Council of the European Union
General Secretariat

Brussels, 09 November 2018

WK 13576/2018 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.

NOTE

From:	EJN
To:	Working Party on Judicial Cooperation in Criminal Matters (COPEN) (E-evidence)
Subject:	Conclusions of the EJN e-Evidence Working Group on the proposals for a Production and Preservation Order and Appointment of a legal representative

Delegations will find attached the above mentioned document.

Conclusions of the EJN e-Evidence Working Group on the proposals for a Production and Preservation Order and Appointment of a legal representative

Background

Crime leaves digital traces which are essential for criminal investigations and prosecutions. Therefore obtaining electronic evidence (e-Evidence) and harmonising the applicable proceedings is a key step for prosecutors and law enforcement authorities to be able to gather all available evidence and bring criminals to justice.

The European Judicial Network (EJN) recognizes that improving the current legal framework and procedures to obtain e-Evidence within the European Union and in relation to non-EU countries is central for all kind of investigations, particularly for serious crimes.

EJN e-Evidence Working Group

At the 50th Plenary Meeting of the EJN commemorating its 20th Anniversary, the European Union Institutions and the Contact Points concluded that **feedback from the EJN, both on proposals for legal instruments and the practical application of them is invaluable**. The EJN Contacts Points deal with judicial cooperation in criminal matters on a daily basis and they are experts in this area.

In order for the EJN to provide feedback on the proposals for a Regulation on a European Production Order and a European Preservation Order and a Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings the EJN recently established a Working Group on e-Evidence. The Working Group met on 17 September and discussed the proposals from the perspective of **the practical application of them** – will it work in practice? The EJN Conclusions from this meeting is presented below. The EJN Working Group will continue to follow the further developments of the proposed instruments and is willing to give its further input to the text. The EJN Working Group will also give its feedback on the Annexes to the Regulation, when timely.

EUROPEAN JUDICIAL NETWORK
20 YEARS OF BUILDING MUTUAL TRUST

Conclusions

1. Overall assessment of the proposed new instruments

The EJN Working Group members agreed that the proposed instruments for the gathering of cross-border electronic evidence would be an improvement to the current procedures in place. Since a large part of e-Evidence are required from online service providers based in other jurisdictions, particularly in the United States, there is a need for a new set of rules, establishing a standardised mechanism and clear procedures for obtaining e-Evidence directly from service providers.

The new legal instruments should be consistent and allow for a coherent functioning of the current legal framework such as the Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO); the 2000-Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union; bilateral agreements including those reached under the Cloud Act and the Council of Europe's Budapest Convention on Cybercrime (Budapest Convention). Hence, the aim of these legal instruments should be to complete and complement the current EU/international legal framework.

On that note, the proposed Regulation should not affect the already existing channels for cooperation between judicial authorities and law enforcement authorities and direct cooperation with service providers. For instance, existing mechanisms empowering law enforcement to request/obtain subscriber data from service providers should not be restricted or replaced by the proposed new instruments.

2. Data categories

The data categories (subscriber data, access data, transactional data, and content data) are in line with the current practice established in the United States. Although it provides the additional category of "access data" compared to the Budapest Convention, practitioners are in general used to differentiate and use both mechanisms for cooperation. Furthermore, it is essential that access data, which only aims to identify the user, is subject to the same regime as subscriber data.

3. Deadlines for transmitting the data (Regulation Art.9)

The timeframe proposed in the Regulation to obtain the data is welcomed. In particular the 6 hours deadline in emergency cases is a great advantage for investigations of serious threats that would require prompt access to the information.

4. Competent issuing authorities (Regulation Art.4)

The competent issuing authorities as proposed in Article 4 in the Regulation are not in alignment with the EIO framework or other existing procedures. It would be a great disadvantage for the efficiency if the authorities that are currently competent to request data would not be competent for issuing the production or preservation order, e.g. to exclude a prosecutor from issuing (or validating) a production order regarding transactional and content data. It should also be possible for the Police in urgent cases to issue a preservation order that is validated within a shorter period of time after the preservation has taken place. If there are concerns regarding the legal basis in Article 82 of the TFEU, this matter could be mentioned in the recitals.

Hence, each Member State should have the possibility, like for other instruments, to decide on the competent issuing authorities in order to create consistency with their national legal system.

5. Threshold for issuing a Production Order (Regulation Art.5)

The EJN is of the opinion that the proposed Article 5(2) which provides that "The European Production Order shall be necessary and proportionate…. 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" is a sufficient "threshold", also in relation to transactional data and content data. There are examples of less serious crimes that nevertheless could have a considerable impact on the society, such as non-aggravated fraud or stalking, where the production order may be the only way to retrieve the necessary evidence.

6. Definition of "addressee"

The use of the term "addressee" in the Regulation should be considered. In Article 7 it is stated that a European Production Order or a European Preservation Order should be sent to the Legal representative, the "addressee" (or in certain situations to any establishment of the service Provider in the Union). But in all other Articles, "addressee" seems to indicate the tasks and obligations of the Service provider, which is taken care of by the Legal representative. Hence, in the respective Article the term addressee seems to include both the role of the legal representative as well as the responsibility of the service provider, which makes the relations between them unclear. Hence, when the text concern the duties of the Service Provider it would be better to refer directly to the Service Provider and not to the "addressee".[1]

[1] For Instance Article 8(5); Article 9; Article 10; Article 14 (1.1) (4 to 6) (9) and (10); Article 15 (1) and Article 16 (1) of the [1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters)

7. Conflict of interest and Legal Representatives

A possible conflict of interest can occur if the legal representative represents both the service provider and the person that is being investigated/whose data is being sought. Clear conditions should be established to prevent any breach of confidentiality during the investigation.

8. Role of the Legal representative/Service Provider (Regulation Art.9, Art.14 and Art.15)

For the practical functioning of the proposed new procedure, it is important to have a clearly defined and limited role of the legal representative/service provider, focused on what can reasonable be requested of them. Thus, the legal representative/service provider should only have the role of checking if the order is correct to its content and form and the service provider is covered by the Regulation, and whether or not it is possible to provide the data that is requested, i.e. if it is available (as described in Articles 9(3) and 9(4)). In any case, where the reasoning for not complying to the order refers to "other reasons" in Article 9(5) Para 1, this term should be deleted, since it would give complete discretion to the service providers to comply or not comply with the order.

It is clear that the protection of fundamental rights must be ensured. It does not seem realistic and reasonable though that the service provider, through the legal representative, should have the responsibility for checking possible manifest violations of the Charter of Fundamental Rights of the EU or that the order is abusive as prescribed in Article 9(5) Para 2 of the draft Regulation. This is a task that should be kept within the Member States. Therefore, based on the principle of mutual trust and mutual recognition, the issuing authorities of each Member States should have the responsibility of assessing the legality of the orders and providing the necessary legal remedies to ensure that EU citizens are duly protected. The question is also how much information from the investigation in the issuing state that can be revealed to the legal representative, due to the confidentiality issue, on the one hand and how much information this legal representative would need to perform this checking task on the other hand.

If the EU-legislator would not deem it enough to assign the role of checking the compliance with the Charter only to the issuing authority, it could be considered to introduce a role for the enforcing Member State for the most sensitive data categories. However, it is important that such a role does not imply that the authority in the enforcing Member State becomes an "ordinary" executing authority. Little would have been gained by such a system. Hence, if such a role for an authority in the enforcing Member State is introduced, it could only be in the form of a notification that the order is sent to the legal representative. The notified authority would have to react within a short period of time and the notification should not have a suspending effect in relation to the obligations of the legal representative/service provider. In addition, the introduction of a notification system is a far better alternative than what is foreseen in Article5(7), as regards possible immunities and privileges related to the receiving Member State.

It must also be borne in mind that the legal representative may be designated in any of the Member States of the EU where the service provider is offering its services. Thus, the link between the Member State where the legal representative is designated and the data sought might vary considerably. It is not at all evident that the enforcing Member State would be in a better position than the issuing Member State to do the assessment of all relevant interests.

The procedure for enforcement as provided for in Article 14 is a necessary part of the procedure. The issuing authority must be able to seek assistance from an authority in the receiving State in case of non-compliance by the legal representative/service provider. Nevertheless, it would seem more logic to align/merge the conditions for non-compliance in the respective Article 9 and Article 14 into one Article.

As for the language regime, it would be highly desirable for the efficiency and speediness of the procedure that English would be used.

9. Designation of the Legal Representative

In order to avoid "forum shopping" when choosing where to designate the legal representative, the conditions for the service providers should be similar in the different Member States. Hence, it would be advisable to establish harmonisation on the sanctions for delays or unreasoned refusal to give execution to the orders; the minimum time for the preservation of the data and in general the rules and requirements that could affect the choices of where to designate the legal representative.

10. Notification of the person whose data is being sought (Regulation Art.11) and Legal Remedies (Regulation Art.17)

It should be clarified who shall be informed of that data has been sought. The EJN is of the opinion that an excessive system of notifications must be avoided. In this respect the use of "whose data is being sought" in Article 11 is too wide. Normally it should be enough to inform the suspect/accused, since a broad notification could have a negative effect on ongoing criminal investigations and be very burdensome for the issuing authority.

As for legal remedies concerning the production order, these should be concentrated to the issuing state, regardless of the category of the individual. There should be no legal remedies against the preservation order.

11. Speciality principle

The principle of speciality should not be applied and this should be made clear in the Regulation. First, the specialty principle traditionally applies in cases of extradition/surrender, where a person is moved from one state to another by force. In those cases the suspect is protected from being prosecuted for other crimes not mentioned in the request for extradition/EAW. The production order and the preservation order, on the other hand, are investigative measures and the same protection as for extradition cases does not seem motivated. Second, the speciality principle would not make much of a difference since the room for non-compliance is limited. For instance, there is no requirement of double criminality, which is one of the main reasons for upholding the principle.

12. Real time interception of data in cross-border cases & direct access to e-Evidence

The EJN agrees that real-time interception of data and direct access to e-Evidence are both very valuable investigative measures. However, including them in the scope of the European Production Order and the European Preservation Order, which are instruments for direct cooperation with Service Providers, raises additional questions and therefore they should not be included.