Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)

Adopted on 26 September 2018

Contents

The European Data Protection Board

Having regard to Article 70 (1b) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

HAS ADOPTED FOLLOWING OPINION:

Introduction

In April 2018, the Commission presented a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and a proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purposes of gathering evidence in criminal proceedings. The two proposals COM(2018) 225 final and COM(2018) 226 final are complementary. The overall goal pursued by the Commission is to improve cooperation between Member State authorities and services providers, including those based in non-EU countries, and to propose solutions to the problem of determining and enforcing jurisdiction in cyberspace.

While the draft Regulation foresees the rules and procedures applicable to issue, serve and enforce preservation and production orders on providers of electronic communication services, the draft Directive provides for minimum rules for the appointment of a legal representative for service providers not established in the EU.

In November 2017[1], before the Commission tabled any draft proposal, the Article 29 Working Party (WP29) recalled the necessity to ensure that any legislative proposal fully complies with the existing EU data protection *acquis* in particular, as well as EU law and case-law in general.

In particular, the WP29 warned against limitations to the rights to data protection and privacy with respect to data processed by telecommunications and information society providers, especially when further processed by law enforcement authorities, recalled the necessity to ensure consistency of any EU instrument with the existing Council of Europe Budapest Convention on cybercrime and with the EU Directive on the European Investigation Order (EIO), and recommended to clarify the respective procedural rules governing access to e-Evidence at national and EU level to ensure that the new instrument would not grant authorities new powers they would not have internally. In addition to these general remarks, the WP29 commented on the legislative options considered by the Commission at that time concerning the categories of data concerned and the corresponding safeguards to access them, on the possibility to address production orders/requests to compel service providers to provide data located outside the EU, and on the substantive and procedural conditions necessary safeguards to surround direct access to data.

With the concrete proposals on e-Evidence at hand now, the EDPB wishes to give a more detailed analysis of the proposed legal instruments from a data protection point of view.

[1] See WP 29 statement (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)

1. Legal basis of the Regulation proposal (article 82 TFUE)

The legal basis suggested for the e-Evidence draft Regulation is article 82(1) of the TFEU, concerning judicial cooperation in criminal matters, which provides:

> "*1. Judicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States in the areas referred to in paragraph 2 and in Article 83.*
>
> *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures to:*
>
> *(a) lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions;*
>
> *(b) prevent and settle conflicts of jurisdiction between Member States;*
>
> *(c) support the training of the judiciary and judicial staff;*
>
> *(d) facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions.*"

As underlined by the Commission in the impact assessment accompanying the proposals, "Article 82(1) specifies that judicial cooperation in criminal matters shall be based on the principle of mutual recognition. This legal basis would cover possible legislation on direct cooperation with service providers, in which the authority in the issuing Member State would directly address an entity (the service provider) in the executing State and even impose obligations on it. This would introduce a new dimension in mutual recognition, beyond the traditional judicial cooperation in the Union, so far based on procedures involving two judicial authorities, one in the issuing State and another in the executing State."(emphasis added)

Given the novelty of the use of this legal basis in the context of direct requests between public authorities and private parties, the EDPB regrets that no further analysis nor assessment is provided by the Commission.

Indeed, as already underlined by the Working Party in its previous statement, the EDPB continues to stress its doubts on the appropriateness of this legal basis, which are supported by the analysis of the CJEU and its Advocate General in the Opinion 1/15. Among the developments made concerning the validity of Article 82 as a legal basis for the draft PNR agreement between the EU and Canada, the Court underlined that the Canadian Competent authority "*does not constitute a judicial authority, nor does it constitute an equivalent authority*"[2]. In the context of the e-Evidence proposals, one of the main goal pursued as stated by the Commission appears to be to avoid the "too cumbersome" judicial cooperation. Consequently, the proposal is based on the principle that cooperation should take place between an authority and a service provider rather than between two authorities. The procedure foreseen primarily places private entities in the position to be the receiving party and to answer the requests emanating from judicial authorities.

The EDPB notes that the process of enforcing production or preservation orders could imply the involvement of a receiving authority in the situation where the receiving service provider does not comply with its obligations and will thus trigger the need to call for an ex-post enforcement of the order. However, as the main objective of the procedure set up is precisely not to involve a receiving

[2] See point 103 of Opinion 1/15 and point 108 of the opinion of the advocate general in this case.

authority, the EDPB doubts that this ancillary procedure could justify the use of Article 82 as the sole legal basis for the instrument.

Therefore, the EDPB takes the view that for Article 82 to be used as a legal basis the main procedural steps of the cooperation shall take place between two judicial authorities and that another legal basis should be used for this type of cooperation.

2. Necessity of e-Evidence compared to MLATs and EIO

The EDPB notes that the Commission is committed to review obstacles to criminal investigation, especially regarding the issue of access to electronic evidence. In its explanatory memorandum, the Commission gives the context of the proposal and stresses the volatile nature of electronic evidence, its international dimension as well as the need to adapt cooperation mechanism to the digital age. Proposals for a regulation and a directive for transferring and accessing electronic evidence are not aiming to replace previous cooperation instruments in criminal matters such as the Budapest Convention, the Mutual Legal Assistance Treaty (MLAT) and the European Investigative Order (EIO directive). According to the Commission, e-Evidence proposals aim at improving judicial cooperation in criminal matters between authorities and service providers within the European Union as well as with third countries, the United States of America in particular.

Since these new additional tools will be specifically dedicated to the access and transfer of electronic evidence, the EDPB will assess the added value of the instruments regarding the EIO directive and the MLAT.

a) The necessity of e-Evidence compared to the safeguards provided by EIO and MLATs

The main argument raised by the Commission in favor of the e-Evidence proposals is to speed up the process to secure and obtain electronic evidence that is stored and/or held by service providers established in another jurisdiction.

The EDPB however deplores that the necessity to have a new instrument to organize access to electronic evidence was not demonstrated in the impact assessment. Indeed, the proposals lack a demonstration that no other less intrusive means could have been used to achieve the goal of the e-Evidence proposal, while alternative solutions could have been contemplated. For instance, the possibility to modify and improve the EIO Directive could have been examined and would also have answered the specific requirement under the EIO Directive to evaluate the need to amend the text by 21 May 2019[3]. Another option could have been to foresee the use of preservation orders to freeze the data for as long as a formal request based on an MLAT were issued. These options would have allowed to maintain the safeguards provided in these instruments while ensuring that the personal data sought is not deleted.

The EDPB notes that the time limits established in the EIO Directive are longer than in the e-Evidence proposal. Indeed, the executing authority has 30 days to take its decision on the recognition of the request[4] and then should execute the order within 90 days[5]. The EDPB considers that allowing 30 days

[3] See Art. 37 of the EIO Directive
[4] Art. 12 (3) EIO Directive
[5] Art 12 (4) EIO Directive

of reflection for the executing authorities in the EIO is a crucial safeguard enabling them to assess whether the request for execution is well founded and respects all the conditions for issuing and transmitting an EIO[6].

The EDPB is concerned that the 10-day deadline put forward in the e-Evidence proposals to execute the European Production Order Certificate (EPOC), without any time for reflection, prevents the proper assessment of whether the EPOC meets all the criteria and is completed correctly.

Therefore, the EDPB recommends that more time be provided for the EPOC recipient to determine whether the order should or should not be executed.

The EDPB notes that in case of a European Preservation Order (EPOC-PR), there is no guaranty that the preservation of the data will be limited to what is necessary to produce. Indeed, the duration of preservation of the data may exceed 60 days since there is no time limit for the issuing authority to inform the addressee to refrain from issuing, or to withdraw a production order. Therefore, the EDPB recommends at least a time limit for the issuing authority to refrain or withdraw the production order in order to comply with the principle of data minimization established in the GDPR[7].

Finally, the EDPB notes that the EIO directive establishes the return of evidence from the issuing State to the executing authority[8]. However, the E-evidence Regulation proposal is silent regarding such a possibility. What happens to the electronic evidence after its transmission to the issuing authority is unclear.

Therefore, the EDPB recommends that the Regulation proposal should provide more information on the use of electronic evidence after their transfer to the issuing authority in order to comply with the GDPR and the principle of transparency[9] as well as the principle of specificity established by the MLATs.

b) The abandonment of the dual criminality principle

The EDPB acknowledges that mutual recognition is dependent on the application of the double criminality which is a way for Member States to maintain their sovereignty. However, double criminality is increasingly considered as an obstacle to smooth judicial cooperation. EU Member States are more and more willing to cooperate even if the investigative measures relate to acts that are not considered as an offence in their national law. The EDPB however recalls that the dual criminality principle aims at providing an additional safeguard to ensure that a State cannot rely on the assistance of another to apply a criminal sanction which does not exist in the law of another State. This would for instance prevent a State from requiring the help of another one to imprison someone for their political opinions if these opinions are not criminalized in the requested State or to prosecute someone for having aborted if this person is residing in another State where it is not illegal. The dual criminality principle is also often accompanied by additional limitations or safeguards concerning the sanctions if they differ too much between the requesting and the executing State. The main example is the commitment not to apply the death penalty in certain MLATs when it does not exist in the law of one of the two parties.

[6] Art. 6 EIO Directive
[7] Art. 5 (1) (c) GDPR.
[8] Art. 13 (3) and (4) EIO Directive.
[9] Art. 5(1) (a) GDPR.

The EDPB notes that the dual criminality principle is ruled out in the e-Evidence regulation proposal. However, it does not result only in the deletion of the usual formalities of mutual recognition but also in the deletion of safeguards linked to the dual criminality principle itself.

Indeed, the EDPB notes that no reference is made to the law of the country where the requested service provider is established, and that the preservation of any data, as well as the production of subscriber or access data, may be issued for all criminal offences[10] regardless of whether there are similar criminal offences established in other Member States or not.

Meanwhile, production orders may only be issued and executed if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing State[11]. In addition, as explained by the Commission in the explanatory memorandum of the regulation proposal, the specificity of transactional data and content data is established, as they are considered to be more sensitive. Indeed, orders concerning transactional or content data are based on a threshold of a maximum custodial sentence of at least 3 years in order to ensure respect for proportionality and the rights of the persons affected[12]. However, the EDPB underlines that no harmonization within the EU has taken place yet of criminal offences punished by a maximum of at least 3 years of custodial sentence.

The EDPB opposes the abandonment of the dual criminality principle, which aims at ensuring that a State cannot rely on the help of others to have its national criminal law applied outside of the State's territory by a State which does not share the same approach, especially given the disappearance of other traditional major safeguards in the field of criminal law (see below point 3 on the location criteria and point 7 (g) concerning potential conflicts with third countries' laws).

c) The consequence of addressing the companies directly

The EDPB acknowledges that electronic evidence is increasingly available on private infrastructure and may be located outside the investigating country, owned by service providers.

The EDPB notes that following the *Yahoo!*[13] and *Skype*[14] decisions in Belgium and in the context of terrorist attacks, there is a need for a smoother and faster cooperation between public and private entities. In the impact assessment, the Commission refers to three types of procedural instruments involving both public authorities and service providers. These are judicial cooperation, direct cooperation and direct access. If the first one is not putting the responsibility on the service provider to execute the EIO but on the executing authority[15], the second, direct cooperation, is based on the cooperation of the service provider. The most intrusive is direct access from a service provider's perspective since public authorities are able to access data without the help of an intermediary.

Therefore, the EDPB fears that, when addressed directly, service providers will not ensure the protection of personal data as efficiently as public authorities are able and obliged to do and stresses that it also results in the inapplicability of certain procedural guarantees foreseen in the context of

[10] Art. 5 (3) and Art. 6 (2) of the proposed Regulation on e-Evidence.
[11] Art. 5 (2) of the proposed Regulation on e-Evidence
[12] Art. 5 (4) (a) of the proposed Regulation on e-Evidence
[13] Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1st December 2015.
[14] Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016. (Skype has appealed the decision).
[15] Art. 10 – 16.

judicial cooperation for individuals, as well as for companies themselves[16]. Indeed, for instance, a requested service provider would have to go before the court of another (Member) State to contest the order while in the context of judicial cooperation it would face its own authorities. The EDPB recommends the inclusion of additional grounds in the Regulation proposal certifying that service providers will protect individual fundamental rights as the protection of personal data and the respect of private and family life, as well as the information of the competent data protection authority in order to make sure control is possible.

3. The new ground for jurisdiction and the so-called disappearance of the location criteria

The EDPB notes that the Commission underlines that one of the major changes brought by these proposals is the disappearance of the location criteria and the possibility for competent authorities to request the preservation and production of data regardless of where these data are actually stored.

From a data protection perspective, it is not new that EU data protection law applies regardless of where the data of persons concerned are stored. Indeed, the applicability of the GDPR depends either on the fact that the controller or processor is established within the EU, or on whether EU data subjects' data are processed, even when the controller or processor are not established on the territory of the EU[17], in which case they also have to designate a legal representative in the EU[18]. From the perspective of data protection it is important to note that the extended territorial scope aims at providing a more complete protection to EU data subjects, regardless of where the company processing their data is established.

Therefore, although the disappearance of the location criteria might be new in the field of criminal law, this does not appear as a major change from a data protection perspective. In addition, the EDPB also notes that a link is still maintained with the territory of the EU as only service providers offering services in the Union fall within the scope of the proposals, and the fact that requests can only be addressed in the context of criminal investigations imply a link with the EU (either because the crime was committed in the territory of a Member State or because the victim or the criminal was a citizen of a Member State).

If the disappearance of the location criteria should now be applied in criminal law, the most important question for the EDPB concerns how to ensure that such a development is not detrimental to data protection and criminal procedural rights of the data subjects and the requested service providers. From that perspective, the EDPB acknowledges that within the EU, procedural safeguards have been, at least partially, harmonized and need to be provided in compliance with the European Convention of Human Rights. It can thus be argued that the disappearance of the location criteria would probably have more limited consequences when the evidence is sought within the EU compared to the reverse situation where authorities from third countries request data to companies established within the EU under the same conditions as set out in the e-Evidence draft Regulation. Indeed, the EDPB is particularly concerned this could result in more problematic situations. In this context, authorities from

[16] See also from an international data protection perspective the "Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes", The International Working Group on Data Protection in Telecommunications, 63rd meeting, 9-10 April 2018, Budapest (Hungary).
[17] See Art. 3, in particular (2).
[18] See Art. 27

a third country where different and potentially less procedural safeguards apply in the field of criminal law could have access to data that would be protected by additional safeguards within the EU. From that perspective, the EDPB recalls its concerns about a double standard and a weakening of fundamental rights when service providers and data subjects do not benefit from the procedural safeguards in EU law if the request is made from a third country authority.

Furthermore, as this new ground of jurisdiction "regardless of the location of the data" is coupled with a procedure mainly relying on direct requests from competent authorities to service providers, the EDPB is concerned that data protection safeguards may not be applied by private companies receiving requests and which are not bound by a legal instrument such as an MLAT, traditionally governing the exchanges of data between judicial authorities and providing for safeguards. In particular, in the context of MLATs, minimum data protection safeguards imply for instance confidentiality obligations and the principle of specificity which implies that data will not be processed for another purpose.

At least, the EDPB therefore recalls that the safeguards provided in Directive 2016/680 should be made applicable, including with regards to data transfers, and especially Article 39 in case the service provider would be established in a third country without an adequacy decision in this field. In particular, the EDPB stresses that this provision implies notably the information of the competent data protection authority in the Member State of the issuing authority of the order(s) and the documentation of the transfer, including with regards to the justification concerning the ineffectiveness or inappropriateness of a transfer to the competent authority of the third country.

4. The notion "service providers" should be restricted or complemented by additional safeguards for the data subjects' rights

As regards service providers, the EDPB welcomes the wide definition which allows to include both communication services and Over-The-Top (OTT) services, since all these services are functionally equivalent and therefore the foreseen measures could have a similar impact on the right to privacy and the right to secrecy of communications, as underlined in the statement of the WP29 and previously in Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation. Indeed, the proposal for a Regulation on electronic evidence covers service providers providing either electronic communications services as defined in Article 2(4) of Directive establishing the European Electronic Communications Code, information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535, "for which the storage of data is a defining component of the service provided to the user, including social networks, online marketplaces facilitating transactions between their users, and other hosting service providers", or internet domain name and IP numbering services "such as IP providers domain name registries, domain name registrars and related privacy and proxy services"[19].

However, a service provider in the sense of the draft Regulation being "any natural or legal person that provides one or more of the following categories of services", the EDPB is concerned that this instrument could cover both controllers and processors in the sense of the GDPR. Indeed, as "offering services" as defined in Article 2 (4) of the draft Regulation includes both enabling legal or natural persons in one or more Member State(s) to use the services listed, and having a substantial connection

[19] Article 2 (3) (c) of the proposed Regulation on e-Evidence

to the Member State(s) in question, these activities include activities performed by a processor for a controller, such as storing data, for instance.

Hence, the EDPB fears that without limitations to service providers acting as controllers in the sense of the GDPR, and without any specific obligation of the processor to notify the data controller, when addressed with a production or preservation order, data subjects' rights might be circumvented. This is especially the case since in the context of possible conflicting obligations preventing the addressee to serve the orders received, the judicial authorities are also encouraged in the draft Regulation itself to address the most appropriate actor regardless of the data protection rules applicable, in particular given that any data could be requested, and not only personal data subject to the GDPR[20].

According to the GDPR, a processor only acts on the instructions given by the controller. Therefore, it is the responsibility of the controller to ensure the rights of data subjects are respected, and to provide them with the relevant information, including with regards to recipients of their data, for instance in the context of the exercise of their right of access. The processor will not receive these requests from data subjects and will not be in a position to answer, unless expressly asked by the controller.

Consequently, unless their rights have been limited in application of the GDPR, the EDPB stresses that data subjects benefitting from the application of the GDPR may not be able to exercise their rights efficiently if the controller is not in a position to provide complete information. The EDPB also notes that the likelihood of the absence of information is even higher without any specific obligation imposed on the processor to inform the controller when the data requested concern data subjects who do not benefit from the protection granted by the GDPR. Indeed, the judicial authorities requesting the data will not necessarily have the obligation to inform the data subjects of their own further processing in this case. The EDPB therefore calls on the restriction of the scope to controllers in the sense of the GDPR, or on the introduction of a provision clarifying that in the event where the service provider addressed is not the controller of the data, it shall inform the controller.

5. The notions of "establishment" and of "legal representative" in the context of these proposals should be clearly distinguished from these notions in the context of the GDPR

Given the inapplicability of the location criteria with regards to data, the addressees of production and preservation orders within the scope of the proposed Regulation are limited to service providers offering services in the Union, whether established within the EU or not, with the obligation to appoint a legal representative, according to the rules proposed in the draft Directive. These notions of "establishment" and "legal representative" are therefore defined in the draft instruments.

The EDPB notes that these notions also appear in the context of other EU instruments, and in particular in the context of the GDPR. Consequently, clarifications as to the definition and delineation between these notions in the context of the draft proposals and in the context of the GDPR should be provided.

a) Establishment

The EDPB also recalls that the notion of "establishment" in the context of the draft Regulation shall not be confused with the notion in the context of the GDPR. Indeed, for the purpose of the draft

[20] See Article 7 (3) and (4)

Regulation, the notion of establishment as defined in Article 2 (5) is broader than in the GDPR as it includes "either the actual pursuit of an economic activity for an indefinite period through any stable infrastructure from where the business of providing services is carried or a stable infrastructure from where the business is managed", whether or not processing of personal data takes place in the context of the activities of this establishment. Thus, if "establishment" in the sense of the GDPR was to undoubtedly be included in the establishment defined in the draft Regulation, the contrary might not be the case.

The EDPB therefore warns that establishments of service providers in the sense of the draft Regulation might not necessarily imply that the conditions for the application of the GDPR according to Article 3(1) are met. In this context, controllers and processors are therefore invited to check if the applicability of the GDPR does not derive from Article 3(2) which would imply the designation of a legal representative within the EU and the absence of One-Stop-Shop mechanism.

b) Legal representative

In its statement, the WP29 stressed that any confusion should be avoided between the obligation to designate a legal representative under Article 27 of the GDPR and the legal representative foreseen under the draft Regulation on e-Evidence.

With the draft proposal at hand, the EDPB would like to recall these recommendations, and in particular to underline that in its understanding, the legal representative in the meaning of the draft Directive on the appointment of a legal representative in the context of the e-Evidence proposals shall be designated in any case, be vested with specific functions, independently of a mandate given by the service provider, have the power to answer requests and to act on behalf of the service provider and a stronger liability than the legal representative of the GDPR.

Furthermore, the EDPB stresses that the obligation to designate a legal representative in any case under the e-Evidence draft proposals, whether the service provider is established in the EU or not, the possibility to designate even several legal representatives for the same service provider under the e-Evidence draft Directive, and the obligation to notify the designation of the legal representative to the Member States' authorities differ from the GDPR, which does not provide for such obligation to notify the designated legal representative, exemptions to the designation and limited responsibilities of the legal representative.

Therefore, given the important differences in terms of role, liability and relationship with the other establishments of the service provider in one case and controller or processor in the other, the EDPB recommends that, where a service provider is not established within the EU, but is subject to both the GDPR pursuant to article 3 (2) and to the e-Evidence Regulation, two distinct legal representatives should be designated, each with clear distinct functions according to the instrument on the basis of which it is designated.

6. New categories of data

The proposed regulation defines different categories of data as per article 2: subscriber data, access data, transactional data and content data. Recital 20 of the Commission proposal further specifies that "*The categories of data this Regulation covers include subscriber data, access data, transactional data (these three categories being referred to as 'non-content data') and content data. This distinction, apart from the access data, exists in the legal laws of many Member States and also in the current US legal*

framework that allows service providers to share non-content data with foreign law enforcement authorities on a voluntary basis."

In this context, the EDPB stresses first of all that all four categories of data cited above are to be considered as personal data according to EU data protection law since they do contain information related to an identified or identifiable natural person, whether the data subject is referred to as "subscriber" or "user" in the proposed regulation. Similarly, it is to be noted that "electronic evidence" as defined in Article 2(6) of the Commission's proposal encompasses all four categories of data and therefore relates to personal data. Therefore rather than laying down the rules for access to evidence, defined and qualified as per national law and judicial procedures, the proposed regulation provides for new substantive and procedural conditions related to the access to personal data.

While the proposed regulation establishes new subcategories of personal data for which different procedural conditions of access apply, the EDPB recalls that, in accordance with the relevant CJEU case law, to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way.

Furthermore, the EDPB recalls that in relation to "non-content data" which encompass subscriber data, access data and transactional data as per the Commission proposal, the Court of Justice of the European Union has ruled in its judgement in joined cases C-203/15 and C-698/15 Tele*2 Sverige AB* that metadata such as traffic data and location data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications[21].

As already stated in the WP29 statement on Data protection and privacy aspects of cross-border access to electronic evidence of 29th November 2017, the EDPB therefore reiterates its doubts and concerns with regards to the current delineation between "non-content" and content data, as well as to the four categories of personal data laid down by the proposed regulation. Indeed, the four categories proposed do not appear to be clearly delineated, and the definition of "access data" still remains vague, compared to the other categories. The EDPB therefore regrets that the Commission's impact assessment and proposal did not further substantiate the rationale for the creation of these new subcategories of personal data, and expresses its concerns with regards to the different level of guaranties related to the substantive and procedural conditions for access to the categories of personal data, especially given the practical difficulty to evaluate to which category of data will belong the requested data in some cases. For instance IP addresses could both be classed as transactional data and subscriber data.

In this context, the EDPB also recalls that in recital 14 of its proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy), the Commission considers that "electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication". Since the current and future ePrivacy framework, as well as the related limitations to the right to privacy, will apply to the rules regulating law enforcement access

[21] CJEU Judgment of 21 December 2016, paragraph 99.

to electronic evidence, the EDPB recommends that a broader definition of electronic communication data is included in the proposed regulation, in order to ensure that the appropriate safeguards and conditions for access to be established cover consistently both 'non-content' and 'content data'.

7. Analysis of the procedures for European Preservation and Protection Orders

Broadly speaking, the procedure for addressing a production or preservation order appears to be the following:

- The competent judicial authority – the issuing authority – depending on the type of data requested and on the type of order, issues the order according to the (scarce) conditions enumerated in articles 5 and 6, sends it by using a harmonized certificate to the legal representative of the service provider or to any of its establishment within the EU – the addressee.
- Upon receipt of the certificate, the addressee shall execute the order – meaning transmit the data within 10 days or 6 hours in case of emergency, or preserve them up to 60 days – unless it is impossible do so, because the certificate is incomplete or because of *force majeure* or de facto impossibility for the addressee, or because the addressee refuses on the ground of conflicting obligations, either with regard to fundamental rights or fundamental interests of a third country or based on other grounds.
- In case the addressee has not complied with the order received without providing reasons accepted by the issuing authority, procedures are foreseen to enforce the orders by a competent enforcing authority in the Member State where the service provider is represented or established, unless limited grounds for refusal apply and the enforcing authority objects to the recognition or enforcement of the order.
- In case the addressee issued a reasoned objection to the order based on conflicting obligations, the issuing authority shall refer the case to the competent court in its Member State, which shall then be in charge of assessing the possible conflict and of upholding the order in the absence of a conflict. In the event of a conflict, the competent Court shall, either address the central authorities in the third country, via its national central authorities, with a 15 day deadline to respond, which can be extended by 30 days upon reasoned request, in case of conflicting obligations with regards to fundamental rights or fundamental interests of a third country, or determine itself whether to uphold or withdraw the order for other grounds of refusal invoked by the addressee.
- Without prejudice to remedies available under the GDPR and the LED, persons whose data was obtained via a production order shall also have the right to effective remedies against this order.

The EDPB assessed the procedures foreseen and the safeguards provided in the draft Regulation to surround the different steps and on each of the aspects presented here-after recommends the following safeguards and amendments.

a) Thresholds for issuing orders should be raised and orders shall be issued or authorised by courts

As regards the conditions for issuing orders, the EDPB welcomes the principle of higher safeguards to access transactional or content data. However, it notes that given the absence of full harmonisation of criminal sanctions between Member States, the reference to "criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years"[22] still implies diverging thresholds and discrepancies in the protection of their data for data subjects within the EU.

Furthermore, the EDPB stresses that, especially given the broad definition of subscriber data, the threshold provided appears rather low for preservation orders and for production orders concerning subscriber or access data, as all criminal offences can in principle justify the issuance of such orders. Similarly, the authorities allowed to issue such orders are more limited in the context of production orders concerning transactional or content data, than for the issuance of preservation orders or production orders to produce subscriber or access data, as prosecutors can issue or authorise only the latter orders, while any judge, court or investigating judge can issue or authorise any order.

In particular, the EDPB regrets that the lowest threshold providing for the possibility for law enforcement authorities to request access to subscriber and access data for any criminal offence builds on an "*a contrario"* reading of the case law of the CJEU (which focuses on the other data) to make distinctions as the safeguards to be afforded. Indeed, the CJEU specifically underlined that for traffic and location data, access of the competent authorities shall be restricted solely to fighting serious crime[23]. The EDPB could understand that the proposal would provide for the possibility to request access to very basic information which would just allow to identify a person without revealing any communication data without a prior authorisation from a court. However, it deplores the broad "*a contrario*" reading of this ruling by the Commission and calls for higher safeguards to be introduced in order to restrict the grounds for access to other subscriber data and to access data. The EDPB suggests to restrict access to these data either to a list of crimes provided in the draft Regulation, or at least to "serious criminal offences", especially given the lower prior authorisation threshold foreseen for these data.

In addition, the EDPB underlines that this "*a contrario*" reading also leads to the fact that the proposal opens the possibility for prosecutors to issue or authorise the issuance of orders. The EDPB is of the opinion that, except in case of requests concerning very basic information which would just allow to identify a person without revealing any communication data, this constitutes a step back compared to the case law of the CJEU concerning access to communications data. Indeed, in its case law concerning access to communications data for law enforcement purposes, the CJEU has restricted the possibility to provide for such access, among other criteria, and "*except in cases of validly established urgency*"[24], to a "*prior review carried out by a court or an independent administrative authority*", "*following a reasoned request of competent national authorities submitted within the framework of procedures of prevention, detection or criminal prosecution*." [25]

The EDPB recalls that the notion of "court" is an autonomous notion of EU law, and that the CJEU has constantly underlined and recalled the criteria to be fulfilled to qualify as a court, including the criteria

[22] See Art. 5 (3) (a)
[23] See case 203/15 – Par (125)
[24] See case 203/15 – par (120)
[25] See joint cases C 293/12 and C 594/12 - par (62)

of independence[26] which does not appear to be the case for prosecutors, as recalled also by the ECtHR in its case law[27] .

Consequently, articles 4 (1) (a) and (b) and 3(a) and (b) result in procedures where significantly less safeguards will apply for subscriber and access data since a prosecutor alone will be able to request data, without neither any further control from the authority of the State where the requested data are or from the authority where the legal representative of the requested company will be, nor any control from an independent administrative authority.

Furthermore, the EDPB notes the so-called additional safeguard provided in Article 5 (2) which limits the possibility to issue a production order when a similar measure was available for the same criminal offence in a comparable domestic situation. However, it warns against the counterproductive effect of such a provision: rather than providing additional safeguards it appears as an encouragement for Member States to extend their national possibilities to ask for the production of subscriber or access data in order to ensure production orders could be issued under this Regulation.

b) Time-limits to provide data should be justified

The EDPB notes that European Production orders shall be answered within 10 days at the latest upon receipt of the certificate, unless the issuing authority indicates reasons for earlier disclosure, and at the latest within 6 hours in emergency cases, as provided in Article 9 (1) and (2).

However, the EDPB has not seen any criteria framing the obligation for authorities to demonstrate the emergency to produce data, even *ex post* in order to allow for a possible control of the use of this very fast procedure, while a six hour deadline is likely to imply a very light control before producing the data, if not the absence of any control on the part of the service provider. Indeed, the impact assessment stresses the necessity for competent authorities to have access to data in a timely manner. However, the examples given in the impact assessment all concern evidence needed in case of serious crimes being committed (terrorism cases with hostages, ongoing child sexual abuse situations), but the justification based on the volatility of evidence does not appear to be a good one when there is no specific urgency other than this potential volatility of the data. In addition, the volatility of data does not provide any additional justification as to the proportionality to have access to data with less safeguards in these situations where there is no urgency other than the volatility of data.

In addition, the EDPB doubts the necessity to provide for a six hours deadline while providing that this deadline would not apply until the issuing authority provides additional clarifications “within five days” in case the service provider cannot comply with its obligation.

The EDPB therefore calls for additional elements in the impact assessment to justify the necessity of these deadlines in cases where the crime being committed or prosecuted is not serious, and unless such detailed elements are provided, for explicit criteria to justify the emergency in case EPOCs are issued. For instance, the same model as in the EIO Directive could be foreseen. The EIO Directive provides for a shorter deadline when justified by "procedural deadlines, the seriousness of the offence or other particularly urgent circumstances" (see Art. 12 (2)), or for a 24-hour deadline to decide on provisional measures (see Art. 32 (2)). Indeed the impact assessment of the draft Regulation does not provide for detailed elements to justify why these deadlines are not efficient, the only elements underlined being that the number of requests sent overload the receiving judicial authorities which cannot respect the deadlines.

[26] See for instance case C 203/14
[27] See for instance Moulin c/ France 23/11/2010

c) European Production and Preservation orders shall not be used to request data of another Member State data subject without at least informing the competent authorities of that Member State, in particular for content data

The EDPB recalls that in existing instruments judicial cooperation and thus additional safeguards, are provided, in particular to control the necessity and proportionality of requests, and underlines that these safeguards are all the more justified in cases where requested data are content data which involve more limitations of the rights of data subjects to have their personal data and privacy protected. In this regard, the EDPB recalls that the EIO Directive also provides for the possibility to intercept telecommunication with the technical assistance of another Member State (see Art. 30), as well as for the obligation to notify any interception of data to the competent authority of another Member State where no assistance is needed when the data subject concerned is or will be on the territory of that Member State (see Art. 31).

The EDPB finds no justification for the procedure foreseen in the draft e-Evidence Regulation to allow for the production of content data without any involvement at least of the competent authorities of the Member State where the data subject is.

d) European preservation orders shall not be used to circumvent data retention obligations of the service providers

The EDPB notes that the main aim of European Preservation Orders is to prevent data from being erased.

Although the EDPB recognizes that it may be necessary and proportionate in some cases, it deplores the lack of safeguards surrounding the issuance of such orders. In particular, the EDPB recommends that when preservation orders are addressed for specific data only, where the draft seems to allow for broad requests, and that when such orders are issued for data scheduled to be erased in compliance with the data retention principle, the order shall never serve as a basis for the service provider to process the data after the initial date of erasure. In other words, data should be "frozen".

In addition, the link between the preservation order and the subsequent request for the production of data, be it through a European Production order, an EIO request or a mutual legal assistance request, should be strengthened, in order to ensure that European Preservation orders are issued only when the other request is certain (and not just contemplated as a possibility), and that when the other request is refused, the preservation order also expires, without having to wait for 60 days[28] if the subsequent request is refused earlier.

e) Confidentiality and user information

The EDPB notes that a specific Article[29] concerning the confidentiality of orders addressed has been introduced in the draft Regulation. In order to avoid any confusion and misunderstanding with the right to data protection, the EDPB recalls that although the GDPR provides that limitations to the rights of data subjects to safeguard the prevention, investigation, detection or prosecution of criminal penalties, should be provided by law and therefore publicly accessible[30] and that these legislative

[28] See Art. 10 (1)
[29] See Art. 11
[30] See Art. 23 (1) (d)

measures shall contain specific provisions as to the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction[31], it does not provide for the obligation to inform individually data subjects of each access request made by law enforcement authorities.

However, in the meantime, the EDPB recalls that the Data protection directive provides for this right of information for the data subjects from the competent authorities themselves, unless this right has been limited, to any data subject without limiting this right only to data subjects residing in the territory of the EU.

f) Procedure for the enforcement of an order when the service provider refuses to execute it

The EDPB notes that Article 14 of the draft Regulation provides for a procedure to ensure the enforcement of an order when the addressee does not comply with it, relying on a judicial cooperation between the issuing authority and a competent authority in the enforcing State.

However, it appears that this procedure does not allow the enforcing authority to refuse to enforce the order transmitted on other grounds than purely procedural ones (the same as the addressee, mainly concerning the lack of information provided or the factual impossibility to provide the data), because the data concerned is protected by an immunity or privilege under its national law or because its disclosure may impact its fundamental interests such as national security and defence[32].

The EDPB therefore reiterates its concerns as regards the removal of any double check by the receiving competent authority of the order transmitted, compared to the other instruments. Even the ground to refuse to enforce an order on the ground that it would violate the Charter appears higher than the classic threshold relating to a breach of the fundamental rights of the person concerned. Consequently, following the examples of the European Arrest Warrant, which provides for mandatory as well as optional grounds of refusal, or at least of the EIO Directive, which generally provides that the presumption according to which "the creation of an area of freedom, security and justice within the Union is based on mutual confidence and a presumption of compliance by other Member States with Union law and, in particular, with fundamental rights" is rebuttable[33], the draft Regulation should at least foresee the minimum classic derogation that if there are substantial grounds for believing that the enforcement of an Order would result in a breach of a fundamental right of the person concerned and that the executing State would disregard its obligations concerning the protection of fundamental rights recognised in the Charter, the enforcement of the order should be refused.

g) Enforcement of orders and conflicting obligations under third country laws (articles 15 – 16)

The EDPB welcomes the possibility provided in the draft Regulation for addressees to refuse an order on the ground that it would conflict with fundamental rights as it is aimed at providing safeguards in case of conflicting legal obligations. It also deems essential that the proposal provides for the consultation of third-countries authorities, at least where a conflict arises, as well as the obligation to lift the order when a third-country's authority raises an objection.

[31] See Art. 23 (2) (h)
[32] See Art. 14 (2)
[33] See recital 19 of the EIO Directive

Therefore, the procedure foreseen to refuse to execute an order on the ground of conflicting obligations under third country laws should be considerably improved.

First, the EDPB notes that the draft Regulation entrusts a private company, as addressee of a production order, to assess whether or not that order would be in conflict with applicable laws of a third country prohibiting the disclosure of the data requested. The company has to provide a reasoned objection including all relevant details of the law of the third country, its applicability to the case at hand and the nature of the conflicting obligations.

Most importantly, the EDPB is concerned that when such an objection is raised, the competent court of the Member State of the issuing authority alone assesses whether a conflict exists or not, since it is only when the court finds a conflict that it shall get in contact with the third country authorities. The competent EU court is therefore granted the competence to conclusively interpret the law of a third country in this context, without being that much of a specialist on the substance. The EDPB considers that the obligation to consult the competent authorities of the third country is therefore too limited in the current proposal. In the field of data protection, the EDPB draws the attention of the legislator to the fact that in case a competent court of a third country would interpret the GDPR to assess whether it is conflicting with its own requirements, the data protection authorities of the EU and the competent courts would remain competent to assess the legality of the transfer based on a judgment of a court or tribunal or on a decision of an administrative authority of a third country requiring a transfer or disclosure of personal data within the scope of the GDPR[34].

In addition, the EDPB underlines that the assessment of the law of the third country by the competent court of the EU requesting State needs to be based on objective elements, and is concerned by the criteria to be taken into account by the competent court when assessing the law of the third country under Article 15 (4) and 16 (5) (a) of the draft Regulation. Indeed, the Court would have to assess the fact that, “rather than being intended to protect fundamental rights or fundamental interests of the third country related to national security or defence”, the law of the third country “manifestly seeks to protect other interests or is being aimed to shield illegal activities from law enforcement requests in the context of criminal investigations” or “the interest protected by the relevant law of the third country, including the third country’s interest in preventing disclosure of data”. For example, although in principle this assessment should require an evidence-based assessment in view of all available information given the potential impact of such a decision, at the very least, the wording ("is being aimed to") appears unclear and should be adapted ("has the aim/objective to").

The EDPB regrets that the only case where the authorities of a third country would be consulted and could object to the execution of a production order, would be where this competent EU court would consider that there is a relevant conflict, transmit all the elements to the central authorities in the third country concerned and the central authority of that third country would object within the tight deadlines of maximum 50 days (15 days, possibly extended by 30 days, and after a last possible reminder giving 5 additional days). In all other cases, the competent court would be in a position to uphold the production order and issue a pecuniary sanction of the service provider refusing to execute the order. Consequently, the EDPB is concerned that the competent EU courts will not have a wider obligation to consult the competent authorities of the concerned third countries in order to ensure that the procedure will more systematically ensure that the arguments of both sides will be taken into consideration and to show even more respect for the laws of third countries.

[34] See Art. 48 GDPR

As already underlined in the statement of WP29 and above, the EDPB recalls that particular attention should be paid to the adoption by third countries of similar instruments potentially affecting the rights of data subjects and their right to privacy within the EU, especially the risk of similar instruments that would enter in direct conflict with EU data protection law.

In addition, the EDPB underlines that the competent court of the Member State of the issuing authority may not even be the competent court to enforce the order foreseen under Article 14 of the draft Regulation, which would even increase the risk of conflicting procedures and the lack of counter-checks in a situation of conflicting laws. This comes from the fact that in some cases, three states could be involved: the one of the authority issuing the order, the third country of the service provider, and the Member State where the legal representative of the service provider in the EU is, and where the order would have to be enforced. Consequently, following the procedure currently foreseen, the court of the requesting authority in Member State A could make its own interpretation of the law of the third country B of the service provider without requiring the views of the authorities of this third country (while they would have objected to the order), and ask a court of another EU Member State C to enforce its decision without any possibility to object.

Besides, the EDPB also welcomes the introduction of specific remedies against production orders, in addition to remedies provided for in the GDPR and in the LED. The WP29 already called for such safeguards in its previous statement. However, the EDPB deplores that such remedies are not also foreseen against preservation orders, as these orders may also result in limitations of the fundamental rights of the individuals whose data are retained. Indeed, preservation orders may have the effect of retaining data for longer than they would have according to the data protection rules. Therefore, in itself, the preservation order results in a limitation of the fundamental rights of the concerned data subject, whose justification shall be subject to a review and to specific remedies, especially in cases where the preservation order will have been issued along with a production order to get the data. As recommended by the WP 29 in its statement, legal remedies, at least equivalent to those available in a domestic case should be foreseen.

h) Security of data transfers when responding to an order

The EDPB notes that the draft Regulation only provides for orders to be addressed to recipients within the European Union, and therefore does not provide for any specific channel for the transfer of data between the addressees and service providers located outside of the European Union.

Although the EDPB welcomes the absence of further derogations to the general framework of the EU for data protection, it recalls that any order sent to an addressee which would then imply a transfer outside the EU would need to respect the legal framework provided by the GDPR. Indeed, circumventing the legal framework of judicial cooperation, which provides for data protection safeguards to be respected, should not result as well in the circumvention of data transfer requirements by addressees of production or preservation orders to comply with such orders.

In addition, while the EDPB welcomes the absence of provision imposing an obligation to decrypt encrypted data[35], it is concerned that the draft proposals do not foresee any specific requirement for addressees to assess the authenticity of data produced and underlines that this assessment is also an added value of traditional instruments relying on judicial cooperation and warns against the increased risks posed for data subjects concerned in the absence of such an assessment.

[35] See recital 19 and page 240 of the impact assessment

Conclusions

Based on this assessment, the EDPB wishes to address the following recommendations to the co-legislators:

1) The legal basis of the Regulation should not be Article 82 (1) TFEU.
2) The necessity of a new instrument compared to the existing EIO Directive or MLAT should be better demonstrated, including with a detailed analysis of less intrusive means with regards to fundamental rights such as amendments of these existing instruments or the restriction of the scope of this instrument to preservation orders in combination with other existing procedures to request access to the data.
3) The Regulation should provide for a longer deadline to allow the executing service provider to ensure safeguards with regards to the protection of fundamental rights can be respected.
4) The dual criminality principle should be maintained, especially if the location criteria of the data is abandoned in order to maintain the obligation to take into consideration the safeguards provided in both concerned States (the State of the requesting authority and the State where the service provider is located).
5) The scope of the Regulation should be restricted to controllers in the sense of the GDPR or it should include a provision that in the event where the service provider addressed is not the controller of the data but the processor, the latter is obliged to inform the controller.
6) The Regulation should include safeguards concerning data transfers in case the service provider would be established in a third country without adequacy decision in this field or refer to the directive 2016/680 as these safeguards will be applicable.
7) Since the mandatory designation of a legal representative differs from the GDPR, the Regulation should precise that, the legal representative designated under the e-Evidence Regulation should be distinct from the one designated under article 3 (2) of the GDPR.
8) The Regulation should contain a broader definition of electronic communication data in order to ensure that the appropriate safeguards and conditions for access to be established cover both non-content and content data.
9) The Regulation should raise thresholds for issuing orders and orders shall be issued or authorised by courts, except for subscriber data provided the definition of this category of data is drastically narrowed to very basic information allowing only to identify a person without involving access to any communication data.
10) The Regulation should restrict the access to subscriber and access data to a list of crimes strictly established or at least to “serious criminal offenses”.
11) The time limit to provide data, especially in case of emergency should be better justified in the Regulation, and the possibility to use a fast6-hour procedure should include the obligation for requesting authorities to demonstrate the emergency triggering the use of this procedure, even a posteriori, in order to allow for a control of the use of such exceptional powers.
12) The procedure allowing the production of content data without any involvement of the competent authorities of the Member State where the data subject is, should be abandoned.
13) Safeguards surrounding the issuing of European Preservation Orders should be improved in the Regulation.
14) The Regulation should at least include the minimum classic derogation that if there is substantial grounds for believing that the enforcement of an Order would result in a breach of a fundamental right of the person concerned leading the executing State to disregard its obligations concerning the protection of fundamental rights recognised in the Charter, the enforcement of the order should be refused.

15) The Regulation should foresee a broader obligation to consult the competent authorities of a third country where the service provider requested to provide data is located in case of conflict of laws in order to avoid subjective interpretations from a single court.
16) The validity and duration of preservation orders should be more linked to the production orders accompanying them.
17) The security of data transfers should be better guaranteed.
18) The verification of the authenticity of the data should be foreseen, in particular where encrypted data could be provided.

For the European Data Protection Board

The Chair

(Andrea Jelinek)