Council of the European Union
General Secretariat

Brussels, 18 September 2018

WK 10710/2018 INIT

LIMITE

CYBER
COPEN
JAI
DROIPEN
ENFOPOL
TELECOM
DAPIX
EJUSTICE
MI

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	German delegation
To:	Working Party on Judicial Cooperation in Criminal Matters (COPEN) (E-evidence)
Subject:	Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters - Additional safeguards into Articles 5 and 11 of the EPOC Regulation

Delegations will find attached a proposal from German delegation concerning the above mentioned subject.

Proposal by the Federal Republic of Germany to introduce additional safeguards into Articles 5 and 11 of the EPOC Regulation

During the COPEN negotiations on 19 and 20 July 2018, the Presidency asked Germany for a written proposal on additional safeguards to be introduced into Articles 5 and 11 of the EPOC Regulation.

Germany is pleased to present the requested text so that the negotiations can move forward. The minimum safeguards we consider necessary with regard to Articles 5 and 11 of the EPOC Regulation are evident from the additions we have made below. The cross-border investigative powers of law enforcement authorities on the basis of the EPOC Regulation need to be supplemented by additional safeguards, as uniform criminal law rules across Europe do not yet exist. In view of the complexity of the EPOC Regulation, Germany would like to expressly reserve the right to make amendments to other articles of the EPOC Regulation as well.

Article 5

Conditions for issuing a European Production Order

1. An issuing authority may only issue a European Production Order where the conditions set out in this Article are fulfilled.
2. The European Production Order shall be necessary and proportionate for the purpose of the proceedings referred to in Article 3 (2) and may only be issued if a similar measure would be available for the same criminal offence in a comparable domestic situation in the issuing State.

2a. A European Production Order may not be issued for data that is protected by immunities and privileges because the data

(a) pertains to the core area of private life of the person concerned;

(b) pertains to a client-attorney communication;

(c) was entrusted or became known to clergymen in their capacity as spritual advisor;

(d) has been confided to members of a parliament in their capacity as members of such bodies;

(e) pertains to a communication between a patient and a medical doctor, midwive, acreddited psychotherapist, pharmacist or dentist;

(f) is acquired or created for the purposes of journalism as long as it is controlled by the person who acquired or created it.

2b. A European Production Order may not be issued where it relates to a criminal offence which is alleged to have been committed outside the territory of the issuing State and wholly or partly on the territory of another Member State and is alleged to have no effect in the territory of the issuing Member State.

2c. A European Production Order may not be issued where it would be contrary to the principle of *ne bis in idem*.

3. **Notwithstanding paragraphs (2a) to (2c),** European Production Orders to produce subscriber data or access data may be issued for all criminal offences.

4. **Notwithstanding paragraphs (2a) to (2c),** European Production Orders to produce transactional data or content data may only be issued

(a) for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least ~~3~~ **5** years, or

(b) for the following offences, if they are wholly or partly committed by means of an information system:

– offences as defined in Articles 3, 4 and 5 of the Council Framework Decision 2001/413/JHA[1];

– offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council[2];

– offences as defined in Articles 3 to 8 of Directive 2013/40/EU, of the European Parliament and of the Council;

(c) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council[3].

5. The European Production Order shall include the following information:

(a) the issuing and, where applicable, the validating authority;

(b) the addressee of the European Production Order as referred to in Article 7;

(c) the persons whose data is being requested, except where the sole purpose of the order is to identify a person;

---

1 Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (OJ L 149, 2.6.2001, p. 1).

2 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

3 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

(d) the requested data category (subscriber data, access data, transactional data or content data);

(e) if applicable, the time range requested to be produced;

(f) the applicable provisions of the criminal law of the issuing State;

(g) in case of emergency or request for earlier disclosure, the reasons for it;

(h) in cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, a confirmation that the Order is made in accordance with paragraph 6;

(i) the grounds for the necessity and proportionality of the measure.

6. In cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, the European Production Order may only be addressed to the service provider where investigatory measures addressed to the company or the entity are not appropriate, in particular because they might jeopardise the investigation.

7. If the issuing authority has reasons to believe that **the European Production Order would be contrary to the provisions set out in paragraphs (2a) to (2c)**, ~~transactional or content data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed,~~ or its disclosure may impact fundamental interests of ~~that~~ **the** Member State **concerned** such as national security and defence, the issuing authority has to seek clarification before issuing the European Production Order, including by consulting the competent authorities of the Member State concerned, either directly or via Eurojust or the European Judicial Network. If the issuing authority finds that the requested ~~access, transactional or content~~ data is protected by **the provisions set out in paragraphs (2a) to (2c)** ~~such immunities and privileges~~ or its disclosure would impact fundamental interests of the other Member State, it shall not issue the European Production Order.

8. If – upon receipt and review of the requested data – the issuing authority has reasons to believe that the European Production Order was (fully or to a certain extent) issued or carried out contrary to the provisions set out in paragraph (2a), the issuing authority has to seek clarification before using the data, including by consulting the competent authorities of the Member State concerned, either directly or via Eurojust or the European Judicial Network. Data obtained contrary to the provisions set out in paragraph (2a) shall immediately be deleted. The fact of deletion shall be documented. Data obtained contrary to the provisions set out in paragraph (2a) shall not be used in criminal proceedings against the person concerned in the issuing state.

Article 11

Confidentiality and user information

1. Addressees and, if different, service providers ~~shall take the necessary measures to ensure the confidentiality of the EPOC or the EPOC-PR and of the data produced or preserved and where requested by the issuing authority,~~ shall refrain from informing the person whose data is being sought in order not to obstruct the relevant criminal proceedings.

2. ~~Where the issuing authority requested the addressee to refrain from informing the person whose data is being sought, t~~**T**he issuing authority shall inform the person whose data is being sought by the EPOC **or EPOC-PR** ~~without undue delay~~ **before the the data is produced or preserved** ~~about the data production~~. **If the requested data belongs to a communication between one or more persons any party to such communication shall be informed about the data request.** ~~This information may be delayed as long as necessary and proportionate to avoid obstructing the relevant criminal proceedings.~~

2a. If the identity of the persons concerned is unknown to the issuing authority, it shall inform the persons concerned as soon as their identity becomes known. Investigations to determine the identity of a person are to be carried out only if this appears necessary taking into account the degree of invasiveness of the measure in respect of the person concerned, the effort associated with establishing their identity, as well as the resulting detriment for such person or other persons.

2b. Information shall be dispensed with where overriding interests of an affected person that merit protection constitute an obstacle thereto. Information of a person who was not the target of the measure may be dispensed with if such person was only tangentially affected by the measure and it may be assumed that the person has no interest in being informed.

2c. The issuing authority the information set out in paragraph (2) if providing the information would endanger the purpose of the investigation or would be an imminent threat to life or physical integrity of a person or to significant assets as long as these grounds persist and for a maximum period of six month.

2d. With regard to traffic and content data the information may be delayed for a maximum period of six month. Any further delay of the information is only allowed for the aforementioned reasons and has to be approved by a court. Where the information is delayed, the reasons shall be documented on the file. Any further delay of the information is only allowed for the aforementioned reasons and has to be approved by a court. Where the information is delayed, the reasons shall be documented on the file.

3. When informing the person, the issuing authority shall include information about any available remedies **and their time limits** as referred to in Article 17.

Reasoning:

Regarding Article 5

Regarding paragraphs 2a and 8 (new)

In order to avoid such frictions in particularly sensitive areas, a European Production Order must not relate to data which are protected by the immunities and privileges specified in paragraph 2a. As regards such sensitive data, cross-border production should not take place without an assessment of the individual cases. For this reason, an EPOC should not be issued in respect of such data to begin with. The tools available under the Directive on the European Investigation Order remain unaffected, and provide a more cautious procedure for these particularly sensitive cases, which better reflects the interests and legal systems of the Member States involved or affected in a particular case.

However, since it will not be possible in each individual case to determine, prior to issuing an EPOC, whether this EPOC (at least also) covers data subject to the immunities and privileges set forth in paragraph 2a, the new paragraph 8 sets out the procedure to be followed if, upon receipt and review of the data, it turns out that these are (at least in part) subject to the immunities or privileges defined in paragraph 2a. In these cases where, upon review, there are reasons to believe that the data were (at least partly) obtained in contravention of paragraph 2a, the Member State concerned is to be consulted and the data obtained in contravention of paragraph 2a are to be deleted immediately. These data must not be used in criminal proceedings against the person concerned.

Regarding paragraph 2b (new)

The territoriality clause – which has been further simplified in comparison with previous legal instruments of the European Union – ensures that there is a sufficient link to the jurisdiction of the issuing Member State, while also ensuring that citizens in Europe who operate exclusively in their own legal system and whose offences do not have consequences beyond the borders of their own Member State are protected from criminal investigations from other European countries. This will not lead to investigative gaps. If deemed necessary by the investigating Member State, it may spontaneously inform the affected Member State and suggest an EPOC to this State.

Regarding paragraph 2c (new)

This provision incorporates the concept of *ne bis in idem*. If the purpose of an EPOC is to first establish whether or not there is a case of *ne bis in idem*, the procedure referred to in paragraph 7 becomes applicable.

Regarding Article 11

The proposals relating to Article 11 of the EPOC Regulation aim at providing adequate information to those affected by the measure – which is imperative if relief has to be sought – yet, at the same time, they give due regard to the interests of criminal prosecution. This is particularly true as regards the inclusion of provisions concerning the delay in providing information.

After all, data collection under the EPOC Regulation constitutes a severe interference with the right to respect for private life and the right to the protection of personal data (Articles 7 and 8 of the Charter). Interferences with these rights should be limited to what is strictly necessary (CJEU, Digital Rights, C-293/12 and C - 594/12, margin no. 52). It should furthermore be ensured that effective legal protection is available (Article 47 of the Charter). However, in order for legal protection to be effective, the person affected must be made aware of the interference. Thus, notification of the person affected is an essential element of any system of legal protection (as regards the importance of notification, see CJEU, C 203/15 and C 698/15, Tele2 Sverige AB, margin no. 121. Delays in informing the affected person should also be limited to what is strictly necessary. This might be the case where provision of the information would endanger the purpose of the investigation or pose a threat to the life or physical integrity of a person or to significant assets.

Since this provision of information is highly important for the entire system of legal protection, repeated delays should be subject to judicial review. This is because repeated delays in informing the person concerned pose a threat to the effectiveness of legal protection and should therefore require particular justification. In order to allow for a judicial review of the delay, it is essential that the reasons for this delay are documented.