From Barriers to Bridges

Cloud Computing in Support of Privacy and Security

September 2024

Centre for Information Policy Leadership

HUNTON ANDREWS KURTH

Table of Contents

Executive Summary

CIPL[1] has been at the forefront of the development and promotion of effective global solutions and best practices in accountable and responsible data use in the context of current digital realities. In the modern economy, cloud computing continues to be a transformative technology for digital societies, enabling digital transformation while at the same time driving privacy, security and economic efficiencies. Both public and private sector organisations are embracing the different cloud computing models and the benefits they can offer at scale, such as enhanced data security, strong encryption both in storing and transmitting data, effective access control mechanisms, access to privacy-enhancing technology, secure data transfers, as well as robust data governance and accountability.

However, legal and policy developments, especially in Europe, have created barriers towards truly global public cloud solutions. Digital sovereignty has become a major factor in the EU's digital policy considerations. Initiatives like the Gaia-X project and the European Union's Cloud Certification Scheme under the EU Cybersecurity Act reflect a shift towards centralising more control and management of digital resources in Europe. These initiatives aim to enhance Europe's autonomy in digital technologies and data management in a geopolitically tense environment. At the same time, data protection authorities in Europe have been taking a conservative approach to international data transfers, away from the risk-based approach enshrined in the GDPR.[2]

In response, many cloud providers have developed specialised data localisation solutions. These tools are tailored to meet the specific demands of European clients who are uncertain of their compliance obligations.

In this CIPL discussion paper, we show the complexities in navigating the regulatory landscapes in the context of providing cloud computing services and advance recommendations for the beneficial adoption of cloud computing technologies. In particular, we:

a. demonstrate how the adoption of cloud services can enhance privacy and security and facilitate the deployment of global data compliance programs;

b. critically analyse trends in the enforcement practices around the adoption of cloud services;

c. explore the influence of legal, technical and policy factors on the adoption of cloud services; and

d. present strategies for the development of an efficient and secure cloud infrastructure.

1 CIPL is a global privacy and data policy think and do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website.

2 Theodore Christakis, The "Zero Risk" Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach.

Summary of CIPL recommendations:

1. **Understanding Data Localisation Impact Including on Privacy and Security:** EU Member States and DPAs need to deepen their understanding of the limitations of data localisation measures and adopt a balanced and pragmatic view. It is crucial for regulators and policymakers to recognise the potential of cloud computing for data protection and acknowledge that data localisation does not equate to better security or privacy. In our globally connected world, technical, legal and organisational safeguards should prioritise the protection of data itself, irrespective of geographic borders. With the emerging importance of trusted AI products, it is more essential than ever for data protection to be viewed at the product security and privacy controls level rather than geographic boundaries.
2. **Risk-Based Approach to International Data Transfers:** Adopt a risk-based approach to assessing the risk in international data transfers that appropriately considers the likelihood and severity of risk, balancing the need for privacy protection with the necessity of global data flows in the digital society, including in cloud computing.
3. **Onward Transfers:** Recognise the importance of onward transfers to enable the global functioning of cloud services. Also, acknowledge that onward transfers, as in the case of EU-US DPF, are accompanied by accountability principles and requirements which ensure that personal data transferred from the EU continues to receive adequate protection.
4. **Recognise and Incentivise Accountability-Based Measures:** Promote accountability-based measures in cloud computing, ensuring that service providers can demonstrate their data management, privacy and security practices and safeguards as foreseen in the GDPR via tools such as certifications and approved Codes of Conduct. These should take into account already existing internationally recognised standards and certifications that do not impose data localisation requirements but promote the uptake of secure cloud computing in both the public and private sectors. These advanced certifications should address emerging challenges in cloud computing and focus on robust benchmarks for privacy and data security regardless of the location of the data.
5. **GDPR Concepts of Controller and Processor:** Recognise the evolving nature of GDPR concepts of controller and processor, with cloud service providers also acting as controllers for specific "service data" processing.
6. **Strengthened International Cooperation and Convergence Based on Free Data Flows with Trust:** Actively work towards convergence in international data flows based on free data flows with trust and agreements, enabling e-evidence access to data by law enforcement agencies. This includes supporting and building on frameworks like the Global Cross-Border Privacy Rules (CBPR), the Global Privacy Recognition for Processors (PRP), G7 Data Free Flow with Trust and OECD Principles on Government Access to Personal Data Held by Private Sector Entities. This approach would balance law enforcement access to data with stringent privacy protections, ensuring that cross-border data access respects individual rights and adheres to international norms. Cross-recognition of accountability frameworks, compliance certifications or binding codes of conduct can ensure higher levels of data protection by organisations and elevate the trust of individuals.

I. Introduction

Cloud computing is categorised into various deployment and service models, each offering distinct capabilities to cater to different organisational needs. Deployment models typically include public, private, hybrid and community clouds. Public clouds are managed by third-party providers and offer resources over the Internet to multiple customers. A private cloud, on the other hand, is exclusively used by a single organisation, providing greater control over data and infrastructure. Hybrid clouds combine public and private clouds, allowing data and applications to be shared between them, offering flexibility and optimisation. Lastly, community clouds are shared by several organisations with common interests or regulatory requirements, ensuring that resources are tailored to their specific needs. While this paper primarily focuses on public, hybrid clouds and hyperscalers,[3] many of the challenges raised in this paper also apply to other cloud deployment models.

Cloud computing has become an essential technology in the digital transformation of both private and public sector organisations, delivering IT services, operational efficiency and productivity at scale. With the accelerated developments in AI technologies, cloud computing has become an essential foundation stone for supporting the successful development, training and adoption of AI technologies across all sectors. As such, it is also crucial to the functioning and progress of our digital society. The recent Draghi Report, also, concludes that cloud plays a major role in digital infrastructure.[4]

Eurostat data indicates that in 2023, 45% of EU enterprises utilised cloud computing services, a figure expected to increase substantially in the future.[5] Although the rate of adoption varies within the EU, in some Member States, such as Finland, Sweden, Denmark and the Netherlands, nearly 60% of enterprises now rely on cloud computing services.

This rising trend extends, albeit at a lower rate, to the public sector, where an increasing number of public organisations are turning to cloud services as part of an overall public sector digital modernisation effort or to ensure data security or service continuity in case of a crisis. For example, the UK government operates a 'Cloud First' policy, which requires government organisations to default to cloud services where possible.[6] Estonia opened a Data Embassy, which creates a cloud-based backup of critical and sensitive state data to preserve it in unforeseen circumstances, including in cases of war or physical destruction of data.[7] Similarly, just before Russia's invasion in February 2022, the Ukrainian government moved all of its critical government, tax, banking, education and property data to the cloud. This was to ensure that the data was kept secure and away from the danger of physical destruction, and it has been a successful and essential part of the war effort protecting Ukraine's government and civilians.[8]

3 Hyperscalers are described as large cloud service providers that can provide services such as computing and storage at enterprise scale.

4 Simply put, cloud computing relies on remote servers rather than local servers to deliver resources and services. Cloud computing includes Infrastructure as a Service (IaaS) (providing computing power, storage or network capacities), Software as a Service (SaaS) (ready-to-use applications hosted in the cloud) and Platform as a Service (PaaS) (ready-to-use platforms for developing, running and managing applications), and as already mentioned AI as a Service (cloud-based service offering AI outsourcing). Mario Draghi Report, The Future of European Competitiveness.

5 Eurostat, Cloud computing—statistics on the use by enterprises.

6 https://www.gov.uk/guidance/government-cloud-first-policy.

7 https://e-estonia.com/solutions/e-governance/data-embassy/; https://eimin.lrv.lt/en/structure-and-contacts/digital-embassy-launches-to-improve-security-of-state-data-in-emergencies/

8 https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002.

Some of the efficiencies private and public sector organisations are able to realise when moving to cloud services include:

- access to advanced technologies (artificial intelligence and machine learning);
- scalability and flexibility;
- privacy and security features;
- disaster recovery planning;
- operational efficiencies;
- on-the-go accessibility;
- decreased maintenance requirements;
- global IT support; and
- energy efficiency and sustainability improvements.

In addition to more tangible operational and resource benefits, privacy and security features are becoming equally important factors and often differentiators in the migration to cloud technology. With the exponential increase in security risks and concerns related to cyberattacks, cloud services, when compared to non-cloud-based solutions, will often provide a superior state-of-the-art level of security that, for many organisations, would otherwise be economically unattainable.

Nevertheless, the use of cloud services increasingly faces significant scrutiny in the European Union. Some of the concerns related to geopolitical tensions and supply chain control in the context of cloud services are relevant and need addressing. However, the continued debate around international data transfers and the regulatory approaches of some EU data protection authorities may curtail the full benefits of cloud services without addressing these geopolitical tensions and supply chain concerns or realising significant gains in protecting the rights of the individual. We will critically examine these operational challenges for the use of cloud services and operations below.

II. Benefits provided by cloud services

As stated above, cloud computing is an indispensable asset for private and public organisations as they continue their digital transformation.[9] The COVID-19 crisis accelerated organisational cloud service adoption due to factors like the need to support remote workforce management and online education, among other factors.[10] The use of cloud computing is, of course, subject to data protection and privacy laws and sector-specific legislation and in many ways, cloud computing can support the privacy and cyber security compliance efforts of the organisations and public authorities using it.

This section outlines some of the benefits of cloud computing and provides detailed explanations of how certain data protection and privacy principles find application in the context of cloud computing.

DATA SECURITY AND PRIVACY

- **Cloud service providers prioritise security as a business imperative.** Security is existential and, therefore, a top priority for the cloud business model. A security breach leads to reputational damage and directly impacts customer trust. Investments in state-of-the-art security technology are the topmost priority for cloud providers. This includes sophisticated detection tools in their products as a foundational element of the cloud offering, as well as robust notification procedures. This also requires sophistication that enables rapid incident responses and teams that can apply lessons learned in a security incident to prevent future disruptions. A globally distributed cloud architecture not only enables greater security at the outset, but also the ability to learn from isolated or regional incidents to apply global solutions.
- **Cloud adoption also means bringing more resources to bear on security.** By leveraging cloud services, organisations can make use of the expertise, technology and resources that cloud providers have built where the organisation would not otherwise have sufficient resources to achieve the same level of security.
- **The cloud's homogeneous and consistent operational environment allows for the standardised application of security measures,** in contrast to on-premise solutions that often grapple with complex and disparate systems accumulated over years or even decades. This streamlined approach in the cloud significantly reduces the technical debt typically associated with securing bespoke on-premises infrastructure that is hard to patch for vulnerabilities and malicious attacks.
- **Cloud offers a robust security baseline by default.** Security is a cornerstone of the shared responsibility model.[11] Features like default encryption, engineered into the cloud's fabric, provide immediate safeguards for data. The ability of CSPs to absorb and repel large-scale malicious attacks further underscores the cloud's resilience. This capacity is often beyond the reach of individual organisations managing on-premises security.

9 The Government of Italy is investing €1 bn to migrate local public administration data to a secure cloud infrastructure as part of the EU's Recovery and Resilience Facility (RRF). Under the RRF, similarly to Italy, many other EU Member States are investing cloud transition.

10 See Lukas Werner and Gerald F. Burch, PH.D., Migrating to the Cloud: How the COVID-19 Pandemic Has Affected the IT Landscape, ISACA, 31 December 2021. See "How COVID-19 has pushed companies over the technology tipping point—and transformed business forever," McKinsey & Company, October 2020; see also Gaurav Aggarwal, "How The Pandemic Has Accelerated Cloud Adoption," Forbes, 15 January 2021.

11 In this model, the CSP is responsible for the infrastructure, and the customer is responsible for the data and the configuration of the data in that infrastructure. By delegating the security of the underlying infrastructure to CSPs, security and compliance teams can redirect their focus towards risk assessment, compliance refinement and higher-order security tasks. This strategic reallocation of resources optimises expertise and allows organisations to concentrate on their core competencies.

- **The cloud's software-centric nature facilitates the automation and monitoring of security controls.** Implementing measures like two-factor authentication or consistent firewall rules becomes efficient and scalable across the entire cloud environment.
- **Cloud service providers are more effective in system security by design** than traditional organisations relying on on-premise technologies. Their strategic approach to security also allows a focus on investments in security measures and continued scouting of new technology to develop and maintain high-level secure systems from the design stage. This also includes heavy investments in the security workforce. Cloud services habitually employ thousands of dedicated, full-time security engineers, ensuring a high level of expertise and specialisation in different areas of security.

STREAMLINED PRIVACY COMPLIANCE

- **Centralised data management mechanisms and process automation** inherent to cloud services can streamline cross-functional compliance efforts; this ensures that security and privacy practices align with each other and regulatory requirements from the start of each project.
- **Cloud services allow for streamlined data governance, offering better data mapping.** Privacy compliance requires visibility over data in different systems, and managing data in the cloud can aid in identification, classification and general governance and management of data One of the major challenges in privacy compliance programs is connecting a regulatory requirement with a particular piece of information held internally. Additionally, traditional approaches to privacy compliance present human-centric challenges such as blind spots, familiarity bias and difficulty in indexing requirements and internal data.
- **Cloud technology can support accountability processes and demonstrate privacy compliance** by producing standardised data privacy impact assessments, more efficient responses to individual rights requests (access, correction, deletion), compliance program reports and evidence for auditors and regulators in an automated way.
- **AI allows the acceleration of initiatives like OSCAL,[12] which provides real-time control-related information in machine-readable formats** so that organisations can provide continuous compliance assurance, facilitating regulatory monitoring and oversight. This not only streamlines the compliance process but also helps to ensure that organisations remain compliant with the latest regulations. Some cloud service providers deploy AI-powered solutions to map new laws and regulations into internal controls, freeing resources for higher-value tasks such as validation and refinement.

12 OSCAL (Open Security Control Assessment Language) is an open, machine-readable language for representing security control assessments developed by NIST. It is designed to facilitate the exchange of information about security controls between organisations and systems and enables the automation of security assessments.

III. Challenges and positive developments related to a wider cloud uptake

1. International Data Transfer Challenges

The full benefits provided by global cloud infrastructures require cross-border data transfers of data. As such, restrictions and limitations on the transfer of personal data in data protection laws, such as the GDPR[13] and the regulatory practices of some data protection authorities, create considerable challenges for both cloud service providers and their customers.[14] In addition, recent legislative additions to the EU digital regulatory package, such as the EU Data Act, add similar restrictions on transfers of non-personal data and raise questions about practicable implementation for cloud providers and cloud customers.[15] Addressing these issues is of critical importance.

The international data transfer provisions of Chapter V of the GDPR stipulate that personal data cannot, by default, be transferred to a country outside of the European Economic Area (a "Third Country")[16] unless the third country provides for an essentially equivalent level of protection or appropriate safeguards are put in place. With regards to cloud services, this typically means that personal data is transferred either in accordance with an adequacy decision or by using standard contractual clauses (SCCs) or binding corporate rules (BCRs).

The European Court of Justice, in its *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* decision (*Schrems II*), mandated organisations exporting personal data from the EU to a third country lacking an adequacy decision to conduct transfer risk assessments on the receiving jurisdictions' legal system and, where necessary, implement additional safeguards when using SCCs or BCRs. This had a profound impact on all organisations relying on international data transfers, including cloud service providers and their customers. They are facing the significant burden of having to conduct their own adequacy determination in what essentially amounts to privatising and shifting the burden of adequacy decisions onto thousands of private and public sector organisations. In addition, the focus on theoretical risk and harm, including that of government access to data and the lack of clear and practical guidance on what constitutes appropriate additional safeguards as required by the Court, is particularly problematic in the context of the use and delivery of cloud services. This risks having a demotivating impact on the use of cloud services by European companies and the public sector, especially on SMEs who lack the resources and expertise to conduct individual risk assessments and adequacy determination and need a much more seamless framework in order to reap scaling and other benefits brought by cloud technologies. [17]

13 Chapter 5, GDPR.

14 Several EU data protection authorities (DPAs) have investigated and scrutinised the use of US-based cloud service providers. Most recently, in March 2024, the EDPS concluded an investigation and issued its decision that the European Commission's use of Microsoft 365 violates "several key data protection rules." Among other practices, the EDPS scrutinised the Commission's contract governing its use of Microsoft cloud services, including the provisions related to international data transfers. See Decision, EDPS Investigation into Use of Microsoft 365 by the European Commission (Case 2021-0518), 8 March 2024.

15 Data Act, Chapter VII, contains transfer restrictions to protect non-personal data in the EU from direct transfers or governmental access stemming from third-country legal frameworks containing transfer or access obligations.

16 In addition, if an organisation located in a Third Country is directly subject to the GDPR (pursuant to Article 3), personal data also cannot, by default, be transferred from this Third Country to another Third Country (commonly referred to as "onward transfer").

17 The € 1.2 billion fine was handed down to Meta by the Irish DPC after intervention of the EDPB for transfer violations despite a recognition that Meta had acted in good faith after *Schrems II*, and before a new framework with the US was negotiated added to the legal uncertainty. The IDPC, after extensive investigation in the judgement, notes: "I considered that the Data Transfers were being effected, in good faith, under and by reference to transfer mechanisms provided for at law" (p. 136). However, this conclusion was rejected by the French, German and Austrian Data Protection Authorities and due to the nature of EDPB decision-making, the IDPC was forced to reject this argument. Judgement available here.

2. The EU-US Data Privacy Framework

In July 2023, after extensive negotiations between the EU Commission and the US government and the implementation of new legal and redress safeguards in the US, the European Commission adopted a new adequacy decision for EU-US data flows in the form of the EU-US Data Privacy Framework (the "EU-US DPF") to replace what was previously Safe Harbor and Privacy Shield. The EU-US DPF introduces new binding safeguards to address the concerns raised by the CJEU and presents an improvement on the CJEU requirements of essential equivalence compared to Privacy Shield. It provides legal certainty for those companies certifying with or using the new Framework to legitimise their transfers of personal data and, crucially, to organisations that are transferring personal data to DPF-certified organisations, such as cloud service providers. Importantly, the conclusion of the DPF and the safeguards implemented by the US government also help those organisations using SCC, as it provides necessary safeguards required by the individual risk assessments conducted by data exporters and, crucially, allows the data to flow without supplementary measures.

Moreover, the EU-US DPF also enables accountable onward transfers of personal data to other countries. Onward transfers, which are subsequent transfers of personal data from controllers or processors in a third country to other controllers, processors or recipients in the same or another third country (including international organisations), are particularly important to cloud providers[18]. Public cloud providers have centres providing varying levels of service support worldwide, and the possibility of onward transfers is crucial to enabling true global functioning of the cloud, continuous global threat intelligence gathering, cybersecurity and 24/7 serviceability. The EU-US DPF recognises the global nature of data flows and, in its Principle 3 on Accountability for Onward Transfers, clarifies the requirements for enabling such transfers, as follows:[19]

- Any onward transfers may only apply for limited and specific purposes.
- Transfers may only occur based on a contract between the recipient of the data located in the US and the third party.
- Transfers are permitted only if the contract requires the third party to provide a level of protection equivalent to the DPF Principles.

Accountability for onward transfers under the DPF, subject to the conditions set out therein, ensures that personal data transferred from the European Union continues to receive adequate protection when cloud providers certified under the DPF share that data with third-party recipients in and outside of the US. It provides for ongoing accountability for such transfers so that businesses and users can benefit from international data flows without compromising protection.

Contractually obligating these third-party recipients to maintain appropriate safeguards, the onward transfer principle helps guarantee consistent data protection during transfers governed by the DPF.

3. Digital Sovereignty

As discussed above, cloud computing is a perennial topic in different policy and regulatory dialogues at the EU and member state levels. In particular, the concept of digital sovereignty and data localisation continues to come to the fore and informs and shapes data localisation discussions and practices[20] with a profound impact on data applications.[21]

18 EDPS defines onward transfers as: Onward transfers are subsequent transfers of personal data from controllers, processors or other recipients in the third country or international organisation to other controllers, processors or recipients in another third country or international organisation or in the same third country or international organization, available here.

19 The EU-US Data Privacy Framework (EU-US DPF), Principle 3 .

20 CIPL and TLS Discussion Paper I: The Real Life Harms of Data Localization Policies.

21 The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU (Luciano Floridi); Digital sovereignty for Europe (EPRS Ideas Paper); See France's Macron lays out a vision for European 'digital sovereignty.' Ryan Browne, CNBC, (8 December 2020).

Concept of Digital Sovereignty as reflected by the EU

The European Council, the European Parliament and the European Commission signed the European Declaration on Digital Rights and Principles for the Digital Decade (the "Declaration")[22] in December 2022. It notes that the EU's way to digital transformation, in particular, encompasses digital sovereignty, meaning the capability for the EU to make its own choices on its values and own rules in the digital agenda.[23]

The Council specified in more detail that: "Ensuring the Union's digital sovereignty in an open manner, in particular by secure and accessible digital and data infrastructures capable of efficiently storing, transmitting and processing vast volumes of data that enable other technological developments, supporting the competitiveness and sustainability of the Union's industry and economy, in particular of SMEs, and the resilience of the Union's value chains, as well as fostering the start-up ecosystem and the smooth functioning of the European digital innovation hubs."[24]

The concept of digital sovereignty is not new. Often, concerns about national security, economic and strategic autonomy, and threats to fundamental rights, are cited as necessitating such schemes. For example, there are legitimate use cases for more digital sovereignty; countries prefer to run their military and defence infrastructure within their national borders. However, despite legitimate concerns in some cases, digital sovereignty policies have not been effective in mitigating other concerns, as the examples we describe below demonstrate.

Instead, as CIPL and the Tech, Law & Security Program at American University's Washington School of Law (TLS) documented in the 2023 discussion paper on the *'Real Life Harms' of Data Localization Policies*, such policies have interfered with production and delivery of many digital products and services that provide value to individuals and society at large. Policies motivated by digital sovereignty have also introduced new risks in areas such as cybersecurity, where localisation mandates can degrade the ability to analyse and transmit data on threats, limit access to state-of-the-art defence applications, disrupt operational continuity and reduce resilience to potential physical attacks on computing infrastructure.[25] In addition, as the examples below demonstrate, digital sovereignty schemes have proven difficult to operate in practice. They are unsuitable for many use cases of market operators; they negate substantial investments made by Member States and increase operational costs, as a result making European companies less competitive.

Digital Sovereignty in Practice: from 'Internetz' to EU Cloud Certification Scheme

Over the last decade, the European Union and its Member States have been exploring various infrastructure and policy initiatives for digital sovereignty in the context of cloud computing.

- As early as 2013, Germany began examining the prospect of a "Europe-only cloud," with Deutsche Telekom (DT) announcing its intention to collaborate with other internet providers to ensure that German internet traffic remains within the country. This initiative (referred to as Internetz) aimed at creating a Germany-exclusive internet network, possibly extending to the Schengen area. Potential models for such a cloud included mandatory use for certain sectors, in particular the public sector, or offering a choice to customers, with certification systems to assure compliance within the Europe-only framework. In the end, the project was abandoned. A number of concerns were raised, including competition, data flow restrictions and the difficulties of identifying national versus international data routing.
- The Gaia-X project was initiated to develop a federated, secure cloud infrastructure for Europe and ensure European digital sovereignty.[26] It has received support from European political leaders as a way to counter the dominance

22 https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

23 Elaine Fahey, 2023, Does the EU's Digital Sovereignty Promote Localisation in its Model Digital Trade Clauses?

24 Decision establishing the Digital Decade Policy Programme 2030.

25 CIPL-TLS, The "Real Life Harms" of Data Localization Policies: Discussion Paper 1, March 2023. See also, "The Effects of Data Localization on Cybersecurity," Peter Swire and DeBrae Kennedy-Mayo, Georgia Tech Scheller College of Business Research Paper, pages 7-8, 18 February 2022, and Defending Ukraine: Early Lessons from the Cyber War, Microsoft, 5, 22 June 2022, 5..

26 https://gaia-x.eu/what-is-gaia-x/about-gaia-x/.

of non-European cloud providers. Gaia-X's Vision & Strategy document notes that sovereignty is: "the ability to exercise self-determination. It can translate into several meanings—political, economic, digital, and technical. Gaia-X does not provide any political or economic interpretation of sovereignty, but instead provides a framework to configure sovereignty from a digital and technical perspective." To date, no significant progress has been made, and in the meantime, providers with non-European headquarters have been approved as members.[27]

- The European Union's Cloud Certification Scheme (EUCS),[28] which has been established under the EU Cybersecurity Act, is being negotiated by the European Security Agency, ENISA and the EU Member States. This voluntary certification is intended to offer varying levels of assurance (subject to ongoing negotiations)—to cloud providers. Generally, the EUCS is a welcome initiative for enhancing baseline cybersecurity practices of European cloud customers, as well as adding to legal clarity and certainty for both providers and customers.

  However, while the final outcome still remains uncertain, the EUCS also looked at introducing sovereignty requirements inspired by France's SecNumCloud,[29] potentially excluding non-European cloud companies from the ability to seek the highest security certification levels.[30]

  Despite the voluntary nature of the EU Cybersecurity Act's certification structure, certification could become mandatory for many European organisations under the revised Network and Information Security Directive (NIS2). The sovereignty requirement faced strong resistance from several EU Member States and organisations, who perceive it as a measure against cloud 'hyperscalers' with a potentially negative impact on competition. [31]

In practical terms, the 'sovereign cloud' is challenging to operationalise successfully for the private sector. Solutions to date have incurred high operating expenses and harm to data security, with few tangible benefits in return. Stephanie Combes, President of the French Health Data Hub, which requires a certain level of data security, discussed in an interview in 2023, "The assessment is that, for the moment, we do not have sovereign solutions that can handle the services that we look for."

4. Data localisation

Data localisation policies are one of the chief elements of digital sovereignty programs, although digital sovereignty can manifest in other ways (e.g., local sourcing requirements for manufacturing), and data localisation can be pursued for other purposes (e.g., efforts to foster local economic development).

Localisation laws, regulations and policies are typically grouped into the following three categories:[32]

1. requirements to store and manage data locally and prohibit international data transfers and/or impose nationality requirements for personnel accessing the data;
2. requirements to store data in the original jurisdiction but allow copies of the data to be transferred if certain requirements are met; and
3. de facto localisation requirements that impose restrictions and conditions on data transfers, which make it difficult

27 Clothilde Goujard and Laurens Cerulus, "Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project".

28 https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

29 SecNumCloud is a French National Cybersecurity Agency's revised cloud cybersecurity certification and labelling program. This program limits corporate ownership by specifying that non-EU shareholders cannot possess more than 39 percent of a company providing cloud services in France. Beyond SecNumCloud, a cloud provider must also have its servers physically in France.

30 ecNumCloud imposes strict foreign ownership (individual shareholders outside the EU cannot possess more than 25% of the company), data localisation (cloud providers must store and process all data, including technical data, in the EU territory; administration of the service must be carried out in the EU territory), and local staffing requirements (technical support can only be conducted by staff located in the EU). Key to the sovereignty requirements is the extent of control a European subsidiary of a cloud provider can exercise independently of its non-European parent company. The 'high+' assurance level initially required providers to be EU-based entities, free from non-European influence. However, discussions of appropriate solutions continue, and draft changes in 2023 allowed providers to demonstrate effective measures preventing decisive non-EU influence in decisions, particularly concerning investigation requests. ENISA considerations and discussions with Member States raised a concept of "trusted foreign cloud providers" under specific—currently not clarified—conditions, with indications that similar considerations might be applied to the 'high' assurance level. In addition, there are additional data localisation requirements, with the 'high' level requiring at least one EU-based location and 'high+' necessitating all locations within the EU.

31 In the context of this letter, the Dutch Secretary for the Interior and Kingdom Relations, Alexandra van Huffelen, stated: "We see the risks that the sovereignty requirements, which were included in the scheme, will create unfair competition between the EU member states. It can also result in a market access barrier, which could impact negatively on our strategic partnerships with countries like the U.S. and Japan."

32 CIPL-TLS, The "Real Life Harms" of Data Localization Policies, March 2023.

or impossible to transfer data outside the jurisdiction. Such conditions include the use of certain prescribed transfer mechanisms or a demonstrated absence of transfer risk and local data management requirements in mandatory certification regulations.

Localisation requirements may apply broadly to all personal data processed in-country or may be sector-specific and apply only to certain types of data, such as health or financial data.

Data localisation requirements and their impact

There are many potential drivers for data localisation, but key ones often cited by governments are data privacy and security concerns, especially with unfettered government access to data in the importing country and local economic development. As CIPL noted in its 2023 paper on *The 'Real Life Harms' of Data Localisation*, proponents of data localisation requirements believe they have key advantages, including enhanced national security, increased data security and the promotion of domestic industry and job protection through the stimulation of the local economy.

However, there is strong evidence to demonstrate that data localisation requirements harm a wide range of critical business functions and impede individuals' access to beneficial products, services and activities.[33] To cite a few examples from CIPL 2023 white paper:

- Requiring data storage on local servers hinders the ability of businesses and individuals to leverage the comprehensive advantages of global cloud computing technologies, as well as the scale and operational efficiencies they provide. Global Cloud Service Providers offer numerous benefits, such as cost efficiencies, resilience and superior cybersecurity protections. For instance, they are designed with the operational adaptability to circumvent disruptions like widespread power outages, unlike local services, which may lack the capability to reroute data to international backup servers.
- Lowering cloud customers' ability to compete in the global marketplace by limiting access to the global supply chain, which may provide more affordable and more effective solutions than those available locally, thereby raising the cost of services.
- Reducing competitiveness by walling off domestic businesses from potential customers outside of the home country's borders.
- Disadvantaging domestic industry by forcing organisations to rely on local storage providers that may have less advanced systems and tools, as affirmed in the French Health Data Hub example. Open cloud computing services facilitate seamless data exchange for geographically dispersed businesses through a shared infrastructure. They may also empower smaller enterprises through access to advanced data storage, processing and analytics tools that might otherwise be beyond their reach.
- As noted in the discussion on digital sovereignty above, maintaining data in a single region or nation can generally affect resilience, including in the context of geopolitical conflicts. This was evident in Ukraine just prior to Russia's invasion in February 2022. Ukrainian law initially mandated data localisation for specific government and private sector data. However, in anticipation of conflict escalation, the Ukrainian parliament enacted a law enabling the movement of this data to the cloud. Consequently, the Ukrainian government collaborated with private CSPs to transfer essential government, tax, banking, education and property data to the cloud. This strategic move ensured that Ukraine's critical data was not confined to local servers at risk of disruption or destruction, but instead was securely distributed globally by cloud service providers.[34]

Additionally, data localisation programs do not solve privacy concerns about law enforcement access to data. CIPL and TLS published a discussion paper in 2023 showing that legal systems, in general, provide avenues for governments to require

33 CIPL, The 'Real Life Harms' of Data Localisation, March 2023.

34 See Defending Ukraine: Early Lessons from the Cyber War, Microsoft, 5, 22 June 2022, 5.

companies to respond to data requests, even if data is localised in a different country, and that localisation will, therefore, be ineffective at insulating data from cross-border reach.[35]

5. Challenges related to the interpretation of GDPR controller and processor concepts

Aside from the political and policy developments discussed above, there should be further consideration of how the interpretation of certain GDPR concepts may create tensions and conflicts with the advancement of cloud technology and the reality of our digital society. The GDPR defines data processing roles, such as controller, processor and joint controller, and there is extensive regulatory guidance to help assign these roles to organisations and individuals. However, in the context of cloud computing, these roles are not always clear-cut, especially in complex digital environments where multiple parties wear different hats and may exert varying levels of control over data processing activities.

In cloud services, the differentiation of roles can become particularly complex. Cloud service providers typically act as "processors" with respect to the data that their customers put into the services, as they process that data on their behalf and only according to their customers' instructions. However, cloud service providers may assume the role of "controller" for certain specific processing activities they undertake on other data about how the services are used for specific limited purposes.[36] For example, that data will entail metadata of the processing activities (which is often more technical in nature, consisting of, e.g., logging and diagnostic information), as well as other data types (e.g., billing information, customer contact details, technical support interactions, etc.) that relate to a particular customer use of cloud services.

The processing of that additional data is integral to the operation, maintenance, security and reliability of cloud services. The nature of modern cloud service provision is such that a cloud service provider will also need to process this data for its own purposes: some self-evidently necessary, like billing for the services, and some that ensure valuable service evolution and maintenance that benefit customers (like being able to better understand, anticipate and eliminate service issues, or detect and respond to security incidents).

It is important to recognise that cloud providers occupy this controller role (for service data) and are responsible for compliance with GDPR in their role as controller. This is particularly important given the longstanding position that cloud service providers are only processors for all personal data processed through their services. As such, both cloud providers and their customers should continue assessing the roles and obligations of controllers and processors in a manner grounded in factual analysis. Also, importantly, data protection regulators should ensure that their understanding of cloud services reflects the necessary complexity and nuances of those systems and the actual roles of cloud customers and cloud service providers.[37]

6. Reactions from the Industry

Some global cloud providers have reacted to the increasing challenges of the EU data protection law restrictions, as well as data sovereignty and data localisation policies. For example:

- In 2022, Microsoft announced the rollout of the EU Data Boundary for the Microsoft Cloud, beginning in January 2023.[38] The EU Data Boundary solution is available to public sector and commercial customers in the EU and the European Free Trade Association. The EU Data Boundary allows customers to store and process their customer data within the geographically defined boundary,[39] greatly reducing data flows out of Europe and building on Microsoft's data residency solutions.[40]

35 TLS, Data Localization and Government Access to Data Stored Abroad, March 2023.

36 Ireland Data Protection Commission, Guidance for Organisations Engaging Cloud Service Providers, 2019: Cloud providers generally provide processing services to data controllers but may also provide sub-processing services to other providers. In some cases however, cloud providers are also data controllers, or 'joint controllers'.

37 See CIPL Paper "The GDPR's First Six Years: Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement", p. 16.

38 https://blogs.microsoft.com/eupolicy/2022/12/15/eu-data-boundary-cloud-rollout/

39 https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn

40 https://techcommunity.microsoft.com/t5/partner-updates-denmark-iceland/update-eu-data-boundary-for-the-microsoft-cloud/ba-p/3808127.

- Amazon Web Services (AWS) also offers customers the choice of data storage locations. Most recently, in October 2023, AWS announced that it is launching its European Sovereign Cloud.[41] According to AWS, it will be an "independent cloud for Europe that gives customers in highly regulated industries and the public sector further choice and flexibility to address evolving data residency and resilience requirements" in the EU.
- Google Cloud has also introduced data residency controls—Google Data Regions. These local data storage controls allow customers to choose where their data is located at rest. Google currently provides numerous locations in Europe and is expanding to include more European regions.[42]
- IBM has introduced enterprise cloud for regulated industries with sovereign cloud capabilities. Customers can choose the country or region where they want to host their data. For example, European customers can rely on the Multizone Region in Madrid, Spain, and Frankfurt, Germany.[43]

These examples do represent an important response to the demand from the market and provide an option for local data storage and processing, especially where there is an increased need or higher risk. However, no approach can result in "zero risk" of data access by foreign governments. Pushing too far in that direction has the potential to undermine the huge operational benefits of a global cloud and disadvantage the cybersecurity functions and developments in AI technology, which could result in opportunity costs for companies that will continue to use their own servers on-premise. The progress in the context of the G7 Data Free Flow with Trust initiative and the OECD Government Access to Personal Data Held by Private Sector Entities, as well as the EU-US DPF, should provide a sufficiently robust framework within which international data transfers and, with it, cloud computing can continue to thrive and continue to bring benefits to all.

All of the examples above illustrate somewhat patchwork interpretations and approaches to cloud computing that risk undermining the benefits of this technology to European businesses and public sector organisations. The research by the Leviathan Security Group shows that data localisation measures raise the cost of hosting data by 30 to 60%.[44] Finally, the lack of consistency in the approach of authorities and regulators creates legal uncertainty for both cloud service providers and their customers and could further hinder European competitiveness by creating a chilling effect with respect to the use of cloud computing technology.

41 https://press.aboutamazon.com/2023/10/amazon-web-services-to-launch-aws-european-sovereign-cloud.

42 https://workspace.google.com/blog/product-announcements/assured-controls-and-expanded-data-regions-for-google-workspace

43 https://www.ibm.com/blog/ibm-cloud-delivers-enterprise-sovereign-cloud-capabilities/

44 https://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization

IV. Response from the EU Data Protection Authorities

Decisions, investigations and guidance from the EU data protection authorities also have had a direct impact on cloud providers and their customers in the EU:

- In January 2023, the European Data Protection Board (EDPB) adopted its 2022 Coordinated Enforcement Action on "Use of cloud-based services by the public sector."[45] Throughout 2022, 22 supervisory authorities across the EEA launched coordinated investigations into the public sector's use of cloud-based services. Following the investigations, the EDPB adopted recommendations for public bodies wishing to use cloud-based products or services, including regarding compliance with international data transfer requirements. The EDPB asserts that, especially within the scope of certain Software as a Service (SaaS) implementations, identifying effective supplemental measures can be "impossible or extremely challenging" and could indicate potential non-compliance with the Schrems II ruling.[46] In its recommendations, the EDPB warns organisations to pay careful attention to third-country law enforcement requests for data, reminding organisations that such transfers are also subject to Chapter V[47] of the GDPR. Rather than providing pragmatic guidance for compliance, the EDPB suggests that the use of another cloud service provider may be necessary.[48]
- In November 2022, the German Data Protection Conference (DSK), a gathering of the 16 German Lander/state authorities, published a report on German organisations' use of Microsoft 365 services and whether agreements governing these uses complied with GDPR requirements. Following talks with Microsoft in September 2020, the DSK sought to achieve data protection-compliant improvements and contractual adjustments so that German organisations could carry out data transfers to third countries. The DSK report outlines concerns about transparency related to Microsoft's processing of data for business operations and fear of access to data by the US government. Whilst it did not specifically state that transfers of data to the US were unlawful, the conclusion that transferring data to the US creates doubts as to whether data should, in fact, be transferred.
- Authorities in France, Denmark, the Netherlands and two states of Germany (Baden-Württemberg and Hessen) have all published decisions either banning or expressing concern as to the use of cloud services in schools.

45 EDPB, 2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector, 17 January 2023.

46 d. at 17.

47 Transfers of personal data to third countries or international organisations, Chapter V, GDPR.

48 See supra note 47 at 31.

- The European Data Protection Supervisor (EDPS), in March 2024, adopted a decision on the European Commission's use of Microsoft 365 and ordered the Commission to show compliance by December 2024. The EDPS concluded that the Commission did not adequately document and control the purposes of processing activities and transfers related to the Commission's use of Microsoft 365; in particular, the decision focuses on and proposes a halt to any transfers to non-adequate countries outside of the EEA. In response to the Decision, the Commission and Microsoft separately filed appeals against the EDPS decision in front of the EU General Court. The Commission spokesperson noted that the EDPS interpretation: "unfortunately seems likely to undermine the current high level of mobile and integrated IT services. This applies not only to Microsoft but potentially also to other commercial IT services."[49]

At the same time, policymakers acknowledge and support the benefits of cloud computing. In August 2022, the Dutch government publicly acknowledged the advantages of the cloud, with State Secretary Van Huffelen writing in a letter to the House of Representatives that the "benefits [of the cloud] now outweigh the risks."[50] The lack of consistency in the approach of authorities and regulators creates legal uncertainty for cloud service providers and their customers.

49 Politico Pro Morning Tech, 12 March 2024, statement by European Commission's spokesperson Johannes Barhke.

50 https://www.rijksoverheid.nl/ministeries/ministerie-van-binnenlandse-zaken-en-koninkrijksrelaties/nieuws/2022/08/29/werken-in-de-cloud-wordt-mogelijk-voor-rijksoverheid

V. Finding Solutions to Legal and Policy Challenges

As demonstrated above, the legal landscape governing international data transfers continues to create legal uncertainty and may ultimately cause cloud service providers and customers to adopt an unnecessarily cautious stance that is not motivated by an assessment of actual risk to the data or individual rights but by enforcement actions. Cloud customers, faced with stringent and uncertain legal requirements, will inevitably adopt a conservative approach and consider localised solutions, which in turn may curtail the full potential of cloud technology as described above. This may undermine critical business requirements, like cybersecurity, fraud detection and data protection.[51]

Instead, a "risk-based" approach should be adopted by lawmakers and regulators that includes evidence-based risk assessments of the actual risks associated with data transfer, which must also consider, for example, the type of data being processed. This will allow for a more targeted approach to risk mitigation, for instance, through contractual agreements, imposing the implementation of data protection at the same level as at its origin and technical solutions such as encryption. [52] In the medium to long term, it may also hinder European competitiveness by increasing the cost of data processing and storage and decreasing access to data and functionalities required to train and develop AI solutions at a time when all countries' economic progress depends on the adoption of AI technologies.

Data protection regulators and policymakers must recognise the specific benefits of cloud computing for delivering effective data protection and information security on the ground. Also, they must be ready to evolve the interpretation of GDPR concepts, such as controller and processor, to be more fit with the reality of cloud computing, and in particular, recognise the additional role of cloud service providers as controllers in respect of specific personal data, such as "service data".

Beyond this, organisations may also demonstrate their commitment to adequate data protection by adhering to recognised international standards or certification schemes. These may include formal mechanisms recognised for data transfer in regions with specific data transfer restrictions. Moreover, global accountability-based mechanisms, such as those based on the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, or standalone mechanisms such as Global CBPR and Global PRP, certifications, codes of conduct and BCRs, should be promoted in the context of cloud computing. Such mechanisms emphasise that organisational measures and practices, rather than the location of data, are of primary importance in the laudable goal of protecting individual data privacy principles.

Summary of CIPL recommendations

1. **Understanding Data Localisation Impact Including on Privacy and Security:** EU Member States and DPAs need to deepen their understanding of the limitations of data localisation measures and adopt a balanced and pragmatic view. It is crucial for regulators and policymakers to recognise the potential of cloud computing for data protection and acknowledge that data localisation does not equate to better security or privacy. In our globally connected world, technical, legal and organisational safeguards should prioritise the protection of data itself, irrespective of geographic borders. With the emerging importance of trusted AI products, it is more essential than

51 Id.

52 See Theodore Christakis "The 'Zero Risk' Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach,".

ever for data protection to be viewed at the product security and privacy controls level rather than geographic boundaries.

2. **Risk-Based Approach to International Data Transfers:** Adopt a risk-based approach to assessing the risk in international data transfers that appropriately considers the likelihood and severity of risk, balancing the need for privacy protection with the necessity of global data flows in the digital society, including in cloud computing.
3. **Onward Transfers:** Recognise the importance of onward transfers to enable the global functioning of cloud services. Also, acknowledge that onward transfers, as in the case of EU-US DPF, are accompanied by accountability principles and requirements which ensure that personal data transferred from the EU continues to receive adequate protection.
4. **Recognise and Incentivise Accountability-Based Measures:** Promote accountability-based measures in cloud computing, ensuring that service providers can demonstrate their data management, privacy and security practices and safeguards as foreseen in the GDPR via tools such as certifications and approved Codes of Conduct. These should take into account already existing internationally recognised standards and certifications that do not impose data localisation requirements but promote the uptake of secure cloud computing in both the public and private sectors. These advanced certifications should address emerging challenges in cloud computing and focus on robust benchmarks for privacy and data security regardless of the location of the data.
5. **GDPR Concepts of Controller and Processor:** Recognise the evolving nature of GDPR concepts of controller and processor, with cloud service providers also acting as controllers for specific "service data" processing.
6. **Strengthened International Cooperation and Convergence Based on Free Data Flows with Trust:** Actively work towards convergence in international data flows based on free data flows with trust and agreements, enabling e-evidence access to data by law enforcement agencies. This includes supporting and building on frameworks like the Global Cross-Border Privacy Rules (CBPR), the Global Privacy Recognition for Processors (PRP), G7 Data Free Flow with Trust and OECD Principles on Government Access to Personal Data Held by Private Sector Entities. This approach would balance law enforcement access to data with stringent privacy protections, ensuring that cross-border data access respects individual rights and adheres to international norms. Cross-recognition of accountability frameworks, compliance certifications or binding codes of conduct can ensure higher levels of data protection by organisations and elevate the trust of individuals.

About the Centre for Information Policy Leadership

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at

http://www.informationpolicycentre.com/.

DC Office
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London Office
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels Office
Avenue des Arts 47-49
1000 Brussels
+32 2 643 58 00

© 2024 Centre for Information Policy Leadership. All Rights Reserved.