Statement of the Article 29 Working Party

Brussels, 29 November 2017

Data protection and privacy aspects of cross-border access to electronic evidence

On 8th June 2017, the European Commission issued a non-paper presenting several options aiming at allowing direct access to data retained by telecommunications and information society services providers for law enforcement authorities. The aim of the forthcoming legislative proposal contemplated would be to speed access to relevant electronic evidence.

On 4th August 2017, the European Commission launched a public consultation on "improving cross-border access to electronic evidence in criminal matters", which was closed on 27th October 2017.

In addition, the European Commission has sought the views of data protection authorities through a dedicated expert meeting in order to assess possible options for the reform of the current legal framework, both for cooperation with service providers and for direct access to data by law enforcement authorities.

A. General remarks

The options currently considered for the future instrument vary widely in terms of personal, material and territorial scope, which makes it difficult for the WP29 to assess the various scenarios contemplated in the non-paper issued by the Commission. However, the WP29 wishes to reiterate key principles related to the protection of personal data and privacy, the necessity to align any future proposal with the related EU *acquis* and case-law, and to raise some concerns about the impact of the solutions envisaged in terms of data protection law. Furthermore, any relevant jurisprudence of the European Court of Human Rights will also have to be taken into account when assessing the proposed legislation.

The inception impact assessment made by the Commission mentions Article 82 (1) and (2) TEU as the appropriate legal basis for the adoption of the new legislation on cross-border access to e-evidence[1]. The WP29 has doubts on the choice of such a legal basis, since Article 82 TEU relates to cooperation between judicial and police authorities of different Member States, while the envisaged options in the non-paper of the Commission do not involve the police or judicial authorities of another Member State or a non-EU country. This has already been raised by the Court of Justice in the Opinion 1/15 on the EU-Canada PNR agreement[2].

a. The restriction to the right to data protection

Law enforcement access to personal data, such as subscriber information, metadata (including traffic data, location data and access logs) and content data, constitute an interference with the right to privacy, guaranteed under Article 7 of the Charter, and with the right to the protection of personal data, guaranteed under Article 8 of the Charter. In this regard, it must be recalled that, under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of these rights and freedoms. With due regard to the

[1] See inception impact assessment, page 2.

[2] Case 1/15, 27 July 2017, §103: *"As the Advocate General has observed in point 108 of his Opinion, none of the provisions of the envisaged agreement refer to facilitating such cooperation. As for the Canadian Competent Authority, that authority does not constitute a judicial authority, nor does it constitute an equivalent authority".*

principle of proportionality, limitations may be imposed on the exercise of these rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others[3].

Under the current EU legal framework, the possibility for Member States to foresee limitations of the rights to data protection and to privacy are already provided for by EU law. ***With respect to data processed by telecommunications and information society service providers*** (which are the services that would be subject to the envisaged measures), Article 13 of Directive 1995/46/EC and Article 15 of Directive 2002/58/EC already state to which extent such limitations are acceptable[4].

With respect to personal data processed by law enforcement authorities, Directive 2016/680, which will effectively apply as of 8th May 2018, also provides for a specific data protection regime when data are processed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. Chapter III of this instrument also provides for the possibility to adopt national measures to limit the rights of data subjects when such measures are necessary and proportionate in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned.

- **The WP29 calls on the Commission to align any envisaged proposal with the principles stated in the provisions of the GDPR, the law enforcement Directive and the ePrivacy framework, taking into account the relevant case law at European level.**

b. The existing instruments on cross-border access to electronic evidence

Council of Europe Budapest Convention on Cybercrime

The assessment of legislative options for cross-border access to electronic evidence should also take into account the existing Council of Europe Budapest Convention on Cybercrime, and in particular its Article 32, for which the WP29 has already given its interpretation with regard to its implementation and the articulation with the EU *acquis* and the EU Charter of Fundamental Rights[5]. In this context, the WP29 is following the work of the Cybercrime conference on the drafting of an additional Protocol to the Budapest Convention on an "Enhanced international cooperation on cybercrime and electronic evidence"[6]. The WP29 is concerned that the initiative of the Council of Europe, conducted in parallel to

[3] CJEU Judgement of 15 February 2016, N., C‑601/15 PPU, EU:C:2016:84, paragraph 50. See also "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit", EDPS, 11 April 2017, available at https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[4] As of 25th May 2018, Article 23 of Regulation 2016/679 will apply. In the Commission Proposal for a "e-Privacy regulation", repealing Directive 2002/58/EC, Article 11 states that "Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests." (see Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003 (COD)).

[5] Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime, 05/12/2013

[6] See https://rm.coe.int/t-cy-pd-pubsummary/168076316e.

the work of the EU on this matter, could lead to an instrument which might not be compatible with the legislative initiatives of the Commission, or with the EU *acquis* regarding data protection already recalled above.

- **The WP29 invites the Commission to follow the work of the Cybercrime committee on the drafting of an additional Protocol to the Budapest Convention in order to make sure that both instruments are compatible with the EU law and case-law.**

European Investigation Order Directive

The WP29 also notes that the European Investigation Order Directive[7] was adopted in April 2014 and was supposed to be implemented by the Member States by 22 May 2017. This instrument aims at making the access to data in the territory of another Member State easier. The impact of this new instrument in the field of cooperation cannot yet be performed in order to assess the necessity of another legislative proposal in this respect. The WP29 considers that the impact assessment[8] of the Commission should take the European Investigation Order Directive into account before adopting any measure that might have the same effect.

- **Therefore, the WP29 invites the Commission to take into consideration and assess the potential impact of the Directive on the European Investigation Order on the access to e-evidence located in another Member State before proposing new legislative measures which might overlap with the effects of the Directive on the European Executive Order.**

National procedural laws of Member States

With regards to the means to access e-evidence, the Commission should furthermore clarify whether the future instrument will aim at harmonizing the powers of competent national authorities or merely allow them to use the power they already have towards controllers established outside their territory, either within or outside the EU.

- **The WP29 recommends to clarify the respective procedural rules governing access to e-Evidence at national and European level in order to ensure that the competent authorities will not have different powers and competence depending on the location of the controller who will receive the production order/request.**

B. Additional comments

Against the legal background mentioned above and taking into account the recent case law at European level, in particular the CJEU judgment of 21st December 2016 in joined cases C-203/15 and C-698/15, the WP29 wishes to express a number of observations and reservations regarding the different legislative options currently considered by the Commission and for which experts views have been sought.

a. Personal and material scope

[7] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *O.J.*, 1 May 2014, L 130/1.
[8] See the inception impact assessment https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en.

The legislative options suggested vary significantly concerning the categories of data to be accessed, as well as the type of service providers to be covered and compelled under the future instrument. In its technical documents, the Commission acknowledges the lack of precise definition and interpretation of what is understood by "electronic evidence" and the need to define specific categories of electronic evidence. Such a definition is essential in order to assess the impact of the measures foreseen on the rights of the data subject and on the obligations incumbent to law enforcement authorities and service providers.

On the categories of data concerned and associated safeguards

On the question of the material scope of the future instrument, the WP29 reiterates 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[9].

The Commission in its considered options for production requests/orders, differentiates the procedural safeguards for "non-content" data (subscriber data and metadata) and for content data. However, the Commission did not provide for a precise definition of the different categories of data to be considered under each legislative option.

Furthermore, 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*".

The WP29 therefore expresses doubts about the current delineation between "non-content" and content data as foreseen among the legislative options considered and reminds that metadata may reveal very sensitive data, in line with the considerations of the ECJ in *Digital Rights Ireland*[10] and *Tele2/Watson*[11].

- **As 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 to electronic evidence, the WP29 recommends that a broader definition of electronic communication data, which include metadata, applies to the future proposal, in order to ensure that the appropriate safeguards to be established also covers metadata.**

- **The WP29 also highlights that a precise definition of "subscriber data" is currently lacking in order to assess the direct impact of the measures envisioned on the affected persons' rights to data protection and privacy.**

On the type of service providers covered

[9] Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others EU:C:2003:294, paragraph 75
[10] CJEU Judgement of 8th April 2014 in joined cases C-293/12 and C-594/12
[11] CJEU Judgement of 21st December 2016 in joined cases C-203/15 and C-698/15

Regarding the categories of service providers to be covered by a future instrument, the WP29 reminds the views already expressed in its opinion WP 247, stating that Over-The-Top (OTT) services are functionally equivalent to more traditional communication services and therefore have a similar potential to impact on the privacy and right to secrecy of communications of EU citizens[12].

- **The WP29 thus recommends that substantive and procedural conditions for access to electronic evidence cover both traditional communication services and Over-The-Top (OTT) services in order to ensure a consistent application of the appropriate safeguards to be established.**

b. Territorial scope

The Commission legislative options also include various scenarios depending on the establishment of the service providers and location of the data to be accessed, which imply different consequences related to the competent jurisdictions, as well as the exercise of the rights of the person affected.

The WP29 stresses that the location of the data is not the criterion used under the GDPR to define its territorial scope. The GDPR is indeed applicable when the controller or processor is established in the EU or, if the controller/processor is established outside of the EU, when the processing is targeting individuals in the EU[13].

On production requests/orders to service providers established within the EU

The WP29 stresses that the envisioned production requests/orders to service providers established in the EU must take into account the existing and future EU data protection framework, as well as procedural safeguards as per the EU *aquis*. In this regard, whichever option is finally proposed, the establishment of production requests/orders to service providers established in the EU will notably need to ensure appropriate safeguards equivalent to the existing European Investigation Order (EIO).

In particular, from a data protection perspective, the common conditions and minimum safeguards for production requests/orders within the EU should also include inter alia the following elements:

- The possibility for the service provider to object the production request/order, should it result in a breach of a fundamental right of the person concerned;
- The information to be made available or given to the data subject, in accordance with Chapter III of Directive 2016/680, in particular to provide him/her with the right to object the production request/order on specific legal grounds;
- The availability of legal remedies, at least equal to those available in a domestic case.

On production requests/orders to service providers established outside the EU

Legislative options considered by the Commission also include production requests/orders that would directly compel service providers established outside the EU, outside the framework of potential existing mutual legal assistance treaties or international agreements.

Production requests/orders addressed to service providers established outside the EU would have to ensure appropriate safeguards at least equivalent to existing mutual legal assistance treaties or international agreements, and should comply with the application of Article 32 of the Council of Europe Convention on cybercrime, as interpreted by the WP29. In particular, the application of Article 32

[12] WP29 Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 04/04/2017
[13] See Article 3 GDPR.

provides that data controller "*can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required. Data controllers cannot lawfully provide access or disclose the data to foreign law enforcement authorities that operate under a different legal and procedural framework from both a data protection and a criminal procedural point of view.*"[14]

Establishing an EU legal framework that would compel service providers established outside the EU on the basis of a direct order issued by a Member State authority would contradict the current interpretation of Article 32 of the CoE Convention on Cybercrime, developed to ensure that the application of this Convention does comply with the EU data protection *acquis*.

The WP29 is concerned that the adoption of an instrument compelling organizations not subject to the jurisdiction of an EU Member State would conflict with the applicable law and jurisdiction of the country where the organization is established. The organization subject to a production request/order could indeed be facing a conflict of laws, if the third country where it is established already has a legislation protecting personal data that prohibits the transfer of such data under similar conditions to the GDPR.

- **The WP29 expresses concerns at the envisioned option of production requests/orders that would directly compel service providers to provide data located outside the EU, potentially conflicting with third countries jurisdictions and applicable law, and contradicting the current interpretation of Article 32 of the CoE Convention on Cybercrime.**

Furthermore, the WP29 notes the obligation to appoint a legal representative under the envisaged legislative measure regarding cross-border access to e-evidence when the service provider is not established in the EU. In this regard, the WP29 would like to stress that any confusion should be avoided between this legal representative and the one that has to be designated under Article 27 of the GDPR.

While the legal representative under the GDPR is meant to be the contact point of the Supervisory Authorities of the controllers or processors for the performance of their obligations, the representative under the envisaged measure aims to enforce the production order issued by the competent authority. The two functions seem therefore to cover different responsibilities and tasks. Moreover, the circumstances under which the representative under the GDPR has to be designated will not be the same as the ones under which the legal representative would be appointed under the envisaged measures. For these reasons, the WP29 invites the Commission to clearly distinguish the two functions and roles in the legislative proposals to be adopted in the coming months.

c. Substantive and procedural conditions for direct access to personal data

A series of legislative options also considered by the Commission foresee the possibility for law enforcement authorities to access (and in some cases copy) the data directly from a computer system. These options are also echoing the ongoing discussions for an additional protocol to the Budapest Convention on Cybercrime.

[14] Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime, 05/12/2013

The WP29 reiterates that such direct access cannot be established outside of, or in contradiction with, the current EU data protection framework and reminds the necessary substantive and procedural conditions for access to personal data under EU and European case law.

On open search with the agreement of the person

Several consultation documents refer to an "open search with or without the agreement of the affected person". While the Commission highlights that the consent for access or to receive stored computer data, in the sense of Article 32(b) of the Budapest Convention, does not refer to the consent of the individual for the processing of personal data, several references to "the affected person" seem to imply that for certain legislative options the consent of a data subject could be considered as a legal ground for access.

The WP29 wishes first to remind that, as per recital 35 of Directive 2016/680, *"the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties."* In addition, any future instrument is to comply with the EU *aquis* in the field of procedural rights and in particular Directive 2016/343 the strengthening of certain aspects of the presumption of innocence which notably codifies the application of the right not to incriminate oneself.

Furthermore, as already stated by the WP29 in its interpretation of the application of Article 32 of the Budapest Convention on Cybercrime, companies acting as data controllers usually do not have the "lawful authority to disclose the data" which they process for e.g. commercial purposes according to the EU data protection *acquis*, and that consent should be sought to the competent law enforcement or judicial authorities within the data controller jurisdiction

- **The WP29 recalls that consent of a data subject cannot be considered as a legal ground for law-enforcement access to electronic evidence.**
- **The WP29 also recalls that in a law enforcement context, "consent" is understood to be the consent of law enforcement/judicial authorities that need, in relation to a specific case, to exchange data[15].**

On open search without the agreement of the person

In its judgment in In joined cases C‑203/15 and C‑698/15 (Tele2/Watson), the CJEU confirmed that mandatory requirements of EU law are applicable to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of the Charter, and that such requirements apply regardless of the extent of the obligation to retain data that is imposed on providers of electronic communications services.

[15] See in particular Article 11 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters: "prior consent of the transmitting Member State"

The judgment notably states that access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. In light of this reasoning, the WP29 deplores that no limitation to serious forms of crimes has been foreseen yet for any of the legislative options currently considered.

The current EU legal framework and the most recent case law can furthermore allow the development of a list of substantive and procedural conditions to be taken into account for any future instrument governing law enforcement access to personal data:

- The conditions under which the providers of electronic communications services must grant such access must be **provided by law**.
- Individual access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of **individuals suspected** of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.
- Access of the competent national authorities to data should, as a general rule, except in cases of validly established urgency, be subject to a **prior review carried out either by a court or by an independent administrative body**.
- In **particular situations**, where for example vital national security, defense or public security interests are threatened by terrorist activities, **access to the data of other persons might also be granted** where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.
- The **competent national authorities to whom access to the data has been granted must notify the persons affected**, under the applicable national procedures, **as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities**[16].
- Notification is necessary to **enable the persons affected to exercise**, inter alia, their right to a legal remedy.

➢ **The WP29 could not identify any element supporting the existence of such conditions in the legislative options currently envisioned by the Commission. The WP29 recalls that, in the absence of such guaranties, any envisioned instrument for direct access to electronic evidence would fail to comply with the requirements of EU law.**

[16] Article 13 (3)of the Police Directive states the conditions under which Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject.

C. Conclusion and further considerations

The WP29 will examine closely the Commission proposal once adopted. In light of the preliminary assessment of the different options considered, the WP29 recalls the necessity to ensure that the future legislative proposal fully complies with the existing EU data protection *acquis* in particular, as well as EU law and case-law in general.

While the adoption of a future instrument regulating law enforcement access to electronic evidence should take into account the international dimension of its remits, a particular attention should also be paid to the adoption by third countries of similar instruments potentially affecting the rights to data protection and to privacy within the EU. In this regard, the WP29 expresses concerns that **the adoption of the envisaged production order towards organizations which are not established in the EU could also increase the risk of adoption by non-EU countries of similar instruments that would enter in direct conflict with EU data protection law**.

Such developments are currently observed in the United States, with legislative proposals made to grant direct access to electronic evidence stored in third countries, in addition to the Supreme Court decision to review the decision in the Microsoft warrant case. In this context, the WP29 takes the opportunity to remind that, in line with Article 48 of the GDPR, *"any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter*".

The WP29 therefore recalls that EU data protection law provides that existing international agreements such as a mutual assistance treaty (MLAT), must – as a general rule - be obeyed when law enforcement authorities in third countries request access or disclosure from EU data controllers. The circumvention of existing MLATs or other applicable legal basis under EU law by a third country's law enforcement authority is therefore an interference with the territorial sovereignty of an EU member state. Vice versa, EU law enforcement authorities should also - as a general rule - be required to respect existing international agreements such as MLATs or any other applicable legal basis under EU law when requesting access or disclosure from data controllers in third countries.

Furthermore, the WP 29 stresses that the envisaged EU instrument for access to electronic evidence shall not change the existing EU data protection legal framework for controllers when faced with a request from a third country law enforcement authority.