Council of the European Union

Brussels, 3 August 2018
(OR. en)

11381/18

**Interinstitutional File: 2018/0108(COD)**

**LIMITE**

**COPEN 261**
**JAI 804**
**CYBER 165**
**DROIPEN 108**
**JAIEX 86**
**ENFOPOL 400**
**DAPIX 250**
**EJUSTICE 98**
**MI 550**
**TELECOM 233**
**DATAPROTECT 158**

**NOTE**

| | |
|---|---|
| From: | General Secretariat of the Council |
| To: | Delegations |
| 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 |

Delegations will find in the Annex some brief explanations on Articles 9, 10, 11, 14, 17 and 18 of the draft Regulation on European Production and Preservation Order as prepared by the Presidency together with some questions to foster the discussions during the COPEN (E-evidence) Working Party meeting on 5 and 6 September 2018.

**1. User information (Article 11) and effective remedies (Article 17)**

At the last COPEN WP meeting on 19 and20 July the Commission explained that access of LEA to data stored under the data retention law of the Member State where the service provider resides could not be excluded. Therefore, the requirements developed by ECJ (in particular in the combined cases of *Tele2, C-203/15,* and W*atson et al, C-698/15*) might have to be taken into account.

At that meeting some Member States expressed the wish to discuss the provisions of Articles 11 and 17 together. In addition, some Member States asked for discussions on the basis of different case studies. The Presidency would like to provide the following ones:

**1.1. Production Order case study**:

The Naples Prosecution Service is conducting an investigation into a perpetrator, **Anton**, an Austrian citizen residing in Italy, as well as some other unknown accomplices. It is assumed that Anton was producing and selling child pornography on the internet. In order to identify the unknown perpetrators a production order is issued to retrieve Anton's e-mail communications stored by gmail, the legal representative of which resides in France.

The communication reveals that **Bertrand**, a French citizen living in Brussels, was ordering child pornography and that Anton had been in contact with **Carlos** who was producing child pornography. According to the communication Carlos was acting under the orders of Anton. The identity of Carlos as well as his habitual residence is still unclear. Further investigations will be necessary.

Furthermore, Anton was also communicating with his daughter, **Dina**, about family matters and her plans to get married in the near future. Dina's residence cannot be established from the information sought from gmail.

Finally, Anton was also communicating with **Ellen** about a criminal procedure initiated against him because of drunk driving and speeding in Finland. It seems that Ellen will be defending Anton and it can be assumed that Ellen is a defence lawyer in Finland.

In accordance with the draft Regulation, all persons mentioned above (Anton, Bertrand, Carlos, Dina and Ellen) would be entitled to challenge the production order (Article 17(1) and (2)). Additionally, legal remedies would be available under Directive (EU) 2016/680 as well as Regulation (EU) 2016/679, whereby the legality of the order could be assessed incidentally.

**1.2. Preservation Order case study**:

The last communication between Anton and Carlos took place quite recently and it seems that Carlos was using GMX as an e-mail service. Therefore, the Italian prosecution service issues a preservation order to preserve the IP address with which Carlos logged on to his e-mail account at the time of the communication with Anton. The order is submitted to Germany where the legal representative of GMX resides.

According to the draft Regulation the measure could be challenged by remedies available under Directive (EU) 2016/680 as well as Regulation (EU) 2016/679. In that regard, also the legality of the measure could be revised – incidentally – by the competent data protection authority.

**Questions:**

The Presidency would like to invite delegations to exchange views, in particular with regard to the following questions:

- who should be entitled to challenge the measure in the cases mentioned above?
- who should be informed about the Production Order?
- should the accused be informed and entitled to challenge the Production Order irrespective of whether he/she was subject of the Production Order personally?
- if there is a need to limit the scope of the legal remedy (e.g. Dina could only be entitled to object that her communication will be part of the case file or to request that her communication is deleted since it did not provide any evidence)?
- should additional legal remedies regarding preservation orders be provided for in the draft Regulation?

Delegations are invited to make suggestions for improving the provisions of the draft Regulation where this seems appropriate with a view to the discussion on both case studies as described above.

**2. De facto impossibility (Article 9(4))**

Member States expressed some criticism during the latest discussions regarding the text of Article 9(4) finding the provision too broad or vague. The Presidency would like to seek delegations views on the following proposal for amendment of paragraph 4 of this Article and the text of an accompanying recital 41a:

***9 (4)*** *'If the addressee or, if different, the service provider, cannot comply with its obligation because ~~of force majeure or of de facto impossibility not attributable to the addressee or, if different the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC~~* ***the data were not retrievable at the time the order was received,*** *the addressee shall inform the issuing authority referred to in the EPOC without undue delay, explaining the reasons, using the Form set out in Annex III. ~~If the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC.~~'*

***Recital 41a****: 'The addressee or, if different, the service provider, should not be obliged to comply with the EPOC if the requested data were not retrievable at the time the order was received. Such reasons may, for example, exist in case of force majeure or in case the person whose data is sought is not the customer or the data had already been deleted before receiving the EPOC but not for the reason that the data storage has been outsourced.'*

**The Presidency would like to invite Member States to express their views on the proposed amendments in Article 9(4) and on the text of recital 41a. If the latter are not acceptable, the Presidency would like to encourage delegations to present their suggestions for improvement of the proposal. A similar solution would be used for Article 10(5).**

**3. Role of service providers (Articles 9(5) and 10(6))**

During the COPEN Working Party meetings some Member States requested clarifications regarding the scope of 'other reasons' envisaged in the text of Article 9(5) on the ground of which the service provider could refuse to comply with an EPOC. They also expressed some criticism regarding this provision when read together with paragraph 4 of the same article as providing an 'à la carte' menu for non-execution of the EPOC by the service providers.

A large number of Member States also voiced concerns regarding the task assigned to service providers by Article 9(5) which is in principle a task performed by the State (through its respective competent authorities). In particular this can be said when it comes to assessing a potential infringement of the Charter or whether an EPOC is manifestly abusive. Bearing in mind the limited information provided in the EPOC it seems questionable how such an assessment could be carried out.

Service providers have pointed out that according to Article 9(2) they would be obliged to comply with the order within six hours in emergency situations. However when a link is made between the obligations set in both paragraphs (2 and 5) it becomes questionable whether the service provide would be able to respect the deadline. According to the explanations provided by the Commission the grounds for non-compliance with the EPOC enumerated in Article 9(5) should only apply in very exceptional cases.

However in practice, it is likely that service providers will regularly carry out such an assessment and will lay down respective internal procedures before complying with the order. This will certainly have an impact on the timeframe within which service providers will be able to comply with the order, in particular if received outside the normal business hours. Such practice would be even more likely given the contractual liability of service providers towards their customers. Thus, a thorough assessment of an order would be a matter of fulfilling their liability obligations (cf. also recital 46 which reads that '*Notwithstanding their data protection obligations…*').

**The Presidency would like to invite delegations to discuss the way forward**:

A possible way forward could be to delete subparagraph 2 of Article 9(5).

Further legal certainty for service providers could be achieved by making clear that they have to comply with an order and would not be liable neither contractually or under the data protection rules. In that case a corresponding amendment of recital 46 would be necessary.

Furthermore, delegations are invited to present their suggestions for amendment of paragraphs 1 to 3 and 6.

**4. Preservation Order (Article 10)**

Although a similar measure is provided for by the Budapest Convention the Presidency would propose to keep the provision in the text of the draft Regulation. It offers more efficiency because of the possibility to cooperate directly with the respective service provider and because of the use of a standardised form.

Paragraph 1 states that the data should be preserved beyond the 60 days if the issuing authority confirms that the subsequent request for a production order has been launched. It was criticised by service providers that no further time limits apply and that storage of data is burdensome and expensive for them. In view of this, do Member States see a need to limit the maximum duration of the preservation? A possible solution could be to provide for a rather general rule that authorities should act expeditiously in order to keep the time limit for storage of data as short as possible.

Paragraph 5 of Article 10 should be aligned with Article 9(4).

**5. General questions with respect to the model proposed in Articles 9 and 14**:

The draft Regulation proposes a model that deviates from the 'traditional' mutual recognition instruments, particularly because it provides for a different role of the 'executing authority'. Therefore the Presidency would like to seek delegations' positions on whether the model as proposed in the draft Regulation, i.e. direct cooperation without involvement of an authority of another Member State (be it the Member State where the service provider from which data are sought is located or the Member State where the person concerned is located), could be maintained in general and used as basis for further discussion.

Those delegations that have some reservations regarding the proposed model are encouraged to express their views.

Some Member States voiced concerns regarding the grounds for 'refusal' mentioned under Article 14(4) and (5). What should be the role of the executing authority in the view of Member States?

Finally, the time frame of five working days (para 2) was criticised as being too short. The Presidency would like to postpone the discussion on this issue as long as more fundamental procedural questions have not been agreed upon in the Council. Nevertheless, delegations are invited to state their views about what they would deem to be a reasonable (minimum) time frame.

**6. Privileges and Immunities/ Protection of fundamental interests of another Member State (Article 5(7), 14 and 18)**

The draft Regulation envisages the protection of privileges and immunities in Articles 5(7), 14(2) and 18 and of fundamental interests of another MS such as national security interests and defence in Articles 5(7) and 14(2).

Therefore, the Presidency would like to invite delegations to express their views on the following questions:

1. Which jurisdiction do delegations consider should be envisaged for the protection of privileges and immunities as well as fundamental interests of another Member State? Currently the draft Regulation refers to the Member State where the service provider is addressed (see Article 5(7)) and to the law of the Member State where the addressee is residing (see Article 18).

   If delegations consider that an alternative approach should be taken, the Presidency would like to know whether a possible solution would be to refer to the law of the Member State where the person protected by privileges and immunities is residing (e.g. German law in the case of a German defence lawyer; French law for a French undercover agent)?
   In that case, who according to delegations should be empowered to invoke the privileges and immunities or fundamental interests of a Member State: the Member State or the person concerned (for both: involvement will only be possible from the moment it can be established who the person is and where the person resides)?

2. Additionally, the Presidency would like to highlight the fact that Article 5(7) refers to the law of the service provider that is addressed by an EPOC whereas Article 18 refers to the law of the "addressee". The Presidency would like to hear the views of Member States regarding this distinction.

3. With regard to Article 5(7) some Member States raised some difficulties for the issuing authority to establish in the specific case if privileges and immunities apply under the law of another Member State or if the specific person whose data are sought might be protected by privileges and immunities. This is even more the case where fundamental interests of another Member State are concerned. Delegations are invited to present their views on possible improvements of the text.

4. Could/should any other safeguards be envisaged to ensure the protection of privileges and immunities or fundamental interests of another Member State?