BROADCOM | Queen Mary University of London

Sovereign Cloud for Europe

INDEPENDENT RESEARCH REPORT
PREPARED FOR BROADCOM

Johan David Michels
Researcher, Cloud Legal Project,
Queen Mary University of London
February 2025

Executive summary

KEY FINDINGS

1

DEFINITION
From a customer perspective, sovereign cloud offers a high degree of control over cloud resources, including over who can access customer data. There is a risk that a provider who is subject to foreign jurisdiction might disclose data to a foreign government without a customer's knowledge or permission.

2

DRIVERS
Demand for sovereign cloud is driven by regulatory concerns (including under the GDPR) and by operational needs to protect data from foreign government access, e.g. to protect trade secrets. These concerns apply especially to sensitive and highly regulated sectors, such as healthcare, critical infrastructure, and defence.

3

PROPOSAL
The cloud industry could develop a new Sovereign Cloud Code of Conduct under the GDPR. This will focus attention on reducing risks to data subjects and provide legal certainty to both customers and providers.

Contents

1. Introduction

Global spending on sovereign cloud solutions is projected to reach nearly USD $260 bn by 2027.[1] In Europe, regulations are a major driver of demand for sovereign cloud. Since the Snowden revelations of 2013, European regulators and policymakers have been concerned about foreign government access to European personal data, as illustrated by the strict rulings on US data transfers in the *Schrems I* and *II* cases. More recently, the EU and the US have worked together to facilitate international data transfers and provide a level of protection for European personal data through the 2023 EU-US Data Privacy Framework ('DPF'). But what is sovereign cloud? How does it relate to foreign government access? And why should European organisations care about this now, in 2025?

In this report, Johan David Michels analyses sovereign cloud based on research conducted for the Cloud Legal Project at the Centre for Commercial Law Studies, Queen Mary University of London,[2] and a series of expert interviews.[3] Section 2 below looks at what sovereign cloud means, while Section 3 covers what drives demand for sovereign services, including European data protection law. Section 4 concludes that the market for sovereign cloud is hampered by mixed messages and legal uncertainty. It proposes that industry develop a new Sovereign Cloud Code of Conduct under the GDPR.

This report has been commissioned by Broadcom, but responsibility for views expressed remains entirely with the author. The report does not necessarily reflect views shared by Broadcom.

[1] IDC, "IDC Forecasts Worldwide Sovereign Cloud Spending to Reach More Than $250 Billion in 2027", 13 December 2023, idc.com/getdoc.jsp?containerId=prEUR251542423.

[2] The Cloud Legal Project is made possible by the generous financial support of Microsoft. The author is also grateful to Broadcom for providing funding to conduct the interviews and prepare this report. Responsibility for views expressed, however, remains with the author. For more information about the Cloud Legal Project, see https://www.qmul.ac.uk/cloudlegal/.

[3] From September to November 2024, the author conducted interviews with ten experts on the topic of sovereign cloud. Interviewees included both independent experts and representatives of European and US providers. Interviewees were informed of the research aims and industry funding and given a list of topics beforehand. Transcripts are on file with the author.

2. What is sovereign cloud?

Sovereign cloud means different things to different people. Providers also use the term to promote different types of services. For clarity, it helps to consider sovereignty from different perspectives.

2.1 WHAT DOES SOVEREIGN CLOUD MEAN TO CUSTOMERS?

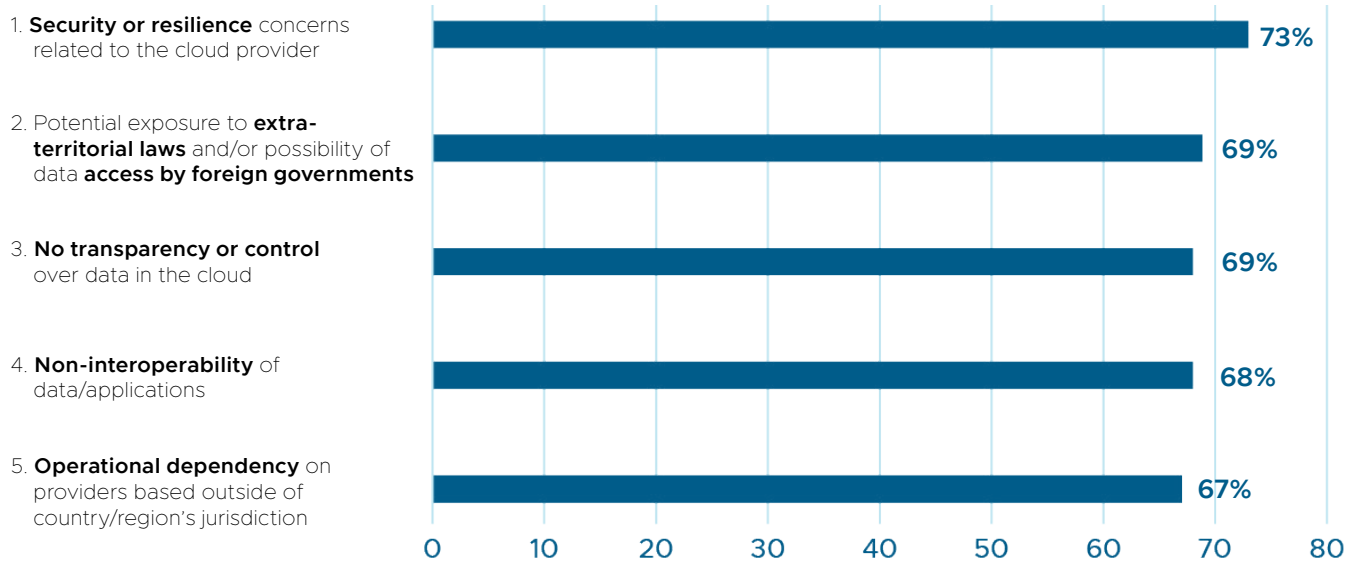
From a customer perspective, the term 'sovereign' cloud is often used to refer to a service that provides a high level of **customer control.** Consider a typical enterprise customer journey. Some ten years ago, many organisations started migrating data from their own on-premises IT to the public cloud. The cloud promised cost savings, scalability, increased functionality, and specialisation. In short, US hyperscalers would provide access to better infrastructure at lower cost, with innovative service features, pay-as-you-go pricing, dynamic scalability, and high availability through the massive deployment of servers across a global data centre network.

Today, many companies are evaluating their cloud use more critically. They are concerned about a loss of control, as illustrated in Figure 1 below.

Does the cloud provider store their data securely? Who can access the data? And can the customer still switch between providers or move data back in-house? Or have they become locked-in, for instance due to a lack of portability and interoperability?

At the same time, the customer's cloud spend has increased as resource use has grown over time. And customers have had to keep some data in-house anyway, whether because the data are too sensitive, or because the workloads are designed to run in a legacy environment and would be too costly to migrate. In effect, customers ended up with hybrid IT deployments as a compromise.

Figure 1: Top five concerns European organisations have about their current cloud environment.



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organisations.

‘Sovereign’ cloud aims to address the above concerns. In this sense, it refers to an ideal outcome centred on customer choice and autonomy, rather than a particular service type. ‘Sovereign’ services offer customers a **high degree of control** over the cloud resources they use. The customer can control who can access the data it stores in the cloud and for what purposes those data can be used.

In this broad sense, ‘sovereignty’ covers a range of issues, including data residency options for both content data and metadata and security measures that limit provider access to data, such as end-to-end encryption. Sovereign cloud can also aim to reduce vendor lock-in and provide transparency regarding the sub-processors a provider uses[4] and the metadata it collects for its own purposes. A customer can then make its own, informed and autonomous decisions about its use of IT resources.

In a narrower sense, the term ‘sovereign cloud’ is also used to refer to the risk of **foreign government access,** specifically. It asks: can the cloud provider protect the confidentiality of customer data from access by a foreign government?

US providers differ from European providers in this respect, since US providers are necessarily subject to US jurisdiction. So, the data they process can be subject to US production orders. For example, US courts can issue warrants for law enforcement purposes under the Stored Communications Act (‘SCA’), as amended by the CLOUD Act, while the National Security Agency (‘NSA’) can issue directives for foreign intelligence purposes under the Foreign Intelligence Surveillance Act (‘FISA’) Section 702. Per the CLOUD Act, production orders can target any customer data within the US provider’s “possession, custody, or control”, regardless of data location. As a result, the US government can order a US cloud provider to disclose European customer data, *even if* the data are stored in Europe by a European subsidiary.[6] This is because data processed by the European subsidiary are considered to fall within the US parent company’s “control”, since the parent company can exercise legal control over its subsidiary. Thus, a US court can issue a production order to the US parent company, which can then order its European subsidiary to hand over European customer data.

As a result, data *residency* (which looks at geographic location) differs from data *sovereignty* (which looks at foreign government access).

[4] Cloud providers typically rely on several sub-contractors to provide services that support the cloud service, such as customer chat and support, customer experience analytics, and content delivery networks. Some sub-contractors can access customer data. See for example Microsoft, “Access your data on your terms”, https://www.microsoft.com/en-gb/trust-center/privacy/data-access.

[5] Capgemini, “The Journey to Cloud Sovereignty”, 2022, capgemini.com/gb-en/insights/research-library/cloud-sovereignty/, p.9.

[6] For a detailed analysis, see Michels et al., “Cloud Sovereignty and the GDPR”, papers.ssrn.com/sol3/papers.cfm?abstract_id=4911552.

[7] Interviews were conducted under the Chatham House Rule. While the quotes can be freely shared, neither the identity nor the affiliation of the speaker(s) may be revealed.

As one interviewee put it:[7]

> **"Everyone focuses on data residency. [...] But just because data is in a country doesn't mean that it's subject to the laws of that country. [...] If your data is only subject to your legislation, then you can claim that data is sovereign. But if it's affected by extra-territorial legislation, then your sovereignty is eroded because you are no longer the only person that's making decisions on how that data is being processed."**

By contrast, a European-owned provider is more likely to offer a service that is effectively immune to US jurisdiction, especially if it does not have customers, assets, or employees in the US.[8] As an interviewee remarked:

> **"Sovereignty is linked to the accessibility of data. We need to make sure that when we provide a sovereign solution, the data is protected from extra-territorial laws."**

In sum, many European customers are reviewing their cloud use in light of sovereignty concerns. Of course, a substantial number will continue to use US hyperscalers. But they might ask those providers to put in place technical or contractual measures to address the above concerns. They may also think more strategically about **hybrid and multi-cloud deployments**[9] which combine traditional US hyperscale public cloud with European private or on-premises cloud and some in-house IT. Different environments suit different workloads depending on factors like technical requirements, cost, and regulatory compliance. For example, some workloads will benefit from the scalability and functionality of US hyperscalers, while other, more sensitive data require protection from foreign governments. One interviewee therefore stated that hybrid cloud "is pivoting from a compromise to a conscious choice". Another opined that:

> **"There's nothing wrong with using some public cloud. But you might want to keep some data assets in a service that means that you know where it is, you know it's only you that's got access to it, and it's not subject to jurisdictional overreach by whatever nation states."**

That said, a hybrid and multi-cloud deployment increases complexity and can present challenges, as discussed further in Section 3.4.

[8] A European company can also be subject to US jurisdiction, depending on its activities in and contacts with the US market. This requires a case-by-case analysis of factors such as whether it serves US customers and has US-based assets and employees; and, if so, whether it operates in the US through a truly independent subsidiary.

[9] Multi-cloud refers to a customer using the services of multiple cloud providers, while hybrid cloud refers to a customer combining resources with different deployment models, such as public and private cloud.

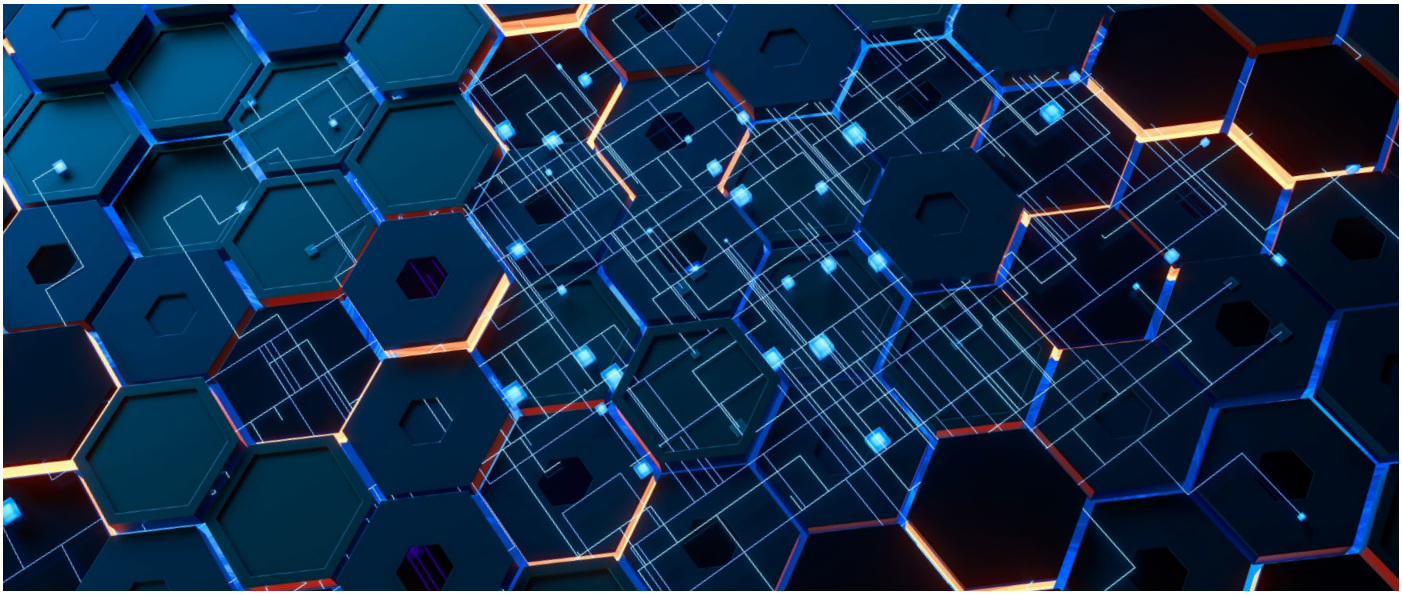
[10] Capgemini, "The Journey to Cloud Sovereignty", 2022, p.14.

2.2 WHAT DOES SOVEREIGN CLOUD MEAN TO EUROPEAN POLICYMAKERS?

For **European policymakers**, sovereign cloud is part of a much broader debate about digital sovereignty that involves geopolitics and technology policy. The overreliance on US services is seen as reducing European **'strategic autonomy'**, that is: Europe's ability to pursue its own goals, free from undue outside influence. For example, since US intelligence agencies could access European cloud data, the US has an information advantage in foreign affairs. Further, the US government could (at least in theory) threaten to order US providers to stop serving European customers, in order to influence European decision-making.[11]

Promoting European clouds is also part of the **EU industrial policy**, which aims to develop an ecosystem of interconnected cloud and edge systems to support the needs of European businesses and harness the value of European data.[12] For instance, the European Commission points out that US hyperscalers currently have access to large amounts of European (meta) data, some of which they can use to develop new services or expand to new markets. The Commission would prefer that European cloud providers benefit from this "data advantage", instead.[13] As one interviewee lamented:

> **"Our cloud industry today is largely taking components, software built in the States. We're not doing the core engineering. Microsoft, Google, AWS in [Europe]: they're sales and marketing organisations. There's no development, there's no engineering, there's no academic research. So the benefit to our economy is very limited."**



[11] For an in-depth discussion, see Michels, Millard, and Walden, "On Cloud Sovereignty: Should European Policy Favour European Clouds?", (2023) papers.ssrn.com/sol3/papers.cfm?abstract_id=4619918.

[12] See e.g. European Commission, "Communication: A New Industrial Strategy for Europe", Brussels, 10.3.2020 COM(2020) 102 final; European Commission, "2030 Digital Compass: the European way for the Digital Decade", (2021) 9.3.2021 COM(2021) 118 final.

[13] See e.g. European Commission, "A European strategy for data", (2020) 19.2.2020 COM (2020) 66 final.

2.3 WHAT DOES SOVEREIGN CLOUD MEAN TO CLOUD PROVIDERS?

European cloud providers often see sovereignty as an opportunity to differentiate their services. For example, IONOS, Schwarz Digits, Orange, and OVHcloud all promote their sovereign cloud credentials;[14] while SAP and Arvato are developing a sovereign cloud (called Delos) for the German public sector,[15] as are Orange and Capgemini (Bleu) in France.[16] As one interviewee put it:

> **"They are American, so a user putting data on the hyperscaler, they are not immune to the extra-territorial law. [...] So only non-sensitive data should go to these hyperscalers. And that's where a smaller-sized provider [...] can compete, because we can provide the sovereignty capacity that the hyperscalers don't have."**

By contrast, **US hyperscalers** see sovereign cloud as both a challenge and an opportunity. They are marketing their own 'sovereign' services, which typically combine data residency guarantees with strong encryption that prevents provider access to customer content data in the clear. This includes client-side and "Bring Your Own Key" encryption; third-party key management by a trusted European partner;[17] and confidential computing.[18]

In addition, US providers can challenge US production orders under US law, including on the basis of comity. Indeed, some providers contractually commit to challenging any foreign government request for access to customer data that conflicts with European law.

Yet there are limits to such approaches. Microsoft's EU data boundary[19] involves some metadata being transferred to the US. Further, encryption can protect data at rest in a simple storage service, but might not work for data in use, especially if the provider needs access to data in the clear in order to offer functionality beyond simple storage. Further, encrypting content data does not protect the metadata a provider collects, while confidential computing is a relatively new technology that adds cost and complexity.

At the same time, US hyperscalers also **downplay the risk** of US government access. They point to the very low number of US law enforcement production orders under the SCA, as recorded in their annual transparency reports. Indeed, AWS states that it has never disclosed customer data stored in Europe pursuant to such an order since it started reporting this data in July 2020.[20]

---

[14] See e.g. cloud.ionos.co.uk/white-paper/cloud-act; schwarz-digits.de/digital-sovereignty; digital.orange-business.com/en-en/expertises/sovereign-cloud; ovhcloud.com/en/about-us/data-sovereignty/

[15] G. Wolf, "First Sovereign Cloud Platform For The German Administration On The Home Straight", 24 September 2024, https://www.bertelsmann.com/news-and-media/news/first-sovereign-cloud-platform-for-the-german-administration-on-the-home-straight.jsp.

[16] "Capgemini and Orange are pleased to announce the launch of commercial activities of Bleu, their future "cloud de confiance" platform", 17 January 2024, https://www.capgemini.com/news/press-releases/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/.

[17] See e.g. T-Systems with AWS and with Google: t-systems.com/de/en/insights/newsroom/news/data-protection-as-managed-service-498622; t-systems.com/de/en/sovereign-cloud/solutions/sovereign-cloud-powered-by-google-cloud#anchor_595270.

[18] See e.g. AWS Nitro: aws.amazon.com/blogs/security/delivering-on-the-aws-digital-sovereignty-pledge-control-without-compromise/.

[19] See Microsoft, "The EU Data Boundary for the Microsoft Cloud", microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb.

[20] AWS, "Meeting digital sovereignty requirements on AWS" (2022), d1.awsstatic.com/events/Summits/reinvent2022/SEC205_Meeting-digital-sovereignty-requirements-on-AWS.pdf.

However, US intelligence agencies also have powers to issue production orders to obtain foreign intelligence information. Under FISA Section 702, the NSA can issue directives to cloud providers and can share the data it obtains with the CIA and the FBI. US law prohibits cloud providers from publishing details of such orders in their transparency reports.[21] This makes it difficult to assess the frequency of such disclosures. As one interviewee noted:

> **"Microsoft, AWS and Google, they say: 'we don't receive a lot of requests'. The reality is we don't know, 'cause they're not allowed to tell us. You could say, well, that's just a theoretical risk, but whether it has been realised or not, we have no way of knowing."**

In response, some European cloud providers object to US hyperscalers labelling their services as 'sovereign', which they consider "sovereignty-washing". One interviewee stated that:

> **"There's a real conflation between data residency and data sovereignty happening in the market at the moment. […] Hyperscalers taking the sovereignty mantle is really dangerous for the local providers because it's the local providers who can provide that absolute niche, genuine sovereign service for the people who genuinely need it."**

Another remarked:

> **"The hyperscalers have a habit of changing terms to suit what it is that they're selling. So something is marketed as X and then they change the meaning of X to meet the marketing."**

At the same time, US companies can also **work together with European providers** to create sovereign cloud solutions. For example, a US company can provide cloud software, while the European company operates the infrastructure, deploys the software, and manages the customer data in such a way that the US company cannot access those data (also called 'isolation'). For instance, both Delos and Bleu will offer Microsoft Office 365 to German and French customers as part of a sovereign cloud package, which they operate in isolation from Microsoft. Similarly, Broadcom supplies VMware software to European providers, who then focus on secure and isolated deployment, delivery, and customer management. Such arrangements benefit European customers by providing access to US software (which is often industry-standard and cutting-edge), while protecting data from foreign government access.[22]

[21] Cloud providers must comply with FISA Section 702 orders in a manner that protects "the secrecy of the acquisition". They can only publish the total number of orders they receive in bands of 1,000, as well as the number of accounts targeted, on a twice-yearly basis. See US Deputy Attorney General J. Cole, "Letter to General Counsels of Facebook, Google, LinkedIn, Microsoft, and Yahoo", 17 January 2014.

[22] Using a US software provider would not expose European customer data to US production orders, provided the US company cannot access European customer data. Those data would not be in the US company's possession, custody, or control – as required under the SCA, amended by the CLOUD Act.

3. What is driving demand for sovereign cloud?

3.1 WHY CHOOSE SOVEREIGN CLOUD?

Regulation is the primary external driver for European customers seeking sovereign cloud.

In particular, there are concerns under the **GDPR** as to whether a US provider can offer the sufficient guarantees of compliance required of a processor of European personal data.[24] These concerns are described in more detail in Section 3.2.

In addition, some Member States also impose **national regulations** that require data localisation in Europe and the use of cloud providers not subject to foreign control. For example, the French SecNumCloud certification scheme requires a cloud provider that is not subject to foreign ownership. The French government has decided only to use SecNumCloud-compliant cloud services.[25] This policy appears to rule out the use of Office 365 based on Microsoft cloud infrastructure.[26] That said, the policy is not always strictly adhered to in practice. For instance, the French Health Data Hub is hosted by Microsoft, despite objections from the French data protection regulator (the CNIL).[27]

By contrast, it appears that ENISA will not include such requirements in the final version of the EU Cloud Certification Scheme (**'EUCS'**). A leaked draft had previously suggested that the scheme would feature a highest level of assurance that required providers to be subject to European ownership.[28] However, this proposal led to political disagreement between Member States and will reportedly be dropped from the final version.

[23] Capgemini, "The Journey to Cloud Sovereignty", 2022, p.25.

[24] A controller can only use a processor that offers sufficient guarantees of compliance under Art.28 GDPR.

[25] See J. Castex, "Circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État", 5 July 2021, legifrance.gouv.fr/circulaire/id/45205; ANSSI, "Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences", v.3.2, 8 March 2022.

[26] Note aux secrétaires généraux des ministères; objet: doctrine "cloud au centre" et offre 365 de Microsoft, 15 September 2021, https://acteurspublics.fr/upload/media/default/0001/36/acf32455f9b92bab52878ee1c8d83882684df1cc.pdf.

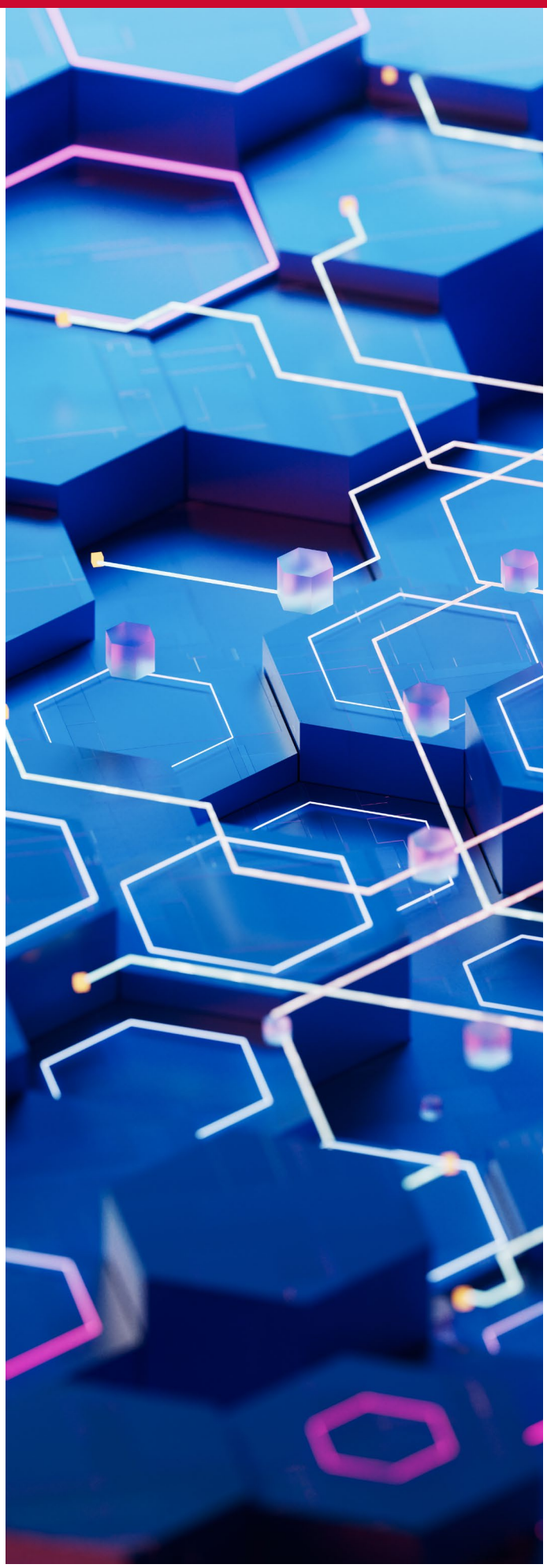
[27] Conseil d'Etat, CE - N° 444937, 14 October 2020. For a discussion of developments in France, see T. Christakis, "The Zero Risk Fallacy", CIPL paper February 2024, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_zero_risk_fallacy_-_t.christakis_feb24.pdf.

[28] See L. Cerulus, "Big Tech cries foul over EU cloud-security label", Politico Pro 22 June 2022, https://www.politico.eu/article/tech-sector-foul-eu-cloud-security-label/.

Finally, some customers have strong **internal reasons** for protecting their data from foreign government access. This includes customers that process data which are sensitive from a geopolitical or national security perspective, such as state intelligence agencies or the defence sector. It can also apply to universities conducting research in sensitive sectors (such as encryption algorithms, AI, or quantum computing), or companies looking to protect valuable trade secrets. Such organisations can also impose sovereignty requirements on their sub-contractors. Thus, sovereignty requirements can pass down through a supply chain.

Other customers simply want the 'comfort' of knowing where their data are stored and who can access them. In some cases, this can stem from fear or uncertainty over regulation, rather than a specific regulatory requirement. As one interviewee noted:

> **"There's other cases where it's regulatory driven, but it's not necessarily prescribed by the regulation. So it's more of an interpretation of regulations or erring on the side of caution. Maybe there's nothing specific that says I can't put this data over here. There are some rules about privacy, so maybe I just feel more comfortable about having it over here."**



3.2 DOES THE GDPR REQUIRE THE USE OF SOVEREIGN CLOUD?

When a cloud provider discloses European personal data to the US government, it does so without customer instructions and without a basis in EU or Member State law.[29] Indeed, in many cases, US law requires the provider to disclose data without notifying the customer.[30] In doing so, the provider would appear to breach the GDPR, as further detailed in Figure 2 below.

This problem applies especially to processing of so-called 'special category' data, such as those relating to health and ethnicity.[31] Both the CNIL in France and the European Data Protection Supervisor ('EDPS') have highlighted concerns regarding the use of cloud providers subject to foreign jurisdiction.[32]

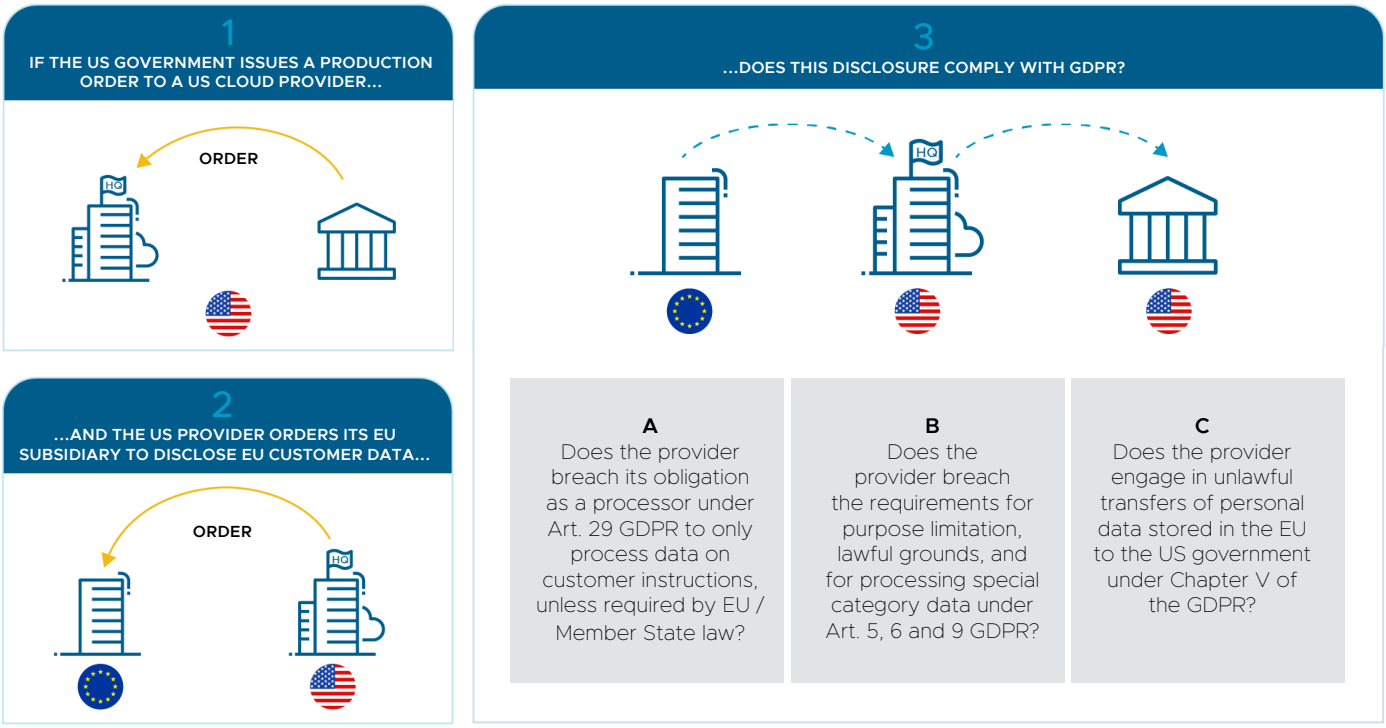


Figure 2: GDPR compliance concerns when a cloud provider discloses data to the US government

[29] For a detailed analysis, see Michels et al., "Cloud Sovereignty and the GDPR", (2024) papers.ssrn.com/sol3/papers.cfm?abstract_id=4911552.

[30] As noted above, cloud providers must comply with FISA Section 702 orders in a manner that protects the secrecy of the acquisition. In addition, a US court can prohibit a cloud provider from disclosing the existence of a production order issued under the SCA, as amended by the CLOUD Act, if necessary to protect an investigation.

[31] See GDPR Article 9.

[32] See CNIL, "Cloud: the risks of a European certification allowing foreign authorities access to sensitive data", 19 July 2024, cnil.fr/en/cloud-risks-european-certification-allowing-foreign-authorities-access-sensitive-data; EDPS, "Investigation into Use of Microsoft 365 by the European Commission" (Case 2021-0518), Decision of 8 March 2024.

The 2023 EU-US Data Privacy Framework[33] ('DPF') does not resolve these issues. The DPF provides a basis for commercial data transfers to the US.[34] It is less clear whether it can support transfers for the purposes of disclosure to the US government. In any event, it simply doesn't address the absence of customer instructions or the lack of lawful grounds for processing under Articles 6 and 29 of the GDPR, which are separate issues from the lawfulness of transfers under Chapter V. Lastly, it remains to be seen whether the CJEU will accept that US law offers an equivalent level of protection or whether it will overturn the DPF. As one interviewee stated:

> **"I had a call with this customer […] and he was really posing the question like: 'What if we will have Schrems 5? Are the US hyperscalers a sustainable solution? […] if we build everything in AWS and at some point, it's not compliant, what then?' […] 'Is this a wise choice?' Looking at the future: will the Data Privacy Framework hold?"**

Regulation	Jurisdiction	Summary of relevant provisions
1. Stored Communications Act ('SCA')	US	Grants US federal agencies and courts powers to issue production orders to cloud providers to disclose data for law enforcement purposes.
2. CLOUD Act	US	Clarifies that the SCA obligations apply to any data within a provider's custody, possession, or control, regardless of data location.
3. FISA Section 702	US	Grants US intelligence agencies powers to issue production orders to cloud providers to disclose data for foreign intelligence purposes.
4. GDPR	EU	Imposes obligations on cloud providers to protect European personal data, including restrictions on international transfers.
5. EU, US Data Privacy Framework ('DPF')	EU	Permits commercial transfers of data from a European exporter to a US importer under the GDPR.
6. Data Act	EU	Imposes obligations on cloud providers to support switching, portability, and interoperability, and to identify the jurisdiction(s) to which the service is subject.

Figure 3: Table of relevant US and EU legislation which can lead to conflicts

[33] https://www.dataprivacyframework.gov/Program-Overview

[34] The DPF supports transfers between a European exporter and a US importer that has self-certified under the DPF program, administered by the International Trade Administration within the US Department of Commerce.

Of course, European governments can also issue production orders to cloud providers to obtain customer data, both for law enforcement and intelligence purposes. So, data held by a European cloud provider are also subject to government access. Yet disclosures to European governments do not pose the same compliance challenges under the GDPR, since there is a legal basis for the disclosure under EU or Member State law. Moreover, unlike US production orders, the exercise of European government powers is subject to European human rights law and is (ultimately) overseen by European courts.

Further, the problem is only partially resolved **in the UK** under the UK GDPR.[35] In 2019, the UK entered into a CLOUD Act Agreement with the US, which permits UK service providers to respond to US production orders (and vice versa) from 2022.[36] This legitimises disclosures of personal data to the US government, as explicitly recognised in the draft Data Use and Access Bill, proposed in October 2024.[37] However, the UK-US agreement is limited to disclosures for law enforcement purposes.[38] So, a cloud provider subject to the UK GDPR can disclose customer data to the US government for the purposes of law enforcement under the SCA. However, it might still breach the UK GDPR if it discloses data for the purposes of foreign intelligence under FISA Section 702. As a result, FISA Section 702 production orders continue to pose a compliance challenge for cloud providers under the UK GDPR.

In future, the conflict between US production orders and European data protection law could be resolved by a **comprehensive EU-US treaty** on cross-border government access to cloud data. Such a treaty could provide a legal basis for cloud providers to disclose European customer data to the US government (and vice versa), both for the purposes of law enforcement and of foreign intelligence. Although politically sensitive, such a comprehensive agreement could form the basis for international "data free flow with trust" among allied nations – a concept endorsed by the Group of Seven ('G7') in 2023.[39]

[35] Post-Brexit, the UK incorporated the rules of the EU GDPR into its domestic law to create the UK GDPR.

[36] Strictly speaking, the agreement requires each State to ensure that its domestic laws permit cloud providers to make such disclosures. See https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern.

[37] See Data (Use and Access) Bill [HL], s.9(a) and Schedule A1 https://bills.parliament.uk/bills/3825.

[38] The Explanatory Memorandum to the Agreement notes that "[o]rders for data can only be made under the Agreement for the purpose of the prevention, detection, investigation or prosecution of a serious crime".

[39] G7, "Ministerial Declaration - The G7 Digital and Tech Ministers' Meeting", 30 April 2023, https://g7g20-documents.org/database/document/2023-g7-japan-ministerial-meetings-ict-ministers-ministers-language-ministerial-declaration-the-g7-digital-and-tech-ministers-meeting.

3.3 WHY NOW?

Recent developments highlight the need for European organisations to carefully consider cloud sovereignty. In March 2024, the **EDPS** held that the Commission had breached **European data protection law** when using Microsoft Office 365 in the cloud.[40] In particular, it found that the Commission had failed to protect the confidentiality of data processed in the EU and to prevent their disclosure to the US government. It ordered the Commission to bring its cloud use into compliance within six months and suggested that the Commission consider running Office 365 software on its own, in-house servers. In May 2024, Microsoft and the Commission appealed the EDPS findings before the CJEU.[41]

Breaching the GDPR can lead to fines of up to €20m or up to 4% of global turnover. In addition, a European organisation that knowingly exposes sensitive personal data to the risk of foreign government access could face significant reputational damage, should such access be publicly revealed. Further, the growing **use of AI** could increase the risk that foreign governments pose to European data subjects. US intelligence agencies might use AI to sift through and spot patterns in ever-larger datasets. As one interviewee observed:

> **"AI will be absolutely jumped upon by security services [...] they've been gathering data for decades. They've just never known what to do with it. Now the new technology has caught up with the massive data that they've got and it enables them to make some sense of it."**

Lastly, the **new Trump administration** might pursue an 'America First' agenda in foreign affairs. This could amplify the concerns European policymakers have about the reliance on US services.

[40] EDPS, "Investigation into Use of Microsoft 365 by the European Commission" (Case 2021-0518), Decision of 8 March 2024.

[41] The appeals cases are pending as of the time of this report. See EDPS, "The EDPS follows up on the compliance of European Commission's use of Microsoft 365", 10 December 2024, https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-follows-compliance-european-commissions-use-microsoft-365_en.

3.4 WHAT CHALLENGES DO EUROPEAN CUSTOMERS FACE WHEN ADOPTING SOVEREIGN CLOUD SOLUTIONS?

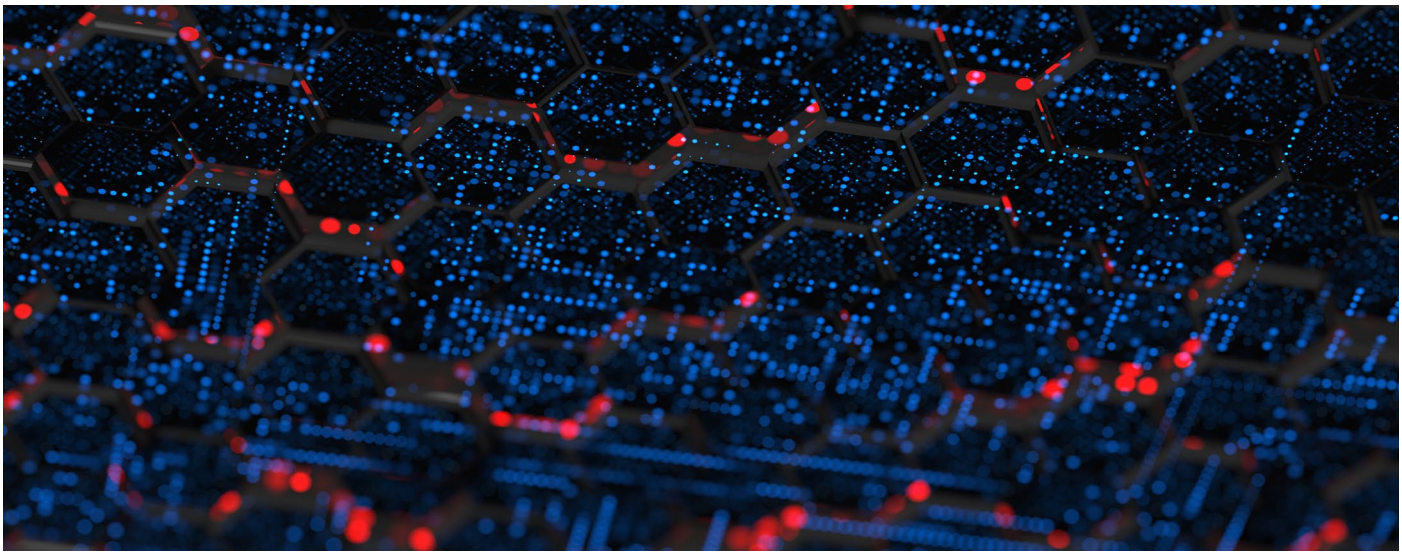
An organisation that wants to adopt sovereign cloud as part of a hybrid or multi-cloud solution can face three main challenges.

First, the organisation needs to review its workloads and **classify the data** it processes in terms of technical, security, and compliance requirements. For example, it needs to understand which data are sensitive and so require extra protection, whether as personal data under the GDPR or from a commercial perspective.

Second, it needs to determine which IT resources best meet its needs, including by comparing and possibly combining services from different providers. However, a **lack of interoperability** can make it more difficult for a customer to combine different services from different providers. Interoperability can support integrated cloud deployments across multiple providers, instead of running separate, siloed workloads.

Lastly, organisations must consider **portability,** a lack of which can prevent customers migrating data or applications from their current cloud provider to another provider. This can hamper a customer who wants to switch cloud providers, so as to benefit from the advantages that different services offer.

In theory, the **EU Data Act** should support customer switching when it applies to cloud providers from September 2025, including by removing egress fees. The Data Act requires IaaS providers to support switching by providing technical support and tools to enable customers to achieve functional equivalence after switching. SaaS providers must provide open interfaces that facilitate the switching process and support data portability and interoperability.[42] However, it is too early to say how these new obligations will be applied and enforced. In any event, the Act is unlikely to resolve all challenges in practice, especially when a customer has



[42] Data Act, Art. 23, 24, 28-29, 30.

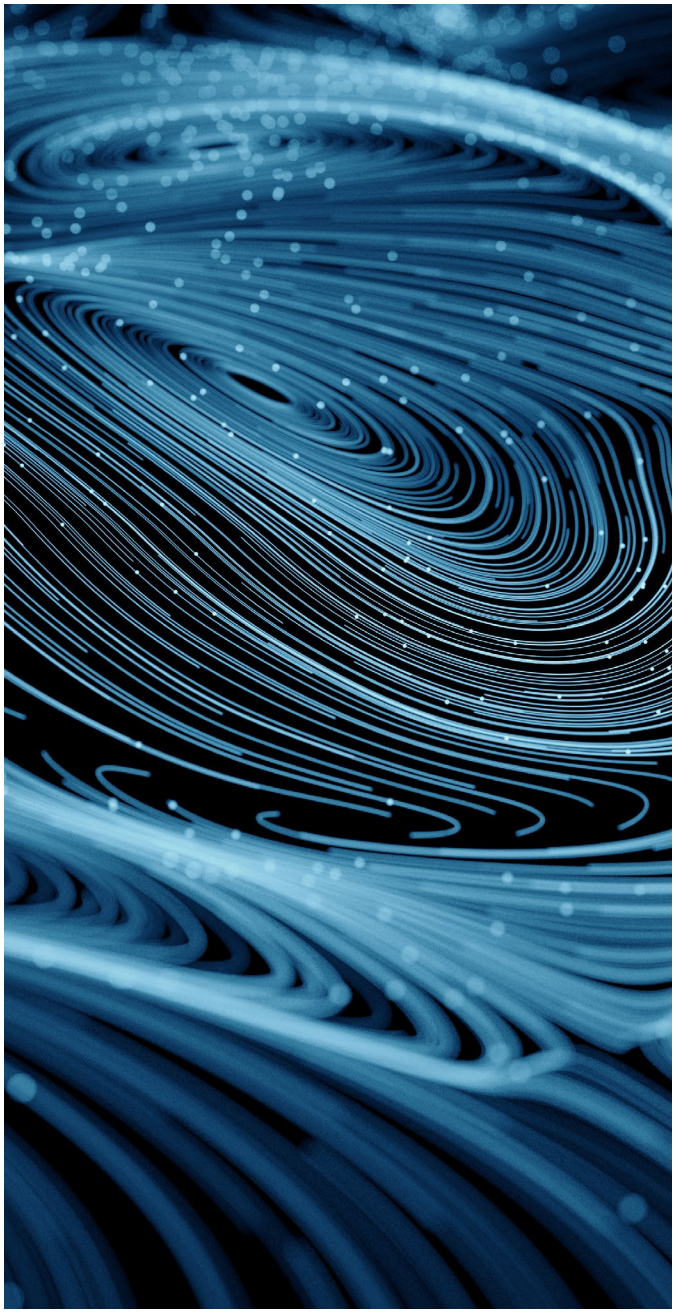
designed its workload to run within a specific provider's cloud environment, including in terms of provider-specific functionality, performance, cost, and security. As one interviewee put it:

> **"They've all waived their egress fees in response to the EU Data Act. But that's not where the real cost of switching lies. It's with reskilling your teams. It's with re-architecting your applications."**

Another interviewee mentioned the example of a bank which had estimated that switching cloud providers would require a multi-$100m USD investment, stating:

> **"They've realised too late that they are now so locked in, it's a total re-architecture of everything they've done. It isn't just a case of moving [...] workloads and storage. It's unpicking the mess [...] of the monitoring tools, the security tools, the networking tools, [...] the backup protection, the operational processes and standards, the governance that flows over the top, which is all unique to the cloud provider."**

Lastly, in some cases, a European organisation might conclude that there simply is no cloud service that can fully support its sovereignty needs. For example, in 2024, the CNIL authorised a public interest group to use a Microsoft cloud service to process health data, after it concluded that there was no "sovereign solution" available that would meet the project's requirements.[43] Similarly, in 2025, the European Commission stated that it had not yet identified a "functionally equivalent alternative" to Microsoft Office 365.[44]



[43] CNIl, "Délibération n° 2023-146 du 21 décembre 2023 autorisant le groupement d'intérêt public " Plateforme des données de santé " à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données dans le domaine de la santé, dénommé " EMC2 ". (demande d'autorisation n° 2229962v1)", 31 January 2024, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000049057224.

[44] J. Wulff Wold, "Internal documents reveal Commission fears over Microsoft dependency", 9 January 2025, Euractiv, https://www.euractiv.com/section/tech/news/internal-documents-reveal-commission-fears-over-microsoft-dependency/.

4. Proposal: A new Sovereign Cloud Code of Conduct

Since there is no official definition of sovereign cloud, both European and US providers promote their own services as 'sovereign'. What's more, there are various areas of legal uncertainty regarding the use of cloud providers subject to foreign jurisdiction. This applies especially to highly regulated sectors that regularly process sensitive personal data, such as healthcare. European regulators have failed to provide clear guidelines on what exactly is required under the GDPR. These mixed messages can confuse customers, some of whom might simply decide not to use cloud services at all.

The cloud industry can address the uncertainty under the GDPR by jointly developing a new **Sovereign Cloud Code of Conduct.** Once approved by a regulator, the Code would provide legal certainty as to the level of protection from foreign government access required under the GDPR. Cloud providers as processors can then adhere to the Code, in order to demonstrate compliance.[45] And customers can confidently use a Code-compliant sovereign cloud, since their data will not be subject to an inappropriate level of risk of foreign government access.

Today, there are **two approved codes of conduct** for cloud services. The first code was approved by the CNIL in 2021 and is adhered to by AWS, OVH, Tencent, and others.[46] The second was approved by the Belgian Data Protection Authority in 2021 and is adhered to by Microsoft, Google, Alibaba, Huawei, Cisco, Dropbox, IBM, Oracle, Salesforce, SAP, and others.[47] Both codes cover a range of topics, including security measures such as physical security, access management, and encryption. However, neither code addresses the risk of foreign jurisdiction and foreign production orders from the US, the Chinese, or any other foreign government.

A new Sovereign Cloud Code would build on these existing codes and address this specific gap. The Code could recognise different models that **reduce the risk** of foreign government access. For example, a European provider might simply not be subject to US jurisdiction because it does not have contacts with the US market. Alternatively, a US provider might reduce the risk through technical measures, such as pseudonymisation, encryption with third-party key management, or confidential computing.

The Code can also help cloud providers comply with new obligations under the Data Act regarding non-personal data. From September 2025, cloud providers are required to: (i) identify "the jurisdiction to which the ICT infrastructure deployed for data processing [...] is subject"; and (ii) describe the "technical, organisational and contractual measures" it has adopted "to prevent international governmental access" to non-personal data stored in the EU.[48]

Unlike the leaked draft of the EUCS, the Code would not focus on European ownership. Instead, it would focus on effectively reducing risks to the fundamental rights and interests of European data subjects, while recognising that providers can reduce those risks in different ways.

[45] See GDPR, Art.28(5), 40-41.

[46] The Cloud Infrastructure Service Providers in Europe ('CISPE') Code.

[47] The EU Cloud Code of Conduct ('EUCoC').

[48] See Data Act, Art.28 (although the obligation to describe measures only applies where foreign government access would "conflict with Union law or the national law of the relevant Member State"). See also Data Act, Art.32.

The Code reframes the issue as one of regulatory risk management, while aiming to avoid contentious policy questions which are subject to Member States' competing political preferences. Further, industry can take the lead in preparing the Code, while engaging with regulators for its approval.

Preparing a code of conduct is an ambitious, multi-year project. It requires assembling a community of providers to act as an industry body that will: (i) agree on a draft code; (ii) select a monitoring body;[49] (iii) hold a consultation on the draft; (iv) obtain an EDPB opinion; and finally, (v) obtain the approval of a national regulator and the Commission for validity across the EU.[50] By participating in this process, providers can demonstrate their commitment to European cloud sovereignty and personal data protection. Once approved by a regulator, the resulting legal certainty should benefit customers and providers alike, as well as assure European data subjects that their fundamental rights are protected in the cloud.

[49] A monitoring body, accredited by the regulator, confirms that a cloud provider complies with a Code. EY Certifypoint monitors the CISPE Code; Scope Europe monitors the EU Cloud Code of Conduct.

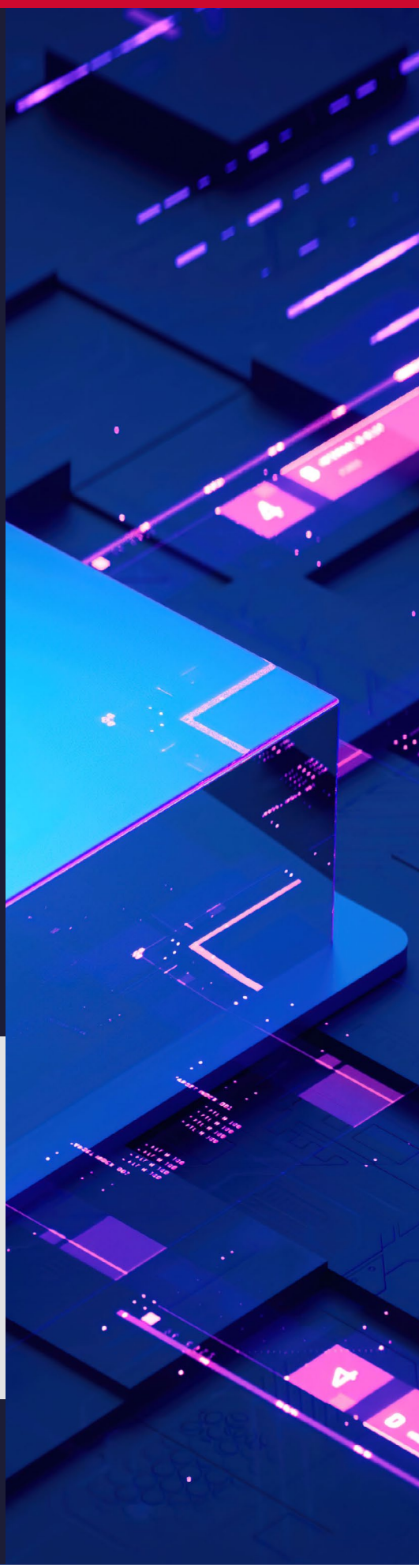
[50] See GDPR, Art.40(6)-(9).

FURTHER READING

- **Blancato, F. G. & Carr, M.** "The trust deficit. EU bargaining for access and control over cloud infrastructures" (2024) Journal of European Public Policy.
- **Brown, I. & Korff, D.,** "Exchanges of Personal Data After the Schrems II Judgment" (2021) Study for the European Parliament LIBE Committee.
- **Chander, A. & Sun, H.** (eds.), Data Sovereignty: From the Digital Silk Road to the Return of the State (OUP, 2024).
- **Chrétien, J. & Drouard, E.**, "European Technological Sovereignty", (2022) Renaissance Numerique.
- **Christakis, T.**, "Data Free Flow with Trust" (2024) Journal of Cyber Policy.
- **Hemmings, J. et al.**, "Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act" (2020) Journal of National Security Law and Policy.
- **Juliussen, B.A., et al.** "The third country problem under the GDPR: enhancing protection of data transfers with technology", (2023) International Data Privacy Law.
- **Lehdonvirta, V. et al.** "Weaponized interdependence in a bipolar world: How economic forces and security interests shape the global reach of U.S. and Chinese cloud data centres" (2025) Review of International Political Economy.
- **Mignon, E.** "The CLOUD Act: Unveiling European Powerlessness" (2020), RED 1:1.
- **Millard, C.** (ed.), Cloud Computing Law (2nd edn, OUP, 2021).
- **Moerel, L. & Timmers, P.** "Reflections on Digital Sovereignty", (2021) EU Cyber Direct Research in Focus Series.
- **Schwartz, P.M.**, "Legal Access to the Global Cloud" (2019) Columbia Law Review.
- **Shurson, J.** "Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law", (2020) International Journal of Law and Information Technology.

ABOUT THE AUTHOR

Johan David Michels is a researcher with the Cloud Legal Project at the Centre for Commercial Law Studies, Queen Mary University of London, and a Guest Teacher at the London School of Economics. He has published articles covering cloud and IT services in leading US and European law journals and is a co-author of Cloud Computing Law (2nd edn, OUP, 2021). Before joining academia, he worked as a Strategy and Policy Associate at Ofcom (the UK telecommunications regulator) and as an Associate Legal Officer at the United Nations in the Hague.



BROADCOM® | Queen Mary University of London