GT GreenbergTraurig

Memorandum

TO:	Dutch Ministry of Justice and Security - NCSC
FROM:	Greenberg Traurig LLP | Herald Jongen, Gretchen Ramos, Wouter van Wengen
DATE:	November 17, 2022
RE:	Number of CLOUD Act requests

On 26 July 2022, we sent you a memorandum on the scope of the US CLOUD Act ("Cloud Memo"). As follow up, you have asked us to advise on the CLOUD Act's practical impact. Specifically, you requested us to investigate how often the US Government invokes the CLOUD Act, and how often this leads to disclosure of personal data of EU residents.

Executive Summary

The risk of disclosure of EU residents' personal data or other data under the CLOUD Act seems to be (very) low. Transparency reports of three of the largest US cloud service providers (Microsoft, Amazon, and IBM) who store personal data outside the US (which is the remit of the CLOUD Act) contain the following relevant information.

- Since the US CLOUD Act became effective in March 2018, Microsoft reported 12 disclosures of non-US based enterprise content data to the US government. Please note that it is uncertain whether any EU resident's personal data was disclosed in relation to these 12 disclosures, since this is not specified in the reports.
- In November 2021, Microsoft stated they "never provided access to any personal data of public sector organizations in the EU to any government authority."
- In 2021, IBM stated they received only 1 US government request for EU client content, which was rejected.
- Since July 2020, Amazon has consistently stated that they have not disclosed any enterprise or government content data stored outside the US, to US law enforcement.

As these companies cover a preponderant share of the market, these results may well be representative for the other US cloud providers that are subject to the CLOUD Act. The number of requests and disclosures are also in line with the findings in the data protection impact assessment (DPIA) performed on Microsoft Teams by the Ministry of Justice and Security (SLM). In case of any remaining uncertainty, there are options available, such as ringfencing, proper encryption, and pseudonymization to protect the data.

TABLE OF CONTENTS

1. The Cloud Memo's Main Conclusion

Some argue that using non-US/EU providers is the panacea for all privacy concerns. However, in the Cloud Memo, we explained that EU Entities can be within the reach of the CLOUD Act, even if the EU Entities are located outside the U.S.[1]

The two central questions of this memorandum are:

(1) How often is the CLOUD Act invoked for requests of personal data of EU residents?
(2) To what extent do CLOUD Act requests lead to disclosures of personal data of EU residents?

2. Research Methodology

In order to answer these questions, we scrutinized the transparency reports of three of the largest US cloud service providers that store personal data outside the US (i.e., that are subject to the US CLOUD Act). A detailed table is included in Annex 1. In addition, we have analyzed the resulting number of requests and disclosures against the numbers and explanations in the DPIA performed on Microsoft Teams by SLM.[2]

---

[1] See also the cover note with which the Cloud Memo was published by NCSC. "Many experts assume that this risk does not exist if a European service provider processes data and certainly if that takes place within Europe. From a legal point of view, however, this is more nuanced, and the US CLOUD-Act may also apply to data processing operations outside the US, for example, in the EU." How the CLOUD-Act works in data storage in Europe | By our experts | National Cyber Security Centre (ncsc.nl)

[2] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad/Public+DPIA+Teams+OneDrive+SharePoint+and+Azure+AD+16+Feb+2022.pdf

3. **Results**

Since the US CLOUD Act became effective in March 2018, Microsoft has received more than 200,000 requests for customer data from governments around the world, including 45,000 requests from US law enforcement authorities. Of those, Microsoft disclosed non-US enterprise content data to US law enforcement on only 12 occasions.[3] These numbers include requests with secrecy orders ("gag orders") and includes those successfully challenged by Microsoft. Microsoft did not specify if any disclosures pertain to EU-based enterprises. Further, the Microsoft definitions of customer content data and enterprise content data may include personal data of EU residents but are not limited to it. Therefore, the requests and disclosures pertaining to personal data of EU residents likely consists of an even smaller number. Furthermore, Microsoft stated in November 2021 that they "never provided access to any personal data of public sector organizations in the EU to any government authority."[4]

In 2021, IBM stated that there had only been one US government request for client content located in the EU, which was rejected.[5]

Since July 2020, Amazon has consistently stated that they have not disclosed any enterprise or government content data to US law enforcement stored outside the US.[6]

While none of the three companies' transparency reports provides a breakdown by country or continent[7], as to the targets of the CLOUD requests, such detail does not appear to be necessary, as these major US cloud providers make far more encompassing statements, as discussed above.

The numbers in these transparency reports correspond with the earlier DPIA on Microsoft Teams by SLM, wherein the risk was set at low.

On the basis of the above, it is fair to conclude that the risk of disclosure of EU residents' personal data or other data under the CLOUD Act is low.

4. Possible Solutions to Mitigate the Residual Risk

We refer to the solutions provided in the CLOUD Memo.

---

[3] https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

[4] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRql1

[5] Government Access To Data: Getting The Facts Straight - IBM Policy

[6] https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF

[7] As stated above, IBM did, however, make a direct statement that it received only one CLOUD Act request involving EU data.

In addition, one of the more recently launched options in the market is a solution consisting of the use of encryption of (i) data at rest, (ii) data in transit and (iii) data in use (with the use of confidential computing / trusted execution environments) in combination with pseudonymization of data. However, this solution is not feasible for all cloud use cases and works effectively for data analysis and machine learning.

Simplified, this comes down to a setup wherein personal data is (i) encrypted at rest, (ii) transferred securely to a cloud provider, then (iii) pseudonymized within a trusted execution environment. This results in a pseudonymized data set that can be used freely. The additional information required for relinkability is only accessible to the data controller. This is a solution that elegantly puts in practice the first three use cases 1 (encryption at rest), 2 (pseudonymization) and 3 (encryption in transit) of the EDPB recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.[8]

[8] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

ANNEX 1 – CLOUD ACT REQUESTS SUMMARY

Company	Identified CLOUD Act Requests	Relevant Period When Requests Received	Number of CLOUD Act requests (if available)	Number of Disclosures
Microsoft	Yes	Jan 2018 - June 2022 *Explanation relevancy*: The CLOUD Act became effective in 2018. This period covers all requests and disclosures since then.	Not available.	12 disclosures of non-US based enterprise content data.
Amazon	No	July 2020 - June 2022 *Explanation relevancy*: Amazon started publishing the number of disclosures of government and enterprise data in July 2020.	Not available.	0 disclosures of government and enterprise data; undisclosed number of individual consumer data disclosures.
IBM	Yes	June 2, 2021 *Explanation relevancy*: This is when IBM made this representation.	1 CLOUD Act request for EU client content and refused to comply.	0 disclosures of EU client content.