANK, is being developed in Belgium to automate the exchange of data and the connection to this platform will be a condition for compensation by the authorities to ensure collaboration of operators and suppliers.

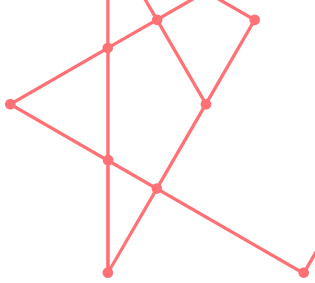
II. AN EFFECTIVE, FEASIBLE AND PRAGMATIC PROCEDURE

A. The limits of data access and encryption

To provide secure services, service providers deploy best possible encryption technologies. These **security measures shouldn't be weakened**. By considering that encrypted data must be provided (recital 19), the addressee would have to communicate the decryption key. Otherwise, the encrypted data would be useless. Yet, these risks undermining the integrity and confidentiality of the service provided to the detriment of the user privacy and trust in the digital ecosystem. Following the same idea, service providers shouldn't be obliged to decrypt data if they don't have the means to do so.

We therefore suggest that it is clarified in an article, that encrypted data should not be decrypted when received a European Preservation or Production Order.

Furthermore, recital 17 mentions that "*data is no longer stored or processed on a user's device but made available on cloud-based infrastructure for access from anywhere*". If it's true that one does not need to be established or to have servers in a specific jurisdiction to provide electronic evidence, it is not accurate that data can be easily accessed from anywhere. For example, in Infrastructure as a Service offerings data processors hold and process data on behalf of the controller but have no access to the content of the data. They may, in some cases, have to provide a large and illegible dataset, which prolongs the actual investigation by retrieving relevant information.



More generally, the proposal doesn't mention how precise the Orders would have to be. On one side, if the request is relatively vague, service providers would have to provide large datasets, therefore the risk of abuses or breaches of GDPR would increase. On the other side, if the judicial authority would ask for a very specific data, one must take the technical feasibility into account.

B. The rigid timeframes

The proposed article 9 obliges addressees to reply to EPOCs within 10 days and authorities can set a shorter deadline where justified. Our member companies regret that the Commission opted for an **unrealistic timeframe, which is rather short** for service providers to comply with the suggested obligation. More flexibility is needed, especially to avoid originating crisis conditions within the company. The regulation should also foresee exceptional procedures, for instance, to allow for an assessment of an uncertain or disproportionate order, if the data extraction reveals particularly difficult or if the legal representative or the qualified officer is not at disposal.

Moreover, the proposal doesn't specify whether electronic evidence has to be provided within 10 **working days** or if it includes non-working days. In case the first scenario applies, the timeframe is obviously reduced to at least 2 days which adds to the unfeasibility of the provision.

In emergency cases, the deadline to reply to EPOCs is 6 hours. FEDIL recognises the necessity for authorities to act quickly in situations where there is an imminent threat to a person's or a critical infrastructure's life or physical integrity (article 2 §15). This deadline should be extended to 72 hours. In addition, the regulation should **include a good faith clause to avoid high penalties where technical constraints wouldn't allow the service provider to be compliant.**

The proposed timeframes do not consider companies' internal processes to retrieve data in respect of other obligations nor do they regard various operational models. For example, if the company provides an infrastructure as a service, the addressee of the Order would have to physically visit the service before being able to extract the requested data. Also, this largely depends on whether the requested data dates from recent past or is older. Clarity and flexibility is needed on this point.

In this context, only *force majeure* or *de facto* impossibility are accepted as justifications for an eventual non-compliance of the service provider. The Commission explains that this is the case when the person whose data is sought wasn't a customer or when the data was lawfully deleted before the order.

Technical burdens should expressively be added to these grounds in order to avoid a restrictive interpretation.

Finally, addressees can delay these deadlines only if an EPOS has been found incomplete, manifestly incorrect or the information provided insufficient. In the proposal as it stands, service providers would need to assess the validity and authenticity of the request. They will also have to verify the compliance with the Fundamental Rights of the EU and Member State laws of the issuing authority.

However, as elaborated above, we think that the service provider should not be responsible for these background checks, the Judicial Authority should be. Such exercise isn't only costly and would oblige companies to recruit extra lawyers but mostly, it is time-consuming, and this is even more crucial where the timeframe is already too short to guarantee compliance of the service provider.

We call on the co-legislators to re-evaluate the timeframe needed by service providers to comply with the Order and amend the proposal accordingly.

C. The inadequate reimbursement

According to article 12 as proposed by the Commission, the service provider may claim reimbursement of its costs only if this possibility is provided by the national law of the issuing State for domestic orders in similar domestic cases.

An operator shouldn't serve a foreign judicial authority free of charge while the foreign operator would be remunerated. **An alignment of the legal systems is urgent to avoid discriminatory treatment.**

Compliance with Orders will require substantial operational and capital costs. The possibility of getting multiple requests from different Member States, combined with tight deadlines and the lack of certainty about the validity, authenticity and proportionality of the Order, will oblige the great majority of service providers to have the Order double-checked by lawyers and thus significantly increase their business expenses. Service providers should be able to transparently indicate the direct costs of providing electronic evidence and have legal means to submit a request for reimbursement to the issuing authorities following the scheme of data portability costs in the GDPR with the difference that reimbursement can apply on first usage. This is even more important when the efforts and the mobilisation of resources didn't pay off and the criminal investigation eventually failed.

FUSSNOTEN

1. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters; Article 1.
2. Council Act 2000/C 197/01 of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union
3. See e.g. European Parliament Resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, where the Parliament is concerned that the Cloud Act *"could have serious implications for the EU as it is far-reaching and creates potential conflict with the EU data protection laws."*
4. Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification : 1. de l'article 1334 du Code civil; 2. de l'article 16 du Code de commerce; 3. de la loi modifiée du 5 avril 1993 relative au secteur financier.
5. Prestataires de Services de Dématérialisation ou de Conservation
6. Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)