The Key to Confidentiality in the Cloud

How organisations can protect themselves from international data transfers

“Data is the new oil”, is a phrase that commonly gets thrown around. While this phrase is not really a perfect fit here – data is so much more than oil – it does have significances in illustrating the economic value of data. Just like oil, data needs to be refined: it needs to be processed in order to provide meaningful information. The Deloitte Tech Trends 2022 publication details how technologies enabling privacy-preserving computing (also known as confidential computing) are on the rise. However, many of these new techniques do not offer a viable alternative yet: computations using technologies like homomorphic encryption are often thousands of times slower than plaintext calculations. This means that in today’s context, organisations operating in the European Union (EU) still must rely on using plaintext user data for their processing activities. This may create hurdles in case these organisations make use of United States (US) cloud providers because of the concerns related to international data transfers.

The Post-Schrems II World

To address this specific topic with regards to European user data, the European Commission proposed a regulation known as the EU–US Privacy Shield in 2016 in cooperation with the United States Department of Commerce. This framework was designed with the goal of ensuring that adequate data protection obligations were in place when international personal data transfers took place, in this case from the EU to the US. The European Court of Justice though, struck down the Privacy Shield on 16 July 2020. The court, among other things, held that the United States' national intelligence agencies infringed on the Fundamental Freedom to Respect for Private and Family Life [5] of EU citizens due to their surveillance initiatives. In short, the legal mechanisms and safeguards used to protect non-Americans from surveillance did not provide for adequate protections under the Privacy Shield Framework. This decision is now known as the Schrems II decision, named after Max Schrems, an Austrian citizen who has challenged the legality of the two frameworks established between the EU and the US.

The results of this decision have been paramount, as there is no longer a mechanism that allows for the streamlined transfer of personal data from the EU to the US. Data protection authorities (DPAs), governmental institutions and watchdogs have demanded organisations to cease transferring data to the US. In fact, the Berlin DPA, Berliner Beauftragte für Datenschutz und Informationsfreiheit, doubled down on this demand. It specifically stated that, "In practice, often used services of US companies or their European subsidiaries can therefore no longer be used in a legally compliant manner in many cases, so that previous business practices sometimes have to be changed considerably.". Additionally, in 2018, the US has enacted the US CLOUD Act, which can allow US federal law enforcement agencies to compel US-based technology companies to provide requested data stored on servers regardless of whether the data is stored in the US or on foreign soil via warrants or subpoenas.

In turn, **DPAs** have further **advised** that organisations **should terminate their agreements with subsidiaries** of US cloud service providers such as Amazon Web Services (AWS) SARL. Some authorities, like for example the Flemish Supervisory Committee (Vlaamse Toezichtscommissie or VTC, the DPA at Flemish government level), have published guidance on acceptable uses of cloud providers. They specifically issued a decision matrix, imposing stringent rules onto Flemish government entities aiming to use cloud services. The VTC stated that **using any non-European cloud provider is not allowed by default**, except if certain supplementary measures for data protection are considered, like for instance "encryption or comparable measures".

Moreover, the guidance from the European Data Protection Board (EDPB) on Standard Contractual Clauses does not provide a straightforward solution. The Court of Justice, while striking down the Privacy Shield, held that Standard

Contractual Clauses (SSCs) can be used to allow the transfer of data to third countries, and therefore, they are now seen as the gold standard for an appropriate mechanism for transferring personal data out of the EU. The EDPB provides an extensive list of technical and organisational measures that can be used to help protect personal data, and in turn protect the Fundamental Rights of European citizens. However, the majority of the EDPB's suggested measures often achieve very little in terms of protecting personal data from third country national intelligence agencies.

It should be noted that the **United States and the European Commission** have proclaimed the **intention to create a new Trans-Atlantic Personal Data Transfer Framework**. In furtherance of this framework, the United States has announced new measures on how non-US citizens' personal data will be accessed. In theory, this is an exciting development for US and EU organisations. In practice however, it may mean very little. Schrems has already addressed the new measures and has highlighted how they do not satisfy the requirements laid out by the European Court of Justice (ECJU) and has declared his intention to bring a new claim to the court. Furthermore, None of Your Business (NOYB), Schrems' non-profit organisation, argues that simply altering the text from "as tailored as feasible" to "necessary and proportionate" in the relevant US executive order does not offer any further protections to European's Fundamental Rights in practice. Rather, the US would have to terminate several surveillance initiatives, to which it has not committed.

"However much the US authorities try to paper over the cracks of the original Privacy Shield, the reality is that the EU and US still have a different approach to data protection which cannot be cancelled out by an executive order."

– Ursula Pachl, Deputy Director General of the European Consumer Organisation (BEUC)

The Lacking European Cloud Provider Situation

Cloud computing has been and still is on the rise, and this trend is only predicted to accelerate in the coming years. Gartner is expecting that half of all IT spending of organisations will be going towards cloud computing by 2025 [14]. Its inherent flexibility and scalability compel more and more organisations to move their workloads to the cloud, making the most of all the as a Service-models being offered by cloud providers. At least: some cloud providers. Looking at cloud provider market shares, one thing immediately becomes clear: three major vendors absolutely dominate the market [15]. **Together, Amazon Web Services, Microsoft Azure, and Google Cloud Platform (GCP) make up more than 60% of the current market in cloud worldwide** (see Figure 1). Importantly, all three market leaders are US-based companies.

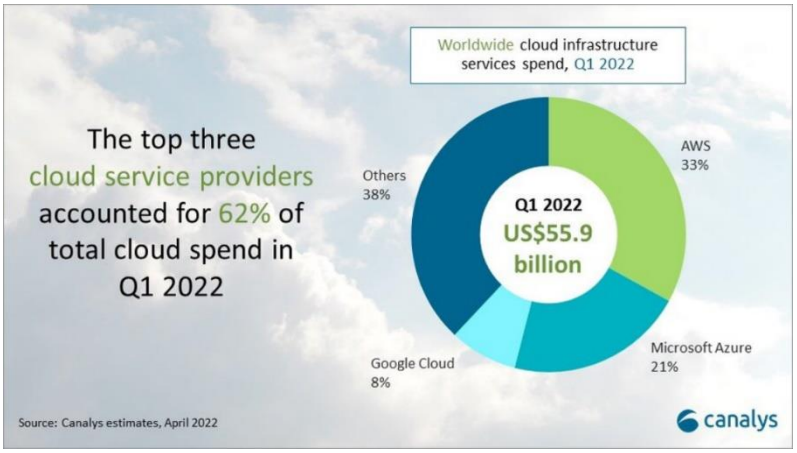

Figure 1: The dominant position of US cloud providers.

This statistic draws a significant dichotomy. On the one hand, DPAs and governmental agencies are demanding that organisations in the EU stop transferring data to the United States and stop using American cloud service providers, even in case of subsidiaries where the data is tied to EU data centres. On the other hand, those same organisations find themselves in an impossible situation when evaluating their options for EU-based compliant vendors because of the state of the European cloud industry. Today, there is **not a single European cloud service provider capable of competing** in any meaningful way against their US-based counterparts in offering similar Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) services. Even though European cloud providers continue to grow, due to their significantly lower growth rates, they are in fact still losing market share to their American competitors today.

The fact that European cloud providers are struggling to compete with the American Big Three is of course not new, and European authorities took notice. Initially created by France and Germany in 2020, **Project GAIA-X**'s aim is to create an open data infrastructure in order to provide reference implementations for

cloud services, which is hoped to enable European technology companies to compete with their US competitors [18]. While initially it appeared that progress was being made, the later updates on GAIA-X are far from positive, with members participating in the initiative complaining about foreign influence on the project. An insider reportedly stated that "[a]s it stands now, Gaia-X [...] will not resolve lock-in effects. On the contrary, it is likely to increase market strength of larger players". It seems that Gaia-X has reached the "trough of disillusionment" and the main question seems to be whether it will manage to get out of there.

Therefore, the **lack of suitable European alternatives** further incentivises European organisations to leverage American cloud service providers. This is not a problem solely related to the United States. Rather, it is a problem relevant for any EU organisation that utilizes a data processor that is either based outside of the EU or that is bound by an obligation to share information with national authorities. For example, the same issues arise if an EU organisation were to use Alibaba or Huawei as their cloud service provider, due to its obligations to report to Chinese national authorities.

Key Management: A Solid Solution

Other solutions, however, exist for organisations based in the EU. In response to the Schrems II decision, the European Commission has published a new set of **Standard Contractual Clauses (SCC)** for organisations to adopt as a new transfer mechanism. The SCCs help provide a legal mechanism that contractually ensures US processors provide adequate safeguards such as having data encrypted at rest and in transit. However, **encrypting** the data is **not a sufficient** safeguard **if foreign government agencies are granted access to the encryption keys**, which is a custom practice when government agencies request personal data regarding an individual. What happens however if the organisation storing the encrypted data (e.g., the American cloud service provider) does not have the encryption keys in its care, custody and control? Two courts have already decided on this question. These courts applied the Schrems II logic to situations in which an EU organisation was using an American cloud service provider or subsidiary, and ultimately held that given the encryption keys were not in control of the processor, the use of the American cloud service provider as processor of personal data was acceptable. These court decisions provide a **clear alternative solution for European organisations** other than terminating their use of foreign cloud service providers. In fact, this solution offers organisations an enhanced safeguard regarding data protection and allows them to continue using the state-of-the-art cloud solutions of the Big Three cloud providers.

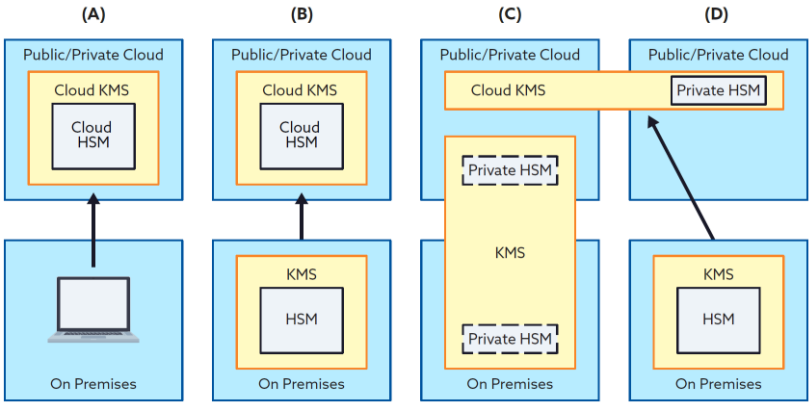

Figure 2: The KMS patterns identified by CSA.

The Cloud Security Alliance (CSA), an international non-profit organisation working on best practices for cloud security, has written extensively about the topic of key management in the cloud. CSA has identified multiple **Key Management System** (KMS) patterns detailing how organisations can organise their key management based either on cloud-native, on-prem, or hybrid KMS solutions. These patterns differ on a multitude of parameters, like for instance on the control over and the possession of the keys, or on the cost, complexity, and implementation time of the KMS. Thus, CSA provides guidance to organisations aiming to create a solution that matches their specific needs. After all, the scenario in which an organisation stores its data and encryption keys in different locations or at different providers described earlier may not always be the most suitable solution for every organisation, as it may be excessively complex for certain use cases.

Conclusion

The Schrems II decision has created a paradigm shift in the cyber world, as it drastically altered international data flows and the technical and organisational requirements needed to transfer data outside EU territory. Today, more than two years after the Schrems II decision, organisations are still unsure on how to move forward. And, while the regulatory landscape around international data transfers continues to evolve, organisations have at least one option at the ready: if they decide to continue leveraging US cloud service providers, they have the option to adopt a Key Management System that would allow them to better maintain control over the encryption keys.

Contact us

Reach out to our Cloud & Emerging Technologies team with your questions on key management systems. If you are interested in documenting the data protection and data privacy aspects of using non-EU based cloud service providers and how key management systems reduce risk to EU data subjects, please get in touch with our Data Protection & Privacy team.

References

[1] Deloitte, "Deloitte Tech Trends 2022," Deloitte Development LLC, 2022.

[2] Academic Consortium to Advance Secure Computation, "Homomorphic Encryption Standardization," Homomorphic Encryption Standardization, [Online]. Available: https://homomorphicencryption.org/introduction/. [Accessed 19 February 2022].

[3] U. Mattsson, "Security and Performance of Homomorphic Encryption," Global Security Mag, June 2021. [Online]. Available: https://www.globalsecuritymag.com/Security-and-Performance-of,20210601,112333.html. [Accessed 19 February 2022].

[4] European Comission, "Commercial sector: EU-US Privacy Shield," European Comission, [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en. [Accessed 17 February 2022].

[5] *Charter of Fundamental Rights of the European Union [2012] OJ C 326, art. 7,* 2012.

[6] *ECLI:EU:C:2020:559, Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, art. 8,* 2020.

[7] B. Robinson, "JDSUPRA," 20 July 2020. [Online]. Available: https://www.jdsupra.com/legalnews/berlin-data-protection-authority-halts-12564/. [Accessed 17 February 2022].

[8] J. Delcker, "German watchdog says Amazon cloud vulnerable to US snooping," Politico, 4 April 2019. [Online]. Available: https://www.politico.eu/article/german-privacy-watchdog-says-amazon-cloud-vulnerable-to-us-snooping/. [Accessed 17 February 2022].

[9] G. LaFever, "German state DPA guidance on protected usable data post-'Schrems II'," IAPP, 2020 September 2020. [Online]. Available: https://iapp.org/news/a/german-state-dpa-guidance-protected-usable-data-and-schrems-ii-requirements-for-supplemental-measures/. [Accessed 17 February 2022].

[10] "Data exports: Basics of data exports to third countries," Berliner Beauftragte fur Datenschutz und Informationsfreiheit, [Online]. Available: https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/datenexporte. [Accessed 25 May 2022].

[11] Vlaamse Toezichtscomissie, "Vlaamse Toezichtscomissie," Vlaamse overheid, [Online]. Available: https://overheid.vlaanderen.be/vlaamse-toezichtcommissie-actueel-cloud. [Accessed 17 February 2022].

[12] European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Versoin 2.0, 2021.

[13] "Open Letter: Announcement of a New EU-US Personal Data Transfer Framework," None of Your Business, [Online]. Available: https://noyb.eu/sites/default/files/2022-05/open_letter_EU-US_agreement.pdf. [Accessed 25 May 25].

[14] S. Moore, "Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025," Gartner, 9 February 2022. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending. [Accessed 11 February 2022].

[15] Canalys, "Global cloud services spend hits US$55.9 billion in Q1 2022," Canalys, 28 April 2022. [Online]. Available: https://canalys.com/newsroom/global-cloud-services-Q1-2022.

[16] J. Novet, "AWS growth accelerates in quarter marred by outages," CNBC, 3 February 2022. [Online]. Available: https://www.cnbc.com/2022/02/03/amazon-web-services-earnings-q4-2021.html. [Accessed 15 February 2022].

[17] Synergy Research Group, "European Cloud Providers Continue to Grow but Still Lose Market Share," Synergy Research Group , 27 September 2022. [Online]. Available: https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share. [Accessed 21 October 2022].

[18] The Gaia-X Hub Germany, "What is Gaia-X?," Federal Ministry for Economic Affairs and Climate Action, [Online]. Available: https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html. [Accessed 15 February 2022].

[19] O. Noyan, "Cracks appear as Gaia-X celebrates its progress," Euractiv, 23 November 2022. [Online]. Available: https://www.euractiv.com/section/digital/news/cracks-appear-as-gaia-x-celebrates-its-progress/. [Accessed 16 February 2022].

[20] I. Scales, "Gaia-X hits the trough of disillusionment," TelecomTV, 7 October 2022. [Online]. Available: https://www.telecomtv.com/content/digital-platforms-services/gaia-x-hits-the-trough-of-disillusionment-45611/. [Accessed 21 October 2022].

[21] "Standard contractual clauses for international transfers," Justice and Consumers, 04 June 2021. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en. [Accessed 21 February 2022].

[22] E. D. P. Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data,* 2020.

[23] C.E. (12th ch.), 12 May 2021, n°250.599, BV QARIN and BV ROTTERDAMSE MOBILITEIT CENTRALE (RMC).

[24] CSA, "Key Management in Cloud Services," 11 September 2020. [Online]. Available: https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/. [Accessed 21 February 2022].