**European Parliament**
2014-2019

*Committee on Civil Liberties, Justice and Home Affairs*

1.4.2019

# 7th WORKING DOCUMENT

on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Enforcement of EPOC(-PR)s

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Birgit Sippel
Co-Author: Ignazio Corrao

## Introduction

This working document on the Commission Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters will deal with the issue of the enforcement of European Production Orders (EPOCs) and European Preservation Orders (EPOC-PRs). As such, it will focus on Article 13 on sanctions towards providers and on Article 9 deadlines given to service providers for executing EPOC(-PR)s. Finally, it will also analyse the enforcement procedure foreseen in Article 14 for cases in which the addressee does not comply with an EPOC(-PR) within the deadline without providing reasons accepted by the issuing authority.

## 1. Sanctions (Article 13)

Article 13 of the Commission proposal stipulates that "without prejudice to national laws which provide for the imposition of criminal sanctions, Member States shall lay down the rules on pecuniary sanctions applicable to infringements of the obligations pursuant to Articles 9, 10 and 11 of this Regulation and shall take all necessary measures to ensure that they are implemented. The pecuniary sanctions provided for shall be effective, proportionate and dissuasive. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them". Consequently, pecuniary sanctions are foreseen for service providers that are not executing an EPOC(-PR) or not respecting the imposed confidentiality obligations.[1]

Such sanctions would be determined and applied by the Member States, besides any additional national sanctions foreseen according to national instruments/national law. Thus, it would be upon the Member States to choose the sanctions which they believe to be the most appropriate, and best fit their respective systems.

In that regard, the Commission proposal, instead of foreseeing harmonised sanctioning rules for all Member States, basically refers to national law. The hybrid nature of the proposed instrument, which has already been touched upon in the second Working Document, is indeed not a full-fledged Regulation, as it cannot be directly applied, but would demand additional national transposition and supplementing legislative measures, thereby resembling more a Directive.[2]

Consequently, the question arises whether, in pursuit of effectiveness, some sort of harmonisation of the sanctioning regime would be required, at least in order to stipulate a mandatory minimum for all Member States. The question of a more harmonised sanctioning regime is also connected with the issue of possible "forum shopping". With Member States alone being responsible for determining and applying sanctions, there is a risk that the service providers would choose to appoint their legal representative in the Member states with the lowest sanctions. At the same time, some Member States might be inclined to keep sanctions as low as possible, in order to appear more attractive and appealing to service providers due to

[1] The issue has been already discussed in WD 2 on legal basis and WD 3 on service providers.
[2] Ibid.

the low sanctions applied.[3] Linked to the previous point, there is also a need to ensure a proper enforcement of the sanctions across Member States.

Consequently, in order to increase the fairness of the sanctioning system and to create a level playing field for all actors involved, sanctions would need to be dissuasive for all companies, regardless of their size. Following the same logic, the Council, in its General Approach, has changed the Commission proposal and introduced a sanctions regime equal to 2% of annual global turnover for companies that fail to disclose data.[4] However, here again, the question arises whether and in how far such a harmonisation of the sanctioning regime, whether in the form proposed by the Council or in another form, would be proportionate and in line with the current legal basis chosen for the proposed Regulation (Article 82(1) TFEU).

**2. Deadline for execution of EPOC (Article 9)**

The question of the appropriate system of sanctions is also heavily connected to the obligations imposed on the providers and their execution of EPOC(-PR)s. Article 9 of the proposed Regulation requires providers to transmit data to the issuing state "at the latest within 10 days upon receipt" of an EPOC, and "within 6 hours" in emergency cases.[5] It has already been argued in the third Working Document that these deadlines seem extremely ambitious. Even though, from a strictly technical point of view, they could possibly be met by big companies, these deadlines seem too ambitious taking into account that the proposed instrument also asks the service providers to assess the legitimacy of EPOCs before providing the data. The problem is even more evident when it comes to SMEs, or even micro enterprises, that might not run 24/7 services, but also for third country service providers, operating in different time-zones.[6]

Notwithstanding the much more general question of whether we should actually transfer the task of guaranteeing fundamental rights protection, until now a sovereign prerogative of state of authorities, to the service providers, already from a practical point of view it seems that the deadlines proposed are not realistic. Therefore, in order to ensure the fairness of any potential sanctions, two options seem to be plausible; either two separate deadline-regimes are introduced, one for the big companies and one for SMEs or, if decided to stick to a single regime for all, deadlines need to be longer than those set by the Commission in its proposal.

**3. Procedure for enforcement (Article 14)**

The Commission's proposal introduces a system whereby a judicial authority (prosecutor for subscriber and access data, and court for transactional and content data)[7] could directly request data from the service provider, or its legal representative within the Union, holding

[3] Problems with the issue of the "legal representative" for EU providers (not for third country providers) have ben already indicated in WD 6.
[4] It seems that the proposal is modelled on Article 83 of the GDPR on administrative fines. However, there the authority to impose such fines is the national supervisory authority and a much more detailed catalogue of different levels of infringements and criteria is provided.
[5] Article 9(1) and (2) of the proposed Regulation.
[6] See 3rd Working Document - Role of Service Providers
[7] The issue has been analysed in WD 2 on the legal basis and WD 6 on remedies and safeguards.

the data. Such a company can object to the request for data, either based on a number of refusal grounds included in Article 14, or because of a so-called conflict of laws with third country law, as defined in Articles 15 and 16. Since the review procedure regarding conflicting obligations with third country law have already been thoroughly analysed in the fourth Working Document, this Working Document will only focus on the grounds for refusal included in Article 14.

According to Article 14 of the Commission proposal, the service provider could oppose, both the EPOC and the EPOC-PR, only if - based on its own assessment - it believes that the conditions listed in paragraph 4, points (a) to (f) (EPOC)[8], and in paragraph 5, points (a) to (e) (EPOC-PR)[9] are fulfilled.

Beside the fact that is generally questionable to leave it to service providers alone (as private entities) to assess such grounds for refusal especially given that service providers will only receive limited information on the actual case via the EPOC(-PR) certificate, there is also a potential risk that service providers interpret these grounds for refusal too broadly. In such a situation, the authority of the Member State where this service provider sits would then need to decide whether or not to enforce the order (see Article 14, paragraph 6). For those service providers, that are aiming at appealing to clients that want to keep their data secure and, to this end, would embrace the possibility of potential sanctions, the current proposal might even create incentives for some bigger service providers to use this mechanism to their own benefit by aiming to oppose the execution of the EPOC-(PR) more often than other service providers.. This would, most likely, favour bigger service providers that are economically better off and have in house legal departments, or that rely on law firms capable of drafting oppositions. To avoid this, without providing a definite answer at this moment, several options could be envisaged:

1. Involving authorities of the state of enforcement (and, possibly, also the state of residence of the person concerned) at an earlier stage (i.e. at the same moment when the EPOC(-PR) is

[8] Those are the following:
(a) the European Production Order has not been issued or validated by an issuing authority as provided for in Article 4;
(b) the European Production Order has not been issued for an offence provided for by Article 5(4);
(c) the addressee could not comply with the EPOC because of de facto impossibility or force majeure, or because the EPOC contains manifest errors;
(d) the European Production Order does not concern data stored by or on behalf of the service provider at the time of receipt of EPOC;
(e) the service is not covered by this Regulation;
(f) based on the sole information contained in the EPOC, it is apparent that it manifestly violates the Charter or that it is manifestly abusive.

[9] Those are the following:
(a) the European Preservation Order has not been issued or validated by an issuing authority as specified in Article 4;
(b) the service provider could not comply with the EPOC-PR because of de facto impossibility or force majeure, or because the EPOC-PR contains manifest errors;
(c) the European Preservation Order does not concern data stored by or on behalf of the service provider at the time of the EPOC-PR;
(d) the service is not covered by the scope of the present Regulation;
(e) based on the sole information contained in the EPOC-PR, it is apparent that the EPOC-PR manifestly violates the Charter or is manifestly abusive.

issued and sent to the service provider), including the possibility of a meaningful notice, either with a positive confirmation possibility or a tacit negative confirmation possibility, by non-reacting in a certain time frame (depending on the different categories of data);

2. If the proposed Regulation was amended and would, indeed, foresee a stronger involvement of the state of enforcement (and, possibly, also the state of residence of the person concerned): Limiting the grounds to oppose the enforcement of the EPOC(-PR) for service providers, for example to orders issued by clearly non-judicial authorities, or to really limited, well-defined situations, such a solution would lead to the deletion of current paragraphs 4 and 5 respectively and would, thereby, also solve the concerns regarding the task of assessing the compliance of the EPOC(-PR) with fundamental rights, which is currently left to the service providers ; or

3. Including in the Production or Preservation Order's Certificates (EPOC or EPOC-PR) - sent to the service provider - a more detailed justification for the grounds for necessity and proportionality of the respective EPOC(-PR); without such information, it is rather doubtful whether the service provider would be able to properly assess the lawfulness of the request.

All these options are closely connected with the more general debate about mutual recognition in EU criminal law. The viewpoints on this issue vary substantially across Member States[10], national authorities, the Commission, CJEU[11], ECHR[12], scholars and practitioners,[13] and it becomes clear that the principle of mutual recognition is still under construction, closely connected to the changing nature of EU integration. Nevertheless, as has already been clarified by the CJEU, it is not an absolute principle that overrules the obligation of a Member State to protect fundamental rights. Consequently, at least a tacit non-recognition ground for serious violations of fundamental rights exists, which is not limited to "flagrant denial of justice", but encompasses all fundamental rights.[14]

**Conclusions**

The points addressed above - the question of sanctions, deadlines and the execution of EPOC(-PR)s - as well as the different options proposed will have to be further debated in the political process, in order to find a way to create an instrument which, on the one hand, helps

[10] This became clear in the debate on e-evidence whereby a group of Member states opposed to the Council general approach. Or the divergent views of the Member states in connection with the recent Council conclusions on mutual recognition in criminal matters (Council doc. 14540/18).
[11] See, for example, CJEU opinion 2/13, and later cases on fundamental rights exceptions in *Aranyosi and Căldăraru*, joined Cases C-404/15 and C-659/15 PPU, and *Minister for Justice and Equality v LM*, case C-216/18 PPU.
[12] There is a different approach between ECHR and CJEU on mutual recognition. See ECtHR, *Avotiņš v. Latvia,* a. no. 17502/07, judgment of 23 May 2016.
[13] *See, for example, A. Weyembergh, E. Sellier, Criminal procedural laws across the European* Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation, 2018, pp. 93-101.
[14] The CJEU did not follow in LM the advocate general proposal to limit it to the more narrow test on "flagrant denial of justice". Such test has been also refused by the co-legislators in the EIO Directive and Regulation (EU) 2018/1805 on the mutual recognition of freezing and confiscation orders.

to improve cross-border cooperation in criminal law, but on the other, is practically feasible and, most importantly, guarantees the protection of fundamental rights.