EUROPEAN CRIMINAL BAR ASSOCIATION

An association of European defence lawyers

ECBA OPINION ON EUROPEAN COMMISSION PROPOSALS FOR: (1) A REGULATION ON EUROPEAN PRODUCTION AND PRESERVATION ORDERS FOR ELECTRONIC EVIDENCE & (2) A DIRECTIVE FOR HARMONSIED RULES ON THE APPOINTMENT OF LEGAL REPRESENTATIVES FOR THE PURPOSE OF GATHERING EVIDENCE IN CRIMINAL PROCEEDINGS

Rapporteurs:

Stefanie Schott (Germany)

Julian Hayes (United Kingdom)

A. Introduction

On 17 April 2018, the European Commission adopted a proposal for a Regulation on European Production Orders ('EPO') and European Preservation Orders ('EPrO') for electronic evidence in criminal matters[1] and an accompanying proposal for a Directive laying down common rules on the appointment of representatives for the purpose of collecting evidence in criminal proceedings.[2]

The stated intention behind the proposals for EPOs and EPrOs is to overcome inefficiencies in the co-operation between entities providing electronic communication services ("service providers") and public authorities, to expedite the provision of electronic data in investigations and prosecutions, and to provide legal certainty of cross border investigative measures.

The overall effect of the proposals would be that the law enforcement authorities of a Member State would have the power to oblige service providers in another Member State to disclose electronic data

[1] (COM (2018) 225 final).
[2] (COM (2018) 226 final).

directly to them within relatively short time frames, without the involvement of the authorities of the state in which the EPO and EPrO is to take effect ('the enforcing State'). Further under the proposals, EPOs and EPrOs could be addressed to service providers offering services in the EU irrespective of whether they were actually based in the Union or whether the data sought was located within the EU or in a third country.

B. Summary view of ECBA

Given the increasingly transnational nature of criminal activity, particularly where cyber-crime is concerned, the ECBA recognises the importance of electronic evidence in criminal investigations and prosecutions. The ECBA also recognises the need for the expedition of cross-border access to stored electronic data by law enforcement authorities.

However, the proposals have been introduced without consideration of the question as to whether existing cross-border cooperation measures – like the European Investigation Orders - are effective or could be improved to achieve the same desired outcome.

In their current form, the ECBA has grave reservations about the proposals and believes that, in trying to achieve a laudable objective, they have been introduced without consideration of whether existing cross-border co-operation measures are effective or could be improved to achieve the same end. It is uncertain that the legal basis claimed for introducing the proposals is sound and they erode safeguards against abuse, thereby jeopardising the rights of citizens. The proposals inherently jeopardise the protection of legally privileged material, allow for disproportionate requests for electronic data, provide inadequate protection for the *ne bis in idem* principle and risk conflict with the European General Data Protection Regulation ("GDPR") which provides minimum standards expected of all states when processing personal data. The ECBA recommends the addition of specific safeguards which might, in the longer term, form the basis for wider international co-operation in the sharing of electronic evidence with law enforcement authorities outside the EU.

C. Specific concerns

The ECBA has the following specific concerns about the proposals for EPOs and EPrOs.

I. Are the proposals necessary?

The Commission envisages that existing measures on which law enforcement authorities currently rely (Mutual Legal Assistance Treaties ('MLATs') and the European Investigation Orders ('EIOs')) will continue to exist but that the EPO and EPrO proposals will provide a "fast track" alternative for electronic evidence. However, it is not clear what consideration has been given as to how Mutual Legal Assistance and EIOs could be improved by way of alternative. The ECBA believes that, before the proposals are implemented, a proper evaluation should take place of existing measures to understand whether they can be or need to be improved.

In particular, the ECBA suggests that the Directive on EIOs[3], with the safeguards which it contains, might be amended to include additional complementary measures concerning electronic evidence. The implementation period for EIOs only expired on 22 May 2017[4] and the measure is due to be evaluated by 21 May 2019 in any event.[5] At the very least, the ECBA believes it would be prudent to delay implementation of the EPO and EPrO proposals until this evaluation has been undertaken in order to avoid introducing possible weaknesses within the framework of the new proposals. In that regard, the ECBA welcomes indications by the Parliament that it is unlikely that the proposals will be put to a vote before the European Parliamentary elections in May 2019 and that, in the meantime, further analysis and consultation will be undertaken.

[3] Directive 2014/41/EU of the European Parliament and oft he Council of 3 April 2014 regarding the European Investigation Order in criminal matters.
[4] (Article 35 (1) Directive 2014/41 / EU).
[5] Art 37 of the EIO Directive.
*1 GDPR, Article 2(2)(d).

II. Legal basis for EPOs & EPrOs & means of rreview in enforcing State

The legal basis for the proposed regulation is that of judicial co-operation in criminal matters as set out in Article 82(1) of the Treaty on the Functioning of the European Union ('TFEU').

However, the proposals provide for direct access by foreign investigative authorities to service providers operating in an EU Member State. In other words, rather than the mutual recognition of judicial decisions envisaged by Article 82(1) of TFEU, under the proposals access would be given directly to the electronic data held by private natural and legal persons. Service providers would be required to comply without prior review of the lawfulness of an EPO and EPrO under the law of the enforcing State.

The proposals would therefore provide for the direct and unilateral execution of both administrative and judicial orders in another Member State. Since the proposals offer limited opportunity to challenge an EPO or EPrO, the ECBA regards them as a far-reaching and disproportionate interference with the sovereignty of individual Member States and the rights of the individual citizens affected.

The ECBA understands that a time-consuming domestic process before an EPO or and EPrO is executed would risk the loss of data which is potentially valuable to an investigation or prosecution. However, this neither justifies the abandonment of the sovereignty of Member States to execute the law in their respective territories and to grant fundamental rights to all subjects within their territories, nor the abrogation of protections afforded to the rights of individuals. A more proportionate encroachment on these would be to allow the temporary deployment of EPrOs, to preserve the data sought, pending – without limitation to specific circumstances – an expedited judicial or regulatory process in the enforcing State to consider whether an EPO was justified. Specific exceptions might be included for particularly important and urgent cases.

Experience of European Arrest Warrants shows that residual control is essential in the enforcing State to safeguard the rule of law and provide adequate protection for fundamental rights under the European Charter of Fundamental Rights as well as under the European Convention on Human Rights, including the protection of human dignity and protection of the right to a private life. As currently drafted, however,

the proposals open up the possibility that they may be used unscrupulously for political or commercial competitive reasons.

The desirability for a review mechanism for EPOs in the enforcing State is particularly important where they seek content and transaction data, and the ECBA suggests that the grounds for non-recognition or non-execution of EIOs set out in Art. 11 of Directive 2014/41/EU might usefully be introduced to the proposals. The necessity of a proper review by the enforcing State becomes even more important because the confidentiality provision in draft Article 11 generally prevents a service provider from informing the person whose data is being sought of the existence of the EPO and EPrO.

It might be possible to devise a central European body to review EPOs and EPrOs before they become individually effective. Such a body may even, in the longer term, facilitate agreements for the sharing of electronic data with non-EU states. However, the ECBA acknowledges that the creation of such a body would be time-consuming and potentially expensive. The most effective means of assuaging concern about improperly motivated EPOs and EPrOs would be to allow judicial control in the enforcing State.

If the introduction of judicial control in the enforcing State or at European level is deemed unacceptable, the ECBA suggests that there at least be a general requirement to notify the enforcing State along the lines of the notification requirement in Article 31 of Directive 2014/41/EU. The competent authority of the enforcing State should be informed before or at the same time as the EPO or EPrO is issued, allowing the competent authority of the enforcing State to object within a certain period of time on the grounds that the measure would not be approved in a comparable domestic case. The notification should have suspensive effect on the obligations of the addressee who might nevertheless be obliged to preserve the data until confirmation is obtained. Exceptions might exist for urgent and important cases, as far as necessary. In this respect too, grounds for non-recognition or non-execution of EIOs set out in Article 11(1) Directive 2014/41/EU could be used as a precedent.

III. No effective review or remedies

As set out below, the risk of fundamental rights violations associated with the lack of judicial oversight of incoming orders in the enforcing State is further aggravated by the fact that the proposals provide very limited opportunity for service providers affected by an EPO or EPrO to challenge such orders.

1. Challenge on grounds of manifest violation of Charter rights

Draft Article 14(4) and (5) of the proposals set out the grounds on which service providers may challenge EPOs and EPrOs, including the ground that the order has not been issued or validated by an issuing authority, because it contains manifest errors or because it would be impossible to comply. Ostensibly, the grounds also include that the EPO or EPrO manifestly violate EU Charter rights. However, the appetite and ability of a service provider to mount a challenge on the grounds of a breach of fundamental rights would be, in practice, be very limited. This is because, as drafted, the proposals limit the information available to service providers which would enable them to recognise that Charter rights were in jeopardy.

As currently envisaged, when an issuing authority grants an order, it would be communicated to the relevant service provider by means of a Certificate.[6] The Certificate must contain specific information,[7] including the name of the issuing authority, the person whose data is being requested, the requested data category, any specific time range for which the data is requested, the applicable criminal provision in the issuing state and any grounds for urgency / expedition. However, the grounds for the necessity or proportionality of the order, and further details about the investigation are expressly excluded from the Certificate.[8] Thus, service providers would be deprived of the very information necessary for them to establish that an individual's Charter rights would be violated by the order. The ECBA can see no justifiable reason to withhold from service providers the essential information that would enable them to guard against the abuse of Charter rights, particularly where the proposals provide for the confidentiality

[6] An EPO Certificate (EPOC) or an EPrO Certificate (EPOC-PR).
[7] Draft Articles 8(3) & (4) and draft Article 5.
[8] Draft Article 8(3) & (4).

of EPOs and EPrOs which would overcome any concern about jeopardy risked to an investigation were such information provided.[9]

In the ECBA's view, at the very least, service providers should have the means of challenging an EPO or EPrO whenever it is evidently unlawful. Article 11(a)-(h) of Directive 2014/41 which provides appropriate grounds on which an executing state may refuse to recognise or execute an EIO, provides a useful precedent for the way in which safeguards may be built into the proposals for EPOs and EPrOs. However, in order to ensure that such safeguards are effective, service providers must be given all of the information listed in draft Articles 5(5) and 6(3).

2. Limited right of appeal by the individual concerned

The proposals specifically allow for remedies for the individuals whose data are sought by means of EPOs and EPrOs.[10] However, the regulation is silent as to what these remedies should look like. Further, it does not provide for the standardisation of remedies against the EPOs and EPrOs. Instead, the remedy is left to the national law of the Member State for the exercise of rights of appeal. Suspects and accused persons would have such rights during criminal proceedings, and those who are not themselves suspects but whose data has been obtained by means of an EPO "shall have the right to effective remedies". As envisaged, such remedies would be exercised in the Courts of the issuing State. The ECBA is disappointed that the regulation focuses heavily on obtaining access to data but fails to devote similar attention to the protection of the rights of individuals.

However, even more disappointing is that the proposals do not envisage that individuals would have any opportunity to seek a remedy against the order in the enforcing State. As mentioned above, the proposals state that, where requested, service providers "shall refrain from informing the person whose data is being sought" to avoid obstructing criminal proceedings. [11]As a result, individual data subjects affected by EPOs and EPrOs would be deprived of the opportunity to supplement any arguments raised by service providers against execution of the order. To act as a deterrent against the

[9] Draft Article 11.
[10] Draft Article 17.
[11] Draft Article 11

abuse of the rights of individuals by issuing States and to go some way to redressing the imbalance caused by an individual's inability to seek a remedy in the enforcing state, the ECBA suggests that data which has been obtained in violation of fundamental rights should automatically be excluded and deleted.

3. Conclusion

The consequence is that as the proposals are currently structured, there is no one – whether the service provider, the institution in the enforcing State on whom the order is served, or the affected individual – who could take any effective steps to challenge an illegal order before the data is released.

IV. Insufficient protection of privileged data

At first sight, the proposals appear to protect transactional and content data containing privileged material. Thus, if the issuing authority has reason to believe that such data is protected by immunities and privileges granted under the laws of the enforcing State, before issuing the order, the issuing authority must seek clarification, including by consulting the competent authorities of the enforcing State concerned.[12]

However, as set out, the consultation obligation only arises where the issuing authority "has reason to believe" that such protection arises. In circumstances where there is no common definition of what may amount to privileged material, it may not be immediately apparent to the issuing authority that any issue arises in the enforcing State

Even where the issuing State does have reason to believe the material sought may be privileged and its consultation obligation arises, the proposals are silent on the nature of the consultation exercise required beyond "seeking clarification" and the issuing state remains the ultimate arbiter of whether the data is protected by privilege or immunities under the laws of the enforcing State. The proposals make

[12] Draft Article 5(7).

no provision for a dispute resolution mechanism in the event that the issuing and enforcing State reach different conclusions.

Even where the issuing State does consult the enforcing State on the data sought and follows its advice, there is no guarantee that either the enforcing or issuing State (or indeed the relevant service provider) would be in a position to determine whether the particular data sought was privileged without additional information from the particular data subject concerned (e.g. whether particular communications had taken place between a data subject and a lawyer engaged to provide advice to him/her). Since the data subject is unlikely to be informed of the existence of the order, the proposals include an inherent risk that the issuing State will inadvertently obtain materials which are protected by immunities and privileges.

With regard to subscriber and access data, there is generally no judicial review under the proposals, although these data might also be covered by immunities and privileges.

The protection of particularly sensitive data depends solely on a careful examination and the correct classification of the data by the issuing authority. The ECBA does not regard this as adequate protection for this type of data and recommends that it be examined by a court or an authority in the enforcing State before the order is executed by the service provider. The ECBA believes the proposals should be amended to require that breach of immunities or privileges in relation to sensitive data should give rise to automatic exclusion of sensitive data from any subsequent proceedings and to its deletion in the hands of the issuing State.

V. Lack of proportionality & excessive territorial scope of EPOs

1. Lack of proportionality

While the promotional documentation accompanying the proposals exemplifies the Commission's arguments in favour of EPOs by reference to how the measures might assist in the fight against terrorism and child sexual abuse, the proposals themselves are not in fact restricted to such serious offences.

Rather, they envisage differing threshold conditions for the issue of EPOs, depending on the nature of the data sought. EPOs may be issued for subscriber and access data for all criminal offences, whereas they may only be sought for transactional or content data where the offence carries a maximum custodial sentence of three years or more.[13]

However, since there is no harmonisation of criminal sentencing across the EU, a particular offence enabling the issue of an EPO in one Member State may be insufficient for the issue of one in another. The use of maximum sentences as a threshold condition for the issue of EPOs therefore risks creating uncertainty because of the lack of harmonisation in sentencing practice between Member States.

Further, the proposals contain no requirement of dual criminality which would require that, for an EPO to be enforceable, the suspected offence would also be an offence in the enforcing State had it occurred there. As currently drafted, therefore, the proposals would risk the issue of EPOs for trivial or "political" offences.

To overcome these difficulties, and to avoid the disproportionate issue of EPOs, the ECBA urges the Commission to specify a list of serious offences for which EPOs would be available rather than including a maximum sentence as a threshold condition. In addition, the ECBA urges the Commission to include dual criminality as one of the threshold conditions for the issue of such orders.

2. Excessive territorial scope

As currently drafted, the proposals would permit the issue of EPOs by any Member State against service providers "established" or "represented" or "offering services" within the European Union. In other words, there is no requirement that an offence has been committed within the jurisdiction of the issuing State. Theoretically, therefore, Member State 'A' could issue an EPO in respect of an individual without there being any nexus to it, whether by virtue of the location of the data, the location or nationality of the individual suspect, or the place where the suspected offence took place. Without there being a requirement for some form of connection with the issuing state, the proposals risk that parallel

[13] Draft Article 5(3) & (4).

investigations / proceedings may take place in respect of the same suspect and for the same offence. Because of the breadth of the application, an issuing State would be able to target an EPO at whichever Member State has the least stringent laws on data transfer/professional privilege/fundamental rights.

Drawing on the precedent of Directive 2014/41/EU,[14] the ECBA urges that the proposals be amended to allow as potential grounds for refusing to comply that the EPO: (i) relates to an offence which took place outside the issuing state and wholly or partially on the territory of the enforcing State; and/or (ii) the execution would be contrary to the principle of '*ne bis in idem'*.

Further, where a service provider operates in multiple jurisdictions across the EU, there is a risk that issuing States may target EPOs at such service providers in Member States where protections for privilege and/or fundamental rights are perceived to be lower, or where the service provider's resources are more limited, as a means of maximising the capture of evidence. To overcome this risk, the Commission should consider amending the proposals to include a requirement for the issue of an EPO for law enforcement in the issuing state to demonstrate that the offence under investigation has some connection with the proposed enforcing State.

VI. Data minimisation

The GDPR enshrines the principle of data minimisation, whereby the processing of personal data must be adequate, relevant and limited to what is necessary.[15] With this in mind, the ECBA notes that the EPO and EPrO proposals omit to include a similar requirement. For example, EPOs shall include the time range over which the data is required but only "if applicable".[16] Similarly, while EPrOs contain a provision that data preservation "shall cease after 60 days", this is subject to the qualification that it may be held beyond the 60 day point where the issuing authority confirms that a subsequent request for an EPO has been launched.[17] However, the stage at which the issuing authority must inform the service provider that continued preservation of the data is no longer required is vague. The issuing authority

[14] Article11(1)(d) & (e).
[15] GDPR, Article 5(1)(c).
[16] Draft Article 5(5)(e).
[17] Draft Article 10(2).

must provide such notification "without undue delay".[18] In such situations, service providers will potentially find themselves subject to conflicting GDPR and EPrO obligations, which places them in an invidious position and in practice is likely to lead to the retention of data longer than is necessary.

To overcome the problems outlined above, the ECBA urges that draft Article 5(5)(e) is amended to mandate the specification of a particular period of time for which data is sought. Further, the ECBA urges a time limit for the issue of an EPO following the issue of an EPrO in respect of the same data.[19]

VII. Non-compliance with EPO on basis of conflict with laws of third country

Where service providers consider that compliance with an EPO would conflict with the applicable laws of a third country, then, as currently drafted, the service provider must provide the issuing authority with its reasons for not executing the order.[20] Where the issuing authority intends to uphold the EPO notwithstanding the service provider's objection, it must first request a review by a competent court in the jurisdiction of the issuing state. That competent court then determines whether a conflict with the third country law actually exists and, if so, whether or not to uphold the EPO.[21]

The ECBA foresees several problems with the proposals as drafted. First, they place on the service provider the onus of giving reasoned objections to justify non-compliance with an EPO based on conflict with the laws of a third country. Service providers will therefore carry a responsibility which they may be unwilling or ill-equipped to discharge. Where service providers operate commercially in the issuing state, they risk being placed in a conflicted situation by such obligations. This could indirectly jeopardise the rights of individuals within the relevant third jurisdiction.

The second problem with the proposals is that, where a potential conflict arises between compliance with an EPO and the laws of a third country, as currently envisaged, it is the courts of the issuing state which determine whether the conflict exists. Since it is quite possible that the court making the

[18] Draft Article 10(3).
[19] Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters – adopted 26 September 2018
[20] Draft Articles 15 & 16.
[21] Draft Articles 15(3)-(5) & 16(3)-(5).

determination will be the same court which originally issued the EPO, there is a risk that the court will be more inclined to find that there is no conflict. Putting that aside, however, the procedure proposed for determining the conflict requires a court in the issuing jurisdiction to adjudicate on the laws of a third country, a task which it is unlikely to be well placed to undertake.

The third problem with the proposals is that, under draft Article 15(4), where a competent court in the issuing state is asked to determine whether a conflict with the laws of a third country has arisen, the court may take into account whether the third country law is protecting fundamental rights or interests, or "manifestly seeks to protect other interests or is being aimed to shield illegal activities from law enforcement requests in the context of criminal investigations."[22] Such a finding, if one were made, would have potentially dramatic consequences for international law and the comity of the relevant nations.

To overcome these problems, the ECBA urges that the proposals be amended in the following ways. If service providers are to remain the "gatekeeper" for the protection of individual rights under third country laws, the proposals should include a specific provision to that effect. In addition, to facilitate that role, specific provision should be made to assist service providers with the increased regulatory burden imposed on them by providing reimbursement for the reasonable expenses involved in complying with an EPO or EPrO.

With regard to the determination of conflicts between EPOs and third country laws, the ECBA suggests that, where a conflict appears to arise, the issuing state's competent court should be required to engage with the enforcing State's central authority at an early stage of the determination process, rather than engaging with them only once an initial determination has been made.[23]

Finally, to demonstrate respect for the laws of third countries and avoid potentially damaging disputes arising, the ECBA recommends that draft Article 15(4) be deleted.

[22] Draft Article 15(4).
[23] Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters – adopted 26 September 2018.

D. Conclusion

The ECBA is greatly concerned that, in the current form, the proposals represent a very significant erosion of the fundamental rights of citizens and sees no urgent need for them when other mechanisms already exist for achieving the same objectives.

The Proposal recognises that a high level of mutual trust is an essential precondition for the proper functioning of the instrument. The ECBA is of the view that the Commission should learn from the lessons learned over the 15 years since the Framework Decision on the EAW (another instrument which required a high degree of mutual trust in order to function properly) was implemented, and ensure proper safeguards at the outset.

As a minimum the ECBA urges the Commission to adopt the following recommendations:-

1. In all cases, prior to the issuing of transaction and content data, a judicial procedure must take place in the enforcing State to ensure the lawfulness of the order in accordance with the matters listed in Article 11 (1) of Directive 2014/41/EU (that execution of the order would transgress the laws of the enforcing State, etc) thus ensuring compliance with minimum legal standards. To carry out this exercise, the enforcing State must be provided with sufficient information to carry out this exercise. The minimum information which should be provided is that which is listed in Article 5 (1) of the Directive 2014/41/EU (the object and reason for the order, a description of the suspected offence, etc).

2. Service providers must be permitted to refuse to comply with EPOs and EPrOs on the grounds listed at Article 11 (1) (a) – (g) of Directive 2014/41/EU[24].

[24] Art. 11 (1) (h) of Directive 2014/41/EU specifies as a ground for non-recognition or non-execution that „the use of the investigative measure indicated in the EIO is restricted under the law of the executing State to a list or category of offences or to offences punishable by a certain threshold, which does not include the offence covered by the EIO“ and is therefore not applicable to the proposals for EPOs and EPROs.

To enable service providers to do so, EPOs and EPrOs must contain substantive information about the subject matter and background of the order, as well as on its necessity and proportionality. The minimum information required is again listed in Art. 5 (1) Directive 2014/41/EU. In addition, the requested data must be justified in terms of content and time.

3. EPOs and EPrOs should only be available for specified offences of a serious nature and where dual criminality exists.

4. Draft Article 5(5)(e) should be amended to mandate the specification of a particular period of time for which data are sought and a time limit should be set for the issue of an EPO following the issue of an EPrO in respect of the same data.

5. The proposals should permit refusal to comply with an EPO where: (i) it relates to an offence which took place outside the issuing State and wholly or partially on the territory of the enforcing State; and/or (ii) the execution would be contrary to the *ne bis in idem* principle.

6. The procedure for identifying data protected by immunities and privileges must be better regulated and an improved dispute resolution mechanism must be provided for in the event that the issuing and enforcing State reach different conclusions on what is privileged.

7. Violation of fundamental rights in the acquisition of data, whether by way of breach of the right to private life or breach of immunities or privilege by the means of Article 8 ECHR, should give rise to automatic exclusion and deletion of such data.

8. To demonstrate respect for the laws of fellow states, it should not be permissible for a Court of the issuing state to determine conflicts between EPO and the laws of a third country. To avoid potentially damaging conflicts disputes, the ECBA recommends that draft Article 15(4) of the proposals be deleted.