ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence

1. Impact of the US CLOUD Act on the EU legal framework for the protection of personal data

The US Congress enacted the US CLOUD Act in March 2018 in the context of a pending case before the US Supreme Court (the "Microsoft Ireland" case)[1] to clarify that according to US law, US authorities have the right to require the production of data stored abroad by a service provider subject to US jurisdiction, thus "mooting" the case.

By choosing to create a legal avenue under US law for US law enforcement authorities to require disclosure of personal data directly from service providers who fall under US jurisdiction, irrespective of where the data is stored, the US Congress enacts into US law a practice of US governmental entities likely to bypass the Mutual legal assistance in criminal matters treaty (MLAT)[2] in force between the European Union and the United States of America[3].

The main objective of the US CLOUD Act is to allow for efficient investigations of US law enforcement authorities by ordering electronic communications services providers or remote computing service providers to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within their possession, custody or control (hereafter "*control*"), "*regardless of whether such communication, record, or other information is located within or outside of the United States*"[4]. The US CLOUD Act therefore entails the possibility that such electronic communication or remote computer service providers are compelled to answer a request by US law enforcement authorities for the disclosure of personal data that are subject to the provisions of the GDPR[5].

The US CLOUD Act provides for a procedure for service providers to file a motion to "*quash*" (annul) or modify an US CLOUD Act warrant, in limited circumstances and subject to several conditions. Most importantly, the US CLOUD Act limits this avenue to providers claiming that the request would violate the law of a country that has entered into executive agreements with the US, and to requests involving data concerning non-US persons. To what extent service providers may and will effectively

[1] See: https://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/
[2] See: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719(02)&from=EN
[3] Cf. the view of the Council of Bars and Law Societies of Europe (CCBE) in its Amicus Curiae brief in the USA v Microsoft corporation case, p. 14, and section B p. 26 and seq.
[4] The US Department of Justice further explained the US CLOUD Act in a White Paper "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act", dated April 2019 and available here: https://www.justice.gov/opa/press-release/file/1153446/download
[5] The EDPB also highlights that, in most cases, where request from a US court or authority which, by virtue of the CLOUD Act, would require the disclosure of personal data that are subject to the GDPR, such personal data being in possession, custody, or control of a provider of electronic communication service or remote computing service is likely to be subject to the provisions of Directive 2002/58/CE concerning the processing of personal data and the protection of privacy in the electronic communications sector.

oppose the order on the ground of "*common law comity*"[6], when such agreements are not in place is unclear.

According to the US Department of Justice, "*[a] request to issue a warrant must be submitted to an independent judge for approval. The judge cannot authorize the warrant unless he or she finds that the government has established by a sworn affidavit that "probable cause" exists that a specific crime has occurred or is occurring and that the place to be searched, such as an email account, contains evidence of that specific crime. Further, the warrant must describe with particularity the data to be searched and seized; fishing expeditions to see if evidence exists are not permitted*"[7]. We note here that the CLOUD Act does not authorise any systematic, large scale and/or indiscriminate collection of personal data, but rather governs targeted requests, subject to procedural safeguards, concerning specific law enforcement investigations.

However, the US CLOUD Act also extends the possibility to request data wherever they are stored or located to the whole of Chapter 121 of USC Title 18 on "Stored wired and electronic communications and transactional records access"[8]. To our understanding, this means that this applies to many other data collection avenues, in particular to requests to access content data through a court order or a subpoena (either administrative, grand jury or trial subpoena)[9]. It also applies to requests for non-content data[10] (so-called "metadata") under §2703 of Chapter 121 USC Title 18[11], which covers (subsection (c)) a whole range of avenues, including warrants and court orders, but also avenues that do not necessarily require judge intervention or a probable cause test, such as formal written requests or subpoenas. Furthermore, the US CLOUD Act opens the possibility for service providers to "intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government" (this covers real-time interception) under the condition that this foreign government has entered into an executive agreement with the US[12].

Other questions regarding the scope of application of the US CLOUD Act remain to be resolved, (*e.g.* whether it applies to EU operators with some "presence" in the US, and how the concept of "control" is to be interpreted in practice, in particular with regard to affiliated companies of US based companies, established in the EU).

The US CLOUD Act thus states an extraterritorial reach of powers under the US Stored Communication Act. Therefore, service providers controlling personal data whose processing is subject to the GDPR or other EU or Member States' law will be susceptible to facing a conflict of laws between US law and the GDPR and other applicable EU or national law of the Member States.

---

[6] As opposed to the fixed procedure for "*Comity analysis of legal process seeking content of wire or electronic communication*" introduced by the US CLOUD Act where an executive agreement between a foreign government and the US has entered into force.

[7] Id., at p. 8.

[8] See new §2713 as inserted in Chapter 121 of USC Title 18 by the US CLOUD Act.

[9] See USC Title 18 Chapter 121, §2703 subsection (b).

[10] The EDPB recalls that in relation to "non-content data" which encompass subscriber data, access data and transactional data, the CJEU has ruled in its judgement in joined cases C-203/15 and C-698/15Tele2 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.

[11] §2703 sets rules about "Required disclosure of customer communications or records ". Its subsection (c) allows service providers to disclose to US law enforcement authorities 6 categories of personal (meta)data: « (…) (A) name ; (B) address ; (C) telephone connection records or records of sessions times and durations ; (D) length of service (including start data) and types of service utilized ; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address ; (F) means and source of payment for such service (including any credit card or bank account number) (…) ».

[12] See new subsection (i) as inserted in Chapter 119 « Wire and electronic communications interception and interception of oral communications » of USC Title 18 by the US CLOUD Act.

Article 48 GDPR ('Transfers or disclosures not authorised by Union law') provides that any judgment of a foreign court or any decision of a foreign administrative authority requiring a controller or a 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 MLAT, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to [Chapter V]*". Article 48 GDPR sets the conditions under which such judgement or decision from a third country authority may be enforceable under EU or Member State law. The title of Article 48 furthermore reflects the legislators' intention to enshrine by law a protection against unauthorised access to personal data.

As the European Commission has argued, "*Article 48 makes clear that a foreign court order does not, as such, make a transfer lawful under GDPR*"[13]. A request from a foreign authority does not in itself constitute a legal ground for transfer. The order can only be recognised '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'.

In the absence of such framework provided by an international agreement (such as the EU US MLAT or a MLAT between a Member State and the US in the context of a US CLOUD Act request) or another legal basis under the GDPR, service providers subject to EU law cannot legally base the disclosure and transfer of personal data to the US on such requests[14]. The EDPB therefore reiterates its position expressed in its guidelines on Article 49 GDPR[15] that: "*In situations where there is an international agreement such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to an existing mutual legal assistance treaty or agreement*". Indeed, we consider that where disclosure of personal data is compelled by a third-country authority, the MLAT process must ensure that data is disclosed in compliance with EU law, and under the supervision of the courts in the EU.

We recall that in cases where service providers are directly addressed by US law enforcement authorities, the related transfer of personal data would not be subject to the provisions of the EU-US Privacy Shield adequacy decision[16], nor to the EU-US Umbrella Agreement[17]. Neither instrument is applicable to transfers in this context and they are therefore not taken into account in this analysis.

It follows from the above that any order under the CLOUD Act for transfer of personal data from the EU could only be lawful if there is a legal basis under Article 6 and Article 49 of the GDPR[18].

This two-step test must be applied when it comes to any transfer of personal data to third countries as per the GDPR: first, a legal basis must apply to the data processing as such together with all relevant

---

[13] See European Commission's Amicus Curiae brief in USA v. Microsoft corporation p. 14. https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf

[14] Where disclosure of personal data is compelled by a third-country authority, the MLAT process ensures that data is disclosed in compliance with EU law, and under the supervision of the courts in the EU.

[15] See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 5. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en

[16] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance).

[17] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences.

[18] The European Commission takes the view that some derogations under Article 49 GDPR might be used, depending on the circumstances of the case (See European Commission's Amicus Curiae brief in USA v. Microsoft corporation, p. 15).

provisions of the GDPR; and as a second step, the provisions of Chapter V must be complied with. Hence, the processing as such (i.e., the disclosure of personal data) must comply with general principles as per Article 5 GDPR and must rely on a legal basis as per Article 6 GDPR. We will examine successively whether and to what extent certain of the lawful grounds under Article 6 (step 1) and Article 49 (step 2) can be applied in case of US CLOUD Act requests.

Step 1. Lawfulness of processing under Article 6

In accordance with Article 6 GDPR, the lawfulness of processing can be ensured if validly relying on one of the legal basis laid down in Article 6(1). The relevant legal basis have been assessed in the context of a request from a US court or authority which, by virtue of the CLOUD Act, would require the disclosure by data controller or processor of personal data the processing of which is subject to the GDPR.

Article 6(1)(c) - processing is necessary for compliance with a legal obligation to which the controller is subject: Under Article 6(3) GDPR, such legal basis for processing should have a basis in Union or Member State law. As per Article 48 GDPR, a request from a US law enforcement authority may only be recognised or made enforceable if based on an international agreement, such as a mutual legal assistance treaty, which may then give such request the effect of a legal obligation to which the controller is subject, as per Article 6(1)(c). In this context, a lawful ground for processing may be provided in or on the basis of a future international agreement concluded between the EU and the US, as notably recommended by the European Commission[19].

Article 6(1)(d) - processing is necessary in order to protect the vital interests of the data subject or of another natural person: We recognise that in specific and established circumstances, the vital interests of the data subject could be cited as a legal basis to reply to a US CLOUD Act request on the condition that the conditions set out in international law are met. This could for instance be the case of requests to access personal data concerning abducted minors or other obvious situations where the transfer is in the vital interest of data subjects themselves.

Furthermore, Article 6(1)(d) envisages the processing of personal data in order to protect the vital interests of a person other than the data subject, which could encompass the transfer of personal data of data subjects on the basis of a direct foreign request in a situation where an imminent threat to the life or physical integrity of other persons in a third country could be validly established. However, following Recital 46, the transfer of personal data "based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis". In the specific case of US CLOUD Act requests, we consider that the vital interests of other persons should not, in principle, be used as a valid legal basis to process personal data of such data subjects since there are other legal basis available for such transfers under EU law, i.e. the EU-US MLAT.

Article 6(1)(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller: We consider that Article 6(1)(e) may not constitute a valid legal basis on which processing could rely when disclosing data solely on the basis of a compelling request from an US authority under the CLOUD Act. As stated above in relation to Article 6(1)(c), where processing is necessary for the performance of a task carried out in the public

[19] Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 05/02/2019, COM(2019) 70.

interest or in the exercise of official authority, according to Article 6(3) GDPR, the processing should have a basis in Union or Member State law.

Article 6(1)(f) - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data: We recall that the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject. The outcome of the balancing test determines whether Article 6(1)(f) may be relied upon as a legal ground for processing[20].

- *Legitimate interest pursued by the data controller or third party*: A data controller may have a legitimate interest in complying with a request to disclose personal data from a US law enforcement authority, in particular if non-compliance with such request would entail sanctions under US law. The GDPR also considers that "The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned"[21] and that "Indicating possible criminal acts or threats to public security by the controller and transmitting relevant personal data in individual cases or in several cases relating to the same criminal acts or threats to public security to a competent authority should be regarded as being in the legitimate interests pursued by the controller"[22]. However, it is to be underlined that US law enforcement authorities are not public or competent authorities established under EU law.

- *Interests or fundamental rights and freedoms of the data subject*: We recall that assessing the impact on the data subject's interests shall take into account any possible (potential or actual) consequences of the data processing for the data subject, the data protection principles of proportionality, as well as elements such as, for example, the seriousness of the alleged offences that may be notified, the scope of the request, applicable standards and procedural guarantees in the US, and applicable data protection safeguards. Such assessment shall also pay particular attention to the nature of the personal data processed and the way personal data are being processed[23]. In addition, the GDPR also introduced the necessity to take into account the reasonable expectations of the data subject.

Taking into account the elements above, and considering in particular that US law enforcement authorities request for access would occur in the absence of a framework provided by an international agreement, we consider that data subjects may be deprived from the protection afforded by the provision of Article 47 of the Charter, such as the right to an effective remedy, or that this right could not be exercised in practice. In addition, the reliance of such direct access on the legitimate interest of the data controller could result in the abandonment of the dual criminality principle, thus depriving data subjects of the related protections and safeguards. In this context and in line with positions previously taken by the WP29, the EDPB and the EDPS take the view that the interests or fundamental rights and freedoms of the data subject would override the controller interest such as not to be sanctioned by the US for eventual non-compliance with the request.

[20] Article 29 Working Party's Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014.
[21] Recital 47 GDPR.
[22] Recital 50 GDPR.
[23] Such assessment shall be based on the methodology referred to in the Article 29 Working Party opinion 06/2014 on the notion of legitimate interests.

It must also be considered that the compelling nature of US law enforcement authorities' request would make it impossible in practice for controllers to comply with their obligations related to the exercise of the different data subjects' rights provided by the GDPR when processing relies on Article 6(1)(f), including the right to object. They would need to act on the basis of limited information, which is due to the nature of the requests. Consequently, service providers receiving requests from US law enforcement authorities would unlikely be able to appropriately perform the required assessment of all the circumstances and possible consequences of such data processing for the data subject(s). We therefore take the view that the difficulty of applying such balance of interests is a strong argument against leaving the performance of such tests to private operators.

Furthermore, the EDPB has recently noted in the case of the proposed rules on European Production and Preservation Orders for electronic evidence in criminal matters, 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 it also results in the inapplicability of certain procedural guarantees foreseen in the context of judicial cooperation for individuals, as well as for companies themselves"*[24].

Step 2. Derogations for transfers under Article 49

The second part of the two-step approach regards the compliance of disclosure following US CLOUD Act requests with the provisions of Chapter V of the GDPR for transfers of data to third countries. This requires examination of the derogations provided for in Article 49 GDPR[25]. Any derogation is to be interpreted strictly so that the exception does not become the rule[26].

In particular, we have considered relevant to examine to which extent such a transfer could be seen either as "*necessary for important reasons of public interest*" under Article 49(1)(d), or "*necessary for the establishment, exercise or defence of legal claims*" under Article 49(1)(e), or "*necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent*" under 49(1)(f) or "*necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject*" under Article 49(1) last paragraph[27].

Article 49(1)(d) - transfer necessary for important reasons of public interest: It is important to recall that Article 49(4) GDPR states that only public interests recognised in Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation, meaning that the public interest of a third country as such is of no incidence. For the application of this derogation, it is not sufficient that the data transfer is requested (for example by a third country authority) for an investigation which serves a public interest of a third country which, in an abstract sense, also exists in EU or Member State law.

Article 49(1)(e) - transfer necessary for the establishment, exercise or defence of legal claims: Regarding Article 49(1)(e) according to which, as another derogation, personal data may be

[24] 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.

[25] The European Commission takes the view that some derogations under Article 49 GDPR might be used, depending on the circumstances of the case (See European Commission's Amicus Curiae brief in USA v. Microsoft corporation p. 15).

[26] See CJEU, Case c-119/12 Probst v. mr.nexnet GmbH, para. 23 ECLI:EU:C:2012:748, cit. in European Commission's Amicus Curiae brief in USA v. Microsoft Corporation, p. 16.

[27] This provision contains additional conditions which are the following: - and only if the transfer is not repetitive, if it concerns a limited number of data subjects, and if the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

transferred to a third country if "*necessary for the establishment, exercise or defence of legal claims*", where the transfer is "*occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies*" (as explained in Recital 111 GDPR). The EDPB has stated in its guidelines that this covers a range of activities, for example in the context of a criminal or administrative investigation in a third country where the derogation may apply to a transfer of data for the purpose of defending oneself or for obtaining a reduction or waiver of a fine legally foreseen. As explained by the EDPB Guidelines, a close link is necessary between a data transfer and a specific procedure and the derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal proceedings may be brought in the future.

Article 49(1)(f) - transfer necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent: As already explained under Article 6(1)(d), we recognise that in certain exceptional, specific and necessary circumstances, the vital interests of the data subject could be validly used as a legal basis to answer US CLOUD Act requests. The same reasoning applies under Article 49(1)(f). The circumstance that data subjects should be physically or legally incapable of giving consent (a condition not mentioned under Article 6(1)(d)) may not exclude situations where the data subject is constituting an imminent threat to the life and physical integrity of other persons[28], providing that sufficient information is provided to establish the validity of transfer in such circumstances. However we reiterate that in the case of US CLOUD Act requests, since there are manifestly other legal basis available for such transfers under EU law, i.e. the EU-US MLAT, the vital interests of other persons should not, in principle, be used as a valid legal basis to process personal of data subjects constituting an imminent threat to the life and physical integrity of other persons.

Article 49(1) last paragraph - transfer necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject: We observe that the conditions set forth under Article 49(1) last paragraph GDPR are setting a particularly high threshold, which is higher than the one of Article 6(1)(f)[29]. Beyond the difficulties for controllers to perform the balancing test already expressed in relation to Article 6(1)(f), there are a number of obstacles to the applicability of this derogation in any situation of US CLOUD Act requests. In particular, Article 49(1) last paragraph imposes a number of cumulative conditions to be met, among which the provision of suitable safeguards by the controller when transferring the data and the obligation to notify both the supervisory authority and the data subject of the transfer and on the compelling legitimate interests pursued. The notification requirement, whether to the Supervisory authority and to the data subject, appears incompatible with "protective orders" often joined to US CLOUD Act warrants, which aim at maintaining the secrecy of the request (in order to avoid compromising the investigation). In any event, the requirement for controllers to provide "suitable safeguards" to the transfer cannot be applied in practice. Therefore, the EDPB and the EDPS consider that Article 49(1) last paragraph cannot provide a valid lawful ground to transfer personal data on the basis of US CLOUD Act requests.

---

[28] In accordance with EU law, and in particular Directive 2016/680, the performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, 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.

[29] See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 15. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en

Conclusions

In light of the initial legal analysis above, the EDPB and the EDPS consider that an international agreement containing strong procedural and substantive fundamental rights safeguards appears the most appropriate instrument to ensure the necessary level of protection for EU data subjects and legal certainty for businesses.

Currently, unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, and therefore can be recognised as a legal obligation, as per Article 6(1)(c) GDPR, the lawfulness of such processing cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject on the basis of Article 6(1)(d) read in conjunction with Article 49(1)(f).

Furthermore, the analysis and conclusion above does not detail other GDPR provisions to be taken into account by controller or processor subject to a US CLOUD Act request, such as the processor obligations as per Article 28(3) and in particular with regard to the processing on documented instruction from the data controller and the transfers of personal data to third country.

We wish to recall that this initial assessment is valid in particular in relation to US CLOUD Act requests and we recognise the need for further analysis with regard to the issues raised in this legal assessment. However we recommend to controllers and competent authorities that they follow this initial assessment in particular in relation to US CLOUD Act requests.

Other impacts

In any case, the conditions for admission under Article 49 provisions of a personal data transfer operated on the basis of an US CLOUD Act request will need careful consideration and may be very difficult to meet, because these derogations are narrow and are to be interpreted strictly[30]. In addition, as some Member States' national legislation (so-called "*blocking statutes*") prevent EU service providers to disclose information to a third country, the US CLOUD Act might also enter into conflict with these important rules.

The US CLOUD Act might also circumvent the protections granted under the Protocol on Privileges and Immunities of the European institutions[31], which prevents cloud service providers from disclosing personal data entrusted to them by European institutions to law enforcement authorities[32]. The EDPS underlined such issues in its Guidelines on the use of cloud computing services by European institutions and bodies published on 16 March 2018[33]. More generally, the issue of diplomatic privileges and immunities could also concern representations of EU Member States.

---

[30] See CJEU, Case c-119/12 Probst v. mr.nexnet GmbH, para. 23 ECLI:EU:C:2012:748, cit. in European Commission's Amicus Curiae brief in USA v. Microsoft Corporation, p. 16.

[31] Protocol (No 36) on the Privileges and Immunities of the European Communities (1965), Official Journal No C 321 E, 29/12/2006, p. 318-324.

[32] This prohibition is a mandatory legal obligation stemming from the Protocol on the Privileges and Immunities of the European Communities, which states in Article 1:(...) "*The property and assets of the Communities shall not be the subject of any administrative or legal measure of constraint without the authorization of the Court of Justice*"; in Article 2: "*The archives of the Communities shall be inviolable*" and in Article 6: "*For their official communications and the transmission of all their documents, the institutions of the Communities shall enjoy in the territory of each Member State the treatment accorded by that State to diplomatic missions.*"

[33] See: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud-computing-services-european_en

Another effect of the US CLOUD Act to be closely monitored is the possibility for US authorities of further sharing personal data obtained under the US CLOUD Act with third countries authorities. The impacts of executive agreements under US CLOUD Act remain to be examined closely, in particular whether this is in line with the obligations set upon US companies by the EU-US Privacy Shield framework about material and procedural conditions for access to personal data and for onward transfers[34]. At the moment of drafting this letter, there is no US CLOUD Act executive agreement in force.

This assessment of the impact of the US CLOUD Act on the European legal framework for the protection of personal data should also be considered within the broader framework of cross-border access to electronic evidence at international level, on which EU supervisory authorities have previously stated their positions[35], and taking into account upcoming developments such as the draft additional protocol to the Council of Europe Convention on Cybercrime or the legislative proposals on electronic evidence currently negotiated at EU level. In this regard, the EDPB has provided an analysis[36] of the European Commission's proposals for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and a Directive laying down harmonized rules on the appointment of legal representatives for the purposes of gathering evidence in criminal proceedings.

2. The opening of negotiations with the US in view of an agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters

On 5 February 2019, the Commission adopted a Recommendation for a Council Decision to authorise the opening of negotiations in view of an international agreement between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matters and negotiating directives[37]. On 6 June 2019, the Council adopted the Council Decision authorising the opening of these negotiations[38].

On 2 April 2019, the EDPS published a formal Opinion on this topic in response to a consultation by the Commission pursuant to Article 42 of Regulation (EU) 2018/1725[39]. Some of the main recommendations of the EDPS, made in the spirit of constructive and objective advice to the EU institutions, are to include Article 16 TFEU as one of the substantive legal bases in the preamble of the Council Decision and to include in the negotiating directives essential improvements and the

[34] The European Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield, notably states in its Recital 27 that: "*Special rules apply for so-called 'onward transfers', i.e. transfers of personal data from an organisation to a third party controller or processor, irrespective of whether the latter is located in the United States or a third country outside the United States (and the Union). The purpose of these rules is to ensure that the protections guaranteed to the personal data of EU data subjects will not be undermined, and cannot be circumvented, by passing them on to third parties (...)*".

[35] WP29 statement on data protection and privacy aspects of cross-border access to electronic evidence, 29 November 2017.

[36] Opinion 23/2018 of the EDPB adopted on 26 September 2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters, p. 20-21.

[37] Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final.

[38] See: https://data.consilium.europa.eu/doc/document/ST-10128-2019-INIT/en/pdf; https://data.consilium.europa.eu/doc/document/ST-10128-2019-ADD-1/en/pdf

[39] See EDPS Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence of 2 April 2019, available here: https://edps.europa.eu/data-protection/our-work/publications/opinions/eu-us-agreement-electronic-evidence_en

reinforcement of several safeguards he recommended in his previous Opinion on the Umbrella Agreement[40].

The EDPS also recommends the involvement of judicial authorities designated by the other Party to the agreement as early as possible in the process of gathering electronic evidence, so that these authorities would have the possibility to review compliance of the orders with fundamental rights and raise grounds for refusal. Finally, the EDPS provided a list of specific recommendations covering specific aspects of the envisaged agreement to be negotiated with the US[41].

In order to comply with EU primary law, the conclusion of an international agreement must in any case provide for appropriate safeguards for transfers and ensure that enforceable data subject rights and effective legal remedies for data subjects are available.

We expect to be kept informed regularly by the European Commission about the negotiations and about the initial and subsequent versions of the draft agreement in order to be able to provide the appropriate guidance and recommendations.

The EDPB and the EDPS will follow closely this issue and may issue further opinions in due time during the course of the negotiations, in particular once the text of the draft agreement becomes available.

Brussels, 10 July 2019.

[40] See Preliminary Opinion 1/2016 of 12 February 2016 on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences, available here: https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf

[41] These specific aspects are related to: the mandatory nature of the agreement; the onward transfers by US competent authorities; the rights of data subjects in the US, in particular the right to information and the right of access; the control by and independent authority in the US; the judicial redress and administrative redress in the US; the categories of data subjects concerned; the definition and types of data covered by the envisaged agreement; the criminal offences covered by the envisaged agreement; the specific safeguards to ensure an appropriate level of security of the data transferred; the type of authorities that can issue orders for electronic evidence; and the possibility for service providers served with an order for electronic evidence to object based on specific grounds.