ALERT MEMORANDUM

European Data Protection Authorities Explore U.S. CLOUD Act's Potential Impact on the GDPR

September 3, 2019

Responding to a request by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), the EU's data protection supervisory bodies released an initial joint opinion on the impact of the U.S. Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") on the EU data protection framework. The preliminary assessment by the European Data Protection Supervisor ("EDPS") and European Data Protection Board ("EDPB") leaves service providers facing a familiar dilemma.

Although the CLOUD Act now makes clear that U.S. disclosure orders have an extraterritorial reach, the EDPS and EDPB see very limited options for service providers to comply with such orders without breaching the EU's General Data Protection Regulation ("GDPR").

Companies will have to carefully consider whether to store data with service providers that may be subject to the Act.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

BRUSSELS

Natascha Gerlach
+32 2 287 2201
ngerlach@cgsh.com

Rue de la Loi 57
1040 Brussels, Belgium
T: +32 2 287 2201

COLOGNE

Elisabeth Macher
+49 221 800 40 156
emacher@cgsh.com

Theodor-Heuss-Ring 9
50668 Köln, Germany
T: +49 221 80040 0

The CLOUD Act

The CLOUD Act, signed into law on March 23, 2018, updated portions of the 1986 Stored Communications Act ("SCA"), which prescribes the circumstances under which the U.S. government may compel production of remotely stored electronic communications. Prior to the enactment of the CLOUD Act, the Supreme Court was poised to rule in the *Microsoft Corporation v. United States of America* case on whether the SCA in its previous form permitted the use of a warrant to obtain electronic communications stored by a U.S. company on foreign servers.

The CLOUD Act rendered this case moot by (i) explicitly stating that the SCA's provisions extend to those held abroad; (ii) establishing a framework for service providers to challenge an SCA warrant; (iii) directing courts to conduct a limited comity analysis when deciding whether to quash a warrant; and (iv) authorizing the United States to enter into executive agreements governing cross-border data requests with foreign governments.[1] Notably, however, the CLOUD Act rendered the Microsoft case moot only as it concerns the question of whether U.S. authorities deem its warrants and other court orders to reach information stored abroad: the flip side – specifically, whether foreign jurisdictions agree that U.S. court orders do not conflict with their data protection laws and therefore can reach data stored in their jurisdictions – remains.

Express Extraterritoriality

Section 103 of the CLOUD Act adds to the SCA Section 2713, which states that a service provider shall disclose information in the service provider's "possession, custody, or control, regardless of whether such . . . information is located within or outside of the United States."[2] This extraterritoriality provision aims to reduce barriers for U.S. law enforcement investigations. Yet, as the Department of Justice ("DOJ") acknowledged in its April 2019 white paper, under Section 2713 of the SCA, service providers may have to answer to two conflicting systems of law when asked by authorities in one jurisdiction to disclose communications that are stored abroad in another.[3]

However, the DOJ also stated that the extraterritoriality provision is not a new concept. Rather, it "makes explicit in U.S. law the long-established U.S. and international principle that a company subject to a country's jurisdiction can be required to produce data the company controls, regardless of where it is stored at any point in time."[4] According to the DOJ, even with the CLOUD Act, much remains the same, including (i) the standard under which U.S. authorities may obtain a warrant and (ii) the fact-specific analysis a U.S. court must undertake to determine whether it has personal jurisdiction over a company.[5]

Mechanism For Quashing A Warrant and Required Comity Analysis

The CLOUD Act provides a way for service providers to challenge or move to quash SCA warrants and requires courts to conduct a limited comity analysis when determining whether to block such warrants.

---

[1] For further analysis of the CLOUD Act, see CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications, Cleary Gottlieb Alert Memorandum (Apr. 4, 2018), https://www.clearygottlieb.com/-/media/files/alert-memos-2018/cloud-act-establishes-framework-to-access-overseas-stored-electronic-communications.pdf.

[2] CLOUD Act § 103(a)(1); to be codified at 18 U.S.C. § 2713.

[3] *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* 2, U.S. Dep't of Just. (Apr. 2019) [hereinafter "DOJ White Paper"], https://www.justice.gov/opa/press-release/file/1153446/download.

[4] *Id.* at 3. See also *id.* at 2-3, 6 n.3 ("The Convention on Cybercrime (also called the 'Budapest Convention') requires each of the more than 60 countries . . . to maintain the legal authority to compel companies in their territory to disclose stored electronic data under their control pursuant to valid legal process, with no exception for data the company stores in another country. . . . [and] Australia, Belgium, Brazil, Canada, Colombia, Denmark, France, Ireland, Mexico, Montenegro, Norway, Peru, Portugal, Serbia, Spain, [and] the United Kingdom" assert such authority.")

[5] *Id.* at 8. For further analysis of the DOJ White Paper, see *DOJ Releases White Paper Addressing Scope & Implications of CLOUD Act*, Cleary Cybersecurity and Privacy Watch post, (Apr. 18, 2019), https://www.clearycyberwatch.com/2019/04/doj-releases-white-paper-addressing-scope-implications-of-cloud-act/.

This "totality of the circumstances" analysis takes into account the interests of both the U.S. and foreign governments and includes factors such as the availability of alternative means to secure the information, and the extent to which compliance with the court order would undermine important interests of the state where the information is located.

Executive Agreements Governing Cross-Border Requests

The CLOUD Act also allows the U.S. Attorney General to enter into executive agreements with foreign governments, when those foreign governments meet certain privacy and human rights requirements.[6] These bilateral agreements would permit both the United States and the foreign government to access and share data stored abroad.[7]

According to the DOJ, these executive agreements may lift barriers to reciprocal data sharing (pursuant to qualifying orders in certain types of criminal cases) and may address the concern that many global service providers have about potential liabilities that would stem from violating the disclosure laws of one country when compelled by another to disclose.

Notably however, the DOJ has also emphasized that an executive agreement in and of itself would not (i) impose new obligations on service providers, (ii) establish the U.S. government's or the foreign government's jurisdiction over service providers, or (iii) require either government to compel a service provider to disclose. Rather, "[t]he only legal effect of a CLOUD agreement is to eliminate the legal conflict," (as it concerns qualifying orders) that would exist between U.S. law and foreign law absent the executive agreement.[8] Ultimately, the executive agreement would require only what is negotiated and agreed to by the U.S. and the foreign government, although any executive agreement would likely "permit U.S.-based global [service providers] to respond directly to foreign legal process in many circumstances."[9] Of course, if the U.S. or a foreign government seeks data that falls outside of the executed executive agreement, "[the] countr[y] may continue to use their existing legal process . . . but may continue to face a conflict of laws in those circumstances."[10] Currently, the United States and EU Member States have not entered into any executive agreement under the CLOUD Act.

Legal Assessment of the EDPS & EDPB

Although the CLOUD Act makes clear the *United States' view* on whether U.S. warrants under the SCA apply to data stored abroad, the GDPR imposes strict rules on data processing[11] and transfers of data abroad. The European Commission ("EC") already emphasized in their amicus brief submitted in the *Microsoft* case that, under Article 48 GDPR, "a foreign court order does not, as such, make a transfer lawful" under EU data protection laws.[12]

The EDPS and EDPB have now undertaken a detailed analysis of the legality of complying with U.S.

[6] The foreign government must "afford[] robust substantive and procedural protections for privacy and civil liberties in light of the data collection." Factors to be considered in making this determination include (i) "adequate substantive and procedural laws on cybercrime and electronic evidence" as detailed in the Budapest Convention; (ii) "respect for the rule of law and principles of nondiscrimination"; (iii) "adher[ence] to applicable international human rights obligations"; (iv) "clear legal mandates and procedures" for the collection, retention, use, and sharing of data, and "effective oversight of these activities"; (v) "sufficient mechanisms to provide accountability and appropriate transparence regarding the collection and use of electronic data"; and (vi) " [a] demonstrate[d] commitment to . . . the global free flow of information and the open . . . Internet", CLOUD Act § 105(a) amending 18 U.S.C. § 2523(b).

[7] While U.S. courts have compelled disclosure of data from foreign jurisdictions in U.S. proceedings, the reverse is not the case. Ironically, the SCA itself prevents disclosure in foreign proceedings by allowing only very limited derogations under which a service provider can disclose, excluding foreign discovery requests. See *Suzlon Energy Ltd. V. Microsoft Corp.* 671 F.3d 726, 728-29 (9th Cir. 2011).

[8] DOJ White Paper at 5.

[9] *Id.* at 4.

[10] *Id.* at 12.

[11] "Processing" means any operation which is performed on personal data, including its collection, use, disclosure, storage and erasure (Article 4(2) GDPR).

[12] Brief of the European Commission on behalf of the European Union as *amicus curiae*, *United States of America v. Microsoft Corporation*, Case No. 14-2985, at 14 (Dec. 13, 2017); see also GDPR, Recital 115.

warrants from an EU data protection perspective ultimately recommending that the EU seek a dedicated international agreement with the United States.[13]

General Assessment

The EDPB and EDPS joint opinion re-affirmed the Commission's view: the request of a U.S. authority alone does not constitute a legal basis for transferring data to the United States. Absent a legal basis grounded in EU or Member State law, service providers disclosing personal data located in the EU in order to comply with a U.S. warrant or subpoena may run afoul of the GDPR.

Article 48 GDPR states that a foreign court order can only be recognized "if based on an international agreement such as a mutual legal assistance treaty, in force between the requesting third country and the Union or Member State."

The EDPB already emphasized in previous guidance on the derogations of Article 49 GDPR that "[i]n situations where there is no international agreement [. . .], EU companies should generally refuse direct requests and refer the requesting third country authority to an existing mutual legal assistance treaty or agreement."[14]

However, under the CLOUD Act, U.S. authorities would not need to go through the – potentially lengthy[15] – judicial assistance procedure laid out by the current mutual legal assistance treaty ("MLAT") or any other international agreement undertaken by way of the CLOUD Act's executive agreements provision, but could directly address the U.S. company to produce data stored in the EU. Service providers subject to the jurisdiction of U.S. courts will be compelled by a U.S. court order alone and refusal will likely result in adverse consequences.[16]

The EDPS and EDPB point out that the extraterritorial application practically invites U.S. authorities and courts to bypass the MLAT currently already in place between the United States and the EU[17] in favor of responding to requests directly regardless of data location.

However, in the absence of the MLAT procedure or a treaty signed via the executive agreement provision of the CLOUD Act, EDPB and EDPS also make clear that service providers subject to EU law cannot legally base the disclosure and transfer of personal data to the United States on foreign orders or requests.[18]

According to the EDPS and EDPB, service providers must then apply the standard two-step process under the GDPR for determining whether they can lawfully comply with the request for disclosure: (i) a legal basis for processing the personal data (as set out in Articles 6 and 9 of the GDPR) must exist and (ii) a means by which the transfer to the United States can be lawfully made, such as meeting the requirements of an Article 49 GDPR derogation, must be established.

Step 1: Lawfulness of Processing under Article 6

Regarding the lawfulness of data processing, i.e., the disclosure of the data as such, the EDPB and EDPS examined (and discarded) a number of potential legal

[13] Initial legal assessment of the impact of the U.S. 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, July 10, 2019, in response to a request by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_response_us_cloudact_coverletter.pdf (cover letter); https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf (analysis).

[14] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 5.

[15] The EDPB and EDPS acknowledge that a "new generation" of MLATs should be implemented, "allowing for a much faster and secure processing of requests in practice."

[16] Similar to the district court's ruling in *Microsoft*, a U.S. court could hold the noncompliant service provider in contempt of court. *See Microsoft Corp. v. United States*, 829 F.3d 197, 200-01 (2d Cir. 2016). However, it remains to be seen how courts will deal with noncompliant service providers in instances where they do not produce data after failing to quash or modify the request from U.S. authorities in court.

[17] Agreement on mutual legal assistance between the European Union and the United States of America, Official Journal L 181 , 19/07/2003 P. 0034 – 0042. .

[18] The EDPB and EDPS point out that neither the EU-US Privacy Shield adequacy decision, nor the EU-US Umbrella Agreement (which only applies to requests between authorities, not requests issued by an authority to a company) are applicable to service providers being directly addressed by U.S. law enforcement authorities.

bases under Article 6 GDPR. Most notably, the authorities held that (i) the service provider cannot rely on the processing being "necessary for compliance with a legal obligation" pursuant to Article 6(1)(c) GDPR, since a request from a U.S. authority is only enforceable if based on an international agreement, such as an MLAT; (ii) service providers can only claim, in exceptional circumstances, that the processing is "necessary in order to protect the vital interests of the data subject," *e.g.* in cases concerning abducted minors; and (iii) the disclosure of data is not "necessary for the performance of a task carried out in the public interest" pursuant to Article 6(1)(e) GDPR, since an order under the CLOUD Act does not qualify as "public interest" in the EU.

While in many instances of data transfers from the EU/EEA to the United States in the context of (civil) litigation and investigations, undertakings will rely on such processing being "necessary for the purposes of its legitimate interests" in accordance with Article 6(1)(f) GDPR, the EDPS and EDPB have discarded this legal basis for processing in response to the request from a U.S. court or authority under the CLOUD Act for data covered by the GDPR. While the undertaking as the controller may have a legitimate interest in complying with the U.S. law enforcement request (*e.g.*, avoiding sanctions under U.S. law) and in the prevention and detection of potential criminal acts, the EDPB and EDPS see such an interest as overridden by the interests and fundamental rights and freedoms of the person whose information is being sought. The EDPS and EDPB considered, in particular, that without the protective nature of an internationally agreed framework, the data subject in law enforcement matters could be deprived of their right to an effective remedy guaranteed in Article 47 of the Charter of Fundamental Rights of the European Union. It is also conceivable that the transfer of data may lead to prosecution for acts not sanctioned in their own country (dual criminality principle).[19]

The EDPB and EDPS further stressed that "the compelling nature" of the U.S. law enforcement request and the limited information flow connected with such requests run afoul of the obligations a controller would have toward the data subject under the GDPR (in particular, transparency), which in turn are directly linked to the data subject being able to exercise the rights bestowed on him or her by the GDPR.

Step 2: Derogations for Transfers under Article 49

Apart from the legal basis for the transfer as an act of processing under the GDPR, the two-step process also requires that Chapter 5 GDPR[20] be satisfied where the transfer is to third countries such as the U.S. As the generally required safeguards are unlikely to apply in this context, the EDPB and EDPS focused on derogations provided for in Article 49 GDPR, with emphasis on a strict interpretation, "so that the exception does not become the rule."[21]

In particular, the EDPB and EDPS held that (i) the transfer would not be "necessary for important reasons of public interest" pursuant to Article 49(1)(d) GDPR, since the public interest of a third country such as the U.S. is of no consequence to the GDPR; and (ii) it is generally not "necessary for the establishment, exercise or defense of legal claims" pursuant to Article 49(1)(e) GDPR, unless there is a close link between the data transfer and a specific procedure.

Finally, the EDPS and EDPB considered the legitimate interest derogation somewhat hidden in Article 49(1) sent. 2 GDPR, but concluded that due to the higher threshold compared to Article 6(1)(f) GDPR and the requirement for notifications to all data subjects and the data protection authorities, which will often be prohibited by the warrant, this is unlikely a valid basis for a transfer. In particular the additional condition of suitable safeguards for the protection of the data will be difficult, if not impossible, to implement for an undertaking in the face of a CLOUD Act request.

Recommendation of the EDPB and EDPS

As a result, the EDPS and EDPB strongly recommended that an international agreement be concluded between the EU and the United States, containing sufficient personal data protection provisions on which the disclosure and transfer of such data could be based in the future.

[19] On the other hand, it is perhaps conceivable that in cases where the behavior is sanctioned in either country, this would weigh in favor of a transfer.

[20] Chapter 5 GDPR sets out principles and prerequisites for the transfer of personal data to third countries.

[21] Opinion p.6.

Absent such an agreement, the lawfulness of complying with a U.S. warrant cannot be ascertained, creating legal uncertainty for businesses and data subjects.

Key Takeaways

The EDPS and EDPB raised questions regarding the scope of certain provisions of the CLOUD Act still to be clarified. In particular, the bodies raised questions regarding the CLOUD Act's application to EU undertakings with a U.S. presence, or EU undertakings that are affiliated with U.S.-based entities. The latter will depend on the application of the concept of "custody or control" over the data in question.

By clarifying that U.S. authorities can use a warrant for criminal cases to reach into foreign jurisdictions to obtain personal data, where it does apply, the CLOUD Act ultimately leaves undertakings subject to the GDPR between the same rock and hard place as before the Act went into effect.

Another open field of question is the option of challenging a CLOUD Act order and the related comity analysis. Notably, the concept of pre-enforcement challenges and comity analyses is not altogether novel. The CLOUD Act's introduction of a procedure for pre-enforcement challenges to SCA warrants and a requisite comity analysis puts the SCA warrant procedure on equal footing with well-established procedures for enforcing subpoenas and civil discovery requests regarding information held abroad by entities otherwise subject to U.S. jurisdiction.[22]

The CLOUD Act provides limited avenues to quash warrants issued under it, particularly where the data might relate to persons not located in the United States, or where laws of countries are violated which have entered into executive agreements with the United States. This leaves open the question of whether a challenge could be brought in the case of a data subject's dual citizenship (if the provider even had that information) and whether an objection could be raised under common law comity at present, since no agreements have yet been entered into under the CLOUD Act.[23]

While the comity analysis the U.S. Supreme Court outlined in *Aerospatiale*[24] could also provide useful guidance in this context, historically U.S. courts have been quick to favor compliance with the order over important interests of the jurisdiction in which the information is located such as European privacy laws or blocking statutes. It is too early to tell if this will change now that the GDPR has become effective.[25] Further guidance on the factors of the comity analysis to be applied with due deference to fundamental rights protected by sovereign nations outside the United States would certainly be desirable.

Any agreement to be negotiated now, apart from being more nimble than the current MLAT proceedings, would have to address the question of enforcement in the Member States where the request is served, as well as include sufficient safeguards to ensure due access to legal remedies for data subjects and provisions for the potential of onward transfers.

Finally, the opinion should be read in its context – an initial legal assessment of the impact of the CLOUD Act for U.S. law enforcement requests on data governed by the GDPR or Member State data protection law. While the EDPB and EDPS emphasized that it should be seen against the larger background of international cross-border access to electronic evidence as well,[26] it should still be read in the context of criminal enforcement. This should also inform the reading of the legal assessment presented for Article 6(1)(f) GDPR (legitimate interest) where the potential consequences of the data processing for the data subject in the absence of a protective framework would outweigh the undertaking's legitimate interest especially where transparency requirements could not (or not fully) be complied with.

…

CLEARY GOTTLIEB

[22] *See Société Nationale Industrielle Aérospatiale v. United States District Court*, 482 U.S. 522 (1987) (established the five factor balancing test under which U.S. courts can compel production of information held abroad).
[23] See also opinion p. 2
[24] *Id.*
[25] Although the recent *Finjan* decision seems rather to indicate business as usual.
[26] Opinion, p. 9