CS CYBERSHERPA
Security by Design

Artes Juris

Cloud security and sovereignty in the EU and Switzerland

Addressing geopolitical risks and evolving US regulatory approach

POINT OF VIEW

May 2025

www.cybersherpa.com wwww.artes-juris.ch

Introduction

Changing context and risks for Europe and Switzerland regarding data transfers to the United States (US)

Historically, international agreements like Privacy Shield (EU/US and Swiss/US) and its successor the Data Privacy Framework (EU/US and Swiss/US) have sought to balance transatlantic data transfers with robust data protection requirements.

However, recent shifts in US policy, including dismissals of certain members of the US Privacy and Civil Liberties Oversight Board, may jeopardise the Data Privacy Framework, and consequently put at risk transfers to the US of European and Swiss personal data.

> ***Recent shifts in US policy could introduce greater access by US authorities to EU and Swiss data, challenging compliance with GDPR and Swiss data protection laws***

With the acceleration of adoption of cloud services and in particular Microsoft M365 as well as a growing use of artificial intelligence, European and Swiss organisations are facing increasing compliance and legal risks. As a reaction to this evolving international context, they have to consider strengthening their sovereignty requirements.

This rapidly shifting regulatory landscape requires proactive measures to safeguard sensitive business and government information as well as personal data.

This paper considers the volatile cyber and regulatory environment and how organisations can ensure the sovereignty, security and continuity of their digital operations.

A challenging context

EU, Swiss organisations face new risks with US providers of Cloud Services

In this volatile context, European and Swiss organisations leveraging US cloud services (Microsoft 365, Salesforce, ServiceNow) or cloud platforms (Azure, AWS, GCP, OCI) should reassess their data sovereignty posture.

Uncertainty is growing about data agreements between the USA and Europe/ Switzerland

▶ **Challenge 1 : Impact on Regulatory Compliance**

A growing uncertainty over data transfers to the US will make compliance with EU/Swiss regulations more challenging:

- **Data Protection Laws**: Ensuring adherence to GDPR, Swiss Data Protection Act may trigger additional requirements, including performance of data transfer agreements, signing of standard contractual clauses with appropriate supplementary measures.
- **EU AI Act**: Diverging approaches towards AI regulations in the US and EU require even more scrutiny on the use of AI solutions.
- **Cyber-security related regulations**: Specific focus is needed on the scope and requirements laid down by the EU NIS 2 Directive, DORA Regulation and other sector specific cyber-security laws and guidelines such as the ones issued by the FINMA.

Uncertainty is also growing about how EU and Swiss authorities may react to potential changes in regulatory practices of the US authorities such as more access to personal and company data.

▶ **Challenge 2 : Increased cyber risks on cloud platforms**

- 2023: Microsoft 365 breach[1] by the threat actor Storm-0558, leading to multiple client breaches
- 2025: Oracle Cloud breach[2] by the threat actor Rose87168

With these and other examples of breaches, can organisations still assume a shared security responsibility with their cloud provider or should they take supplementary measures?

Recent breaches show that the risk of cloud platform compromise can no longer be ignored, even with major Cloud Service Providers.

What practical legal, technical and organisational steps should organisations take to continue using cloud services while addressing (1) their regulatory risks and (2) their cyber risks?

1. Microsoft breach 2023 : https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
2. Oracle breach 2025 : https://www.hipaajournal.com/oracle-health-data-breach/

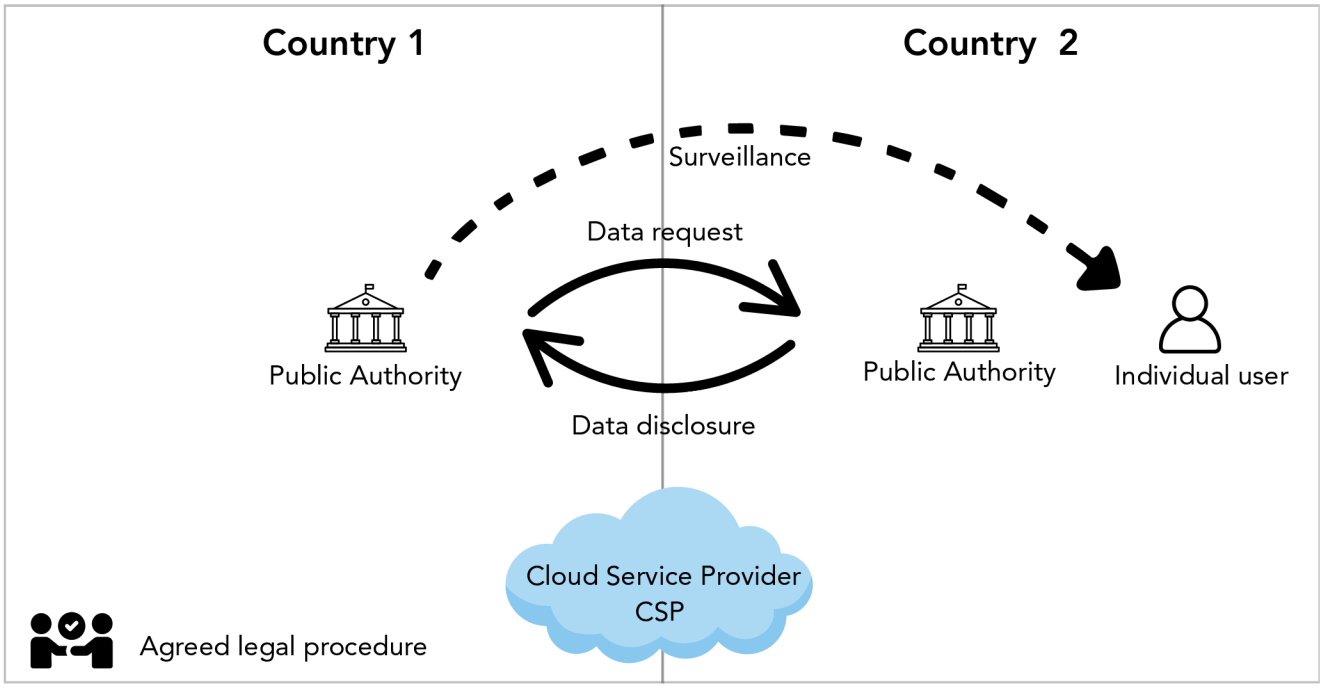
Data disclosure procedures

Understanding the principles

Law enforcement requires access to criminal evidence, which is frequently located abroad. For years, such access to e-evidence could be obtained through inter-States mechanisms defined in Mutual Legal Assistance Treaties (MLATs).
More recently, new Extraterritorial Data Access Laws have been enacted enabling public authorities to request such data directly to Cloud Services Providers (CSPs) established in their territories.

To understand the impact of such changes, let us first lay down the principles of Mutual Legal Assistance Treaties. We take an example where the Cloud Service Provider (CSP) is a company registered in Country 1 and operates in Country 2. We are considering the security and privacy impacts for an individual user located in Country 2.

Case 1 with Mutual Legal Assitance Treaty (MLAT)



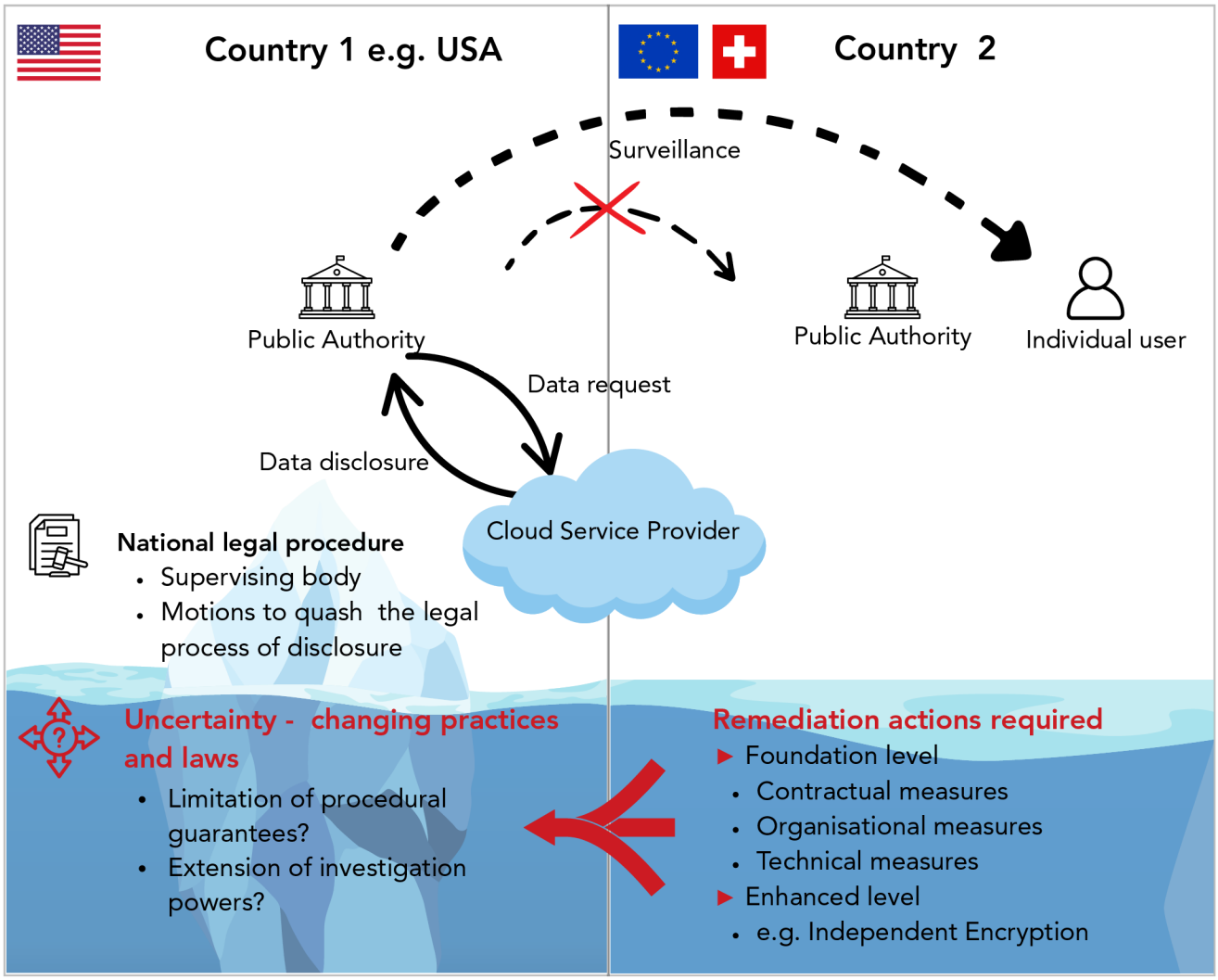
Mutual Legal Assistance Treaties usually ensure a satisfactory level of protection of fundamental rights, while enabling an international cooperation between public authorities. Such procedures are however quite time-consuming and can slow down criminal investigations.

When MLATs are in place, no additional remediations in relation to data disclosure procedures are required.
However, organisations still need to ensure appropriate contractual, organisational and technical measures are in place to mitigate security, privacy and compliance risks.

Data disclosure procedures

Understanding the impact of Extraterritorial Data Access Laws for EU and Swiss organisations

Case 2 *without* MLAT - Extraterritorial Data Access Laws (e.g. US Cloud Act, FISA)



To avoid the significant delays associated to international cooperation, public authorities in countries with Extraterritorial Data Access Laws can request data and e-evidence directly from CSPs established in their territories, irrespective of the actual location of the data.

Despite the conditions and safeguards associated to such data requests, these extraterritorial laws trigger new challenges and risks for privacy rights. GDPR and equivalent national laws require specific compliance actions from organisations using CSPs which can be subject to these data requests procedures.

Last year's decision[3] by the EDPS (European Data Protection Supervisor) on the investigation into the European Commission's use of Microsoft 365 is an example of such challenges. In Switzerland, the Kanton Zurich[4] also issued recommendations in june 2024 for the local authorities on that topic.

Further remediation actions are required to mitigate the risks associated to changing foreign extraterritorial data access laws: notably (1) a foundation of contractual, organisational and technical measures and (2) enhanced measures such as independent encryption.

3. EDPS investigation : https://www.edps.europa.eu/data-protection/our-work/publications/investigations/2024-03-08-edps-investigation-european-commissions-use-microsoft-365
4. Zurich Kanton M365 recommendation : https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_microsoft365_gemeinden.pdf

Foundational measures

Adapting to this changing environment requires an integrated legal and cyber approach

To respond to the shifting regulatory context, organisations often find challenging to ensure the traceability of their regulatory requirements into measures proportionate to their risks.

> ***Cloud services are often subject to protracted exchanges between legal and technical teams, "stuck" on a few controls considered in isolation from the full risk context.***

Organisations need to ensure they have a well integrated foundation of legal, organisational and technical measures.



Contractual and Organisational Measures:

- Update Contracts and Data Processing Agreements (DPAs) with Cloud Services Providers
- Implement Standard Contractual Clauses (SCCs) with supplementary safeguards
- Documented legal opinions under relevant local laws to ensure compliant data flows (US federal and/or state level laws or any other relevant country outside the EU)
- Governance structures and compliance processes as per applicable laws and documented legal opinions

Technical Measures (non exhaustive):

- Enforce data localisation within EU/Swiss data centers
- Encryption-at-rest and encryption-in-transit
- Decide whether to use BYOK (Bring Your Own Key) or Microsoft keys
- Implement strong Identity and access controls (Zero Trust model)
- Utilise advanced auditing and monitoring for data access. (e.g. M365 Customer Lockbox)

Within the technical measures, it is worth noting that BYOK can give the organisation control over key creation, rotation, and revocation, helping with auditability, compliance, and limiting unauthorised access. However, since the key is still stored and managed within the cloud provider's infrastructure, risks like insider threats, Extraterritorial Data Access Laws, or provider compromise remain.

> ***An integrated legal and cyber risk management enables organisations to deal with most of the cloud challenges. There are however, important residual risks which require appropriate actions.***

Three important residual risks to address:
1.a. Unauthorised access by the US cloud provider and/or US authorities
1.b. Service continuity if the cloud service no longer meets EU/Swiss regulations
2. Risk of compromise at the cloud platform service provider

Enhanced measures

Independent encryption - Example with Microsoft 365 Double Key Encryption (DKE)

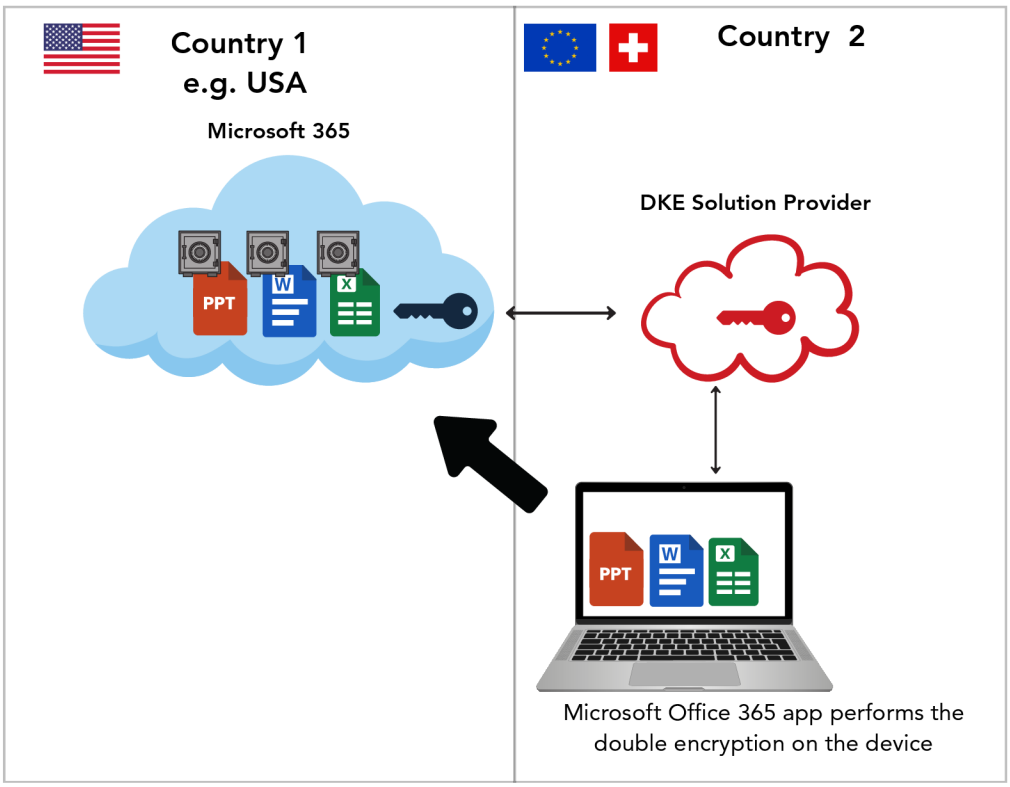
With the rapidly changing landscape, EU / Swiss organisations need innovative ways to protect their data and ensure their regulatory compliance.

Double Key Encryption (DKE)

DKE is an advanced security feature in Microsoft 365, which integrates with a range of DKE solution providers that ensures data protection through two separate encryption keys:

1. **One key** is managed by Microsoft.
2. **A second key** controlled exclusively by the customer via an external "DKE solution".

The cloud provider cannot access the encrypted data without the customer's key.



Transparent for the user

From an end user experience, the Double Key Encryption is transparent. When a user selects a M365 label, the integration between M365 and the DKE solution ensures the file encryption with two different keys with no additional action from the user.

Multi cloud solutions

This type of independent encryption also exists on AWS, leveraging the External Key Store (XKS) module. Similar solutions are also available to encrypt data in other SaaS applications such as Salesforce or ServiceNow.

Independent encryption solutions such as Double Key Encryption (DKE) are an opportunity to address the security and data sovereignty risks on cloud services.

Enhanced measures

Options for DKE solutions and innovation with Multi Party Computation

Options for DKE solutions

DKE services can be implemented in three different ways;

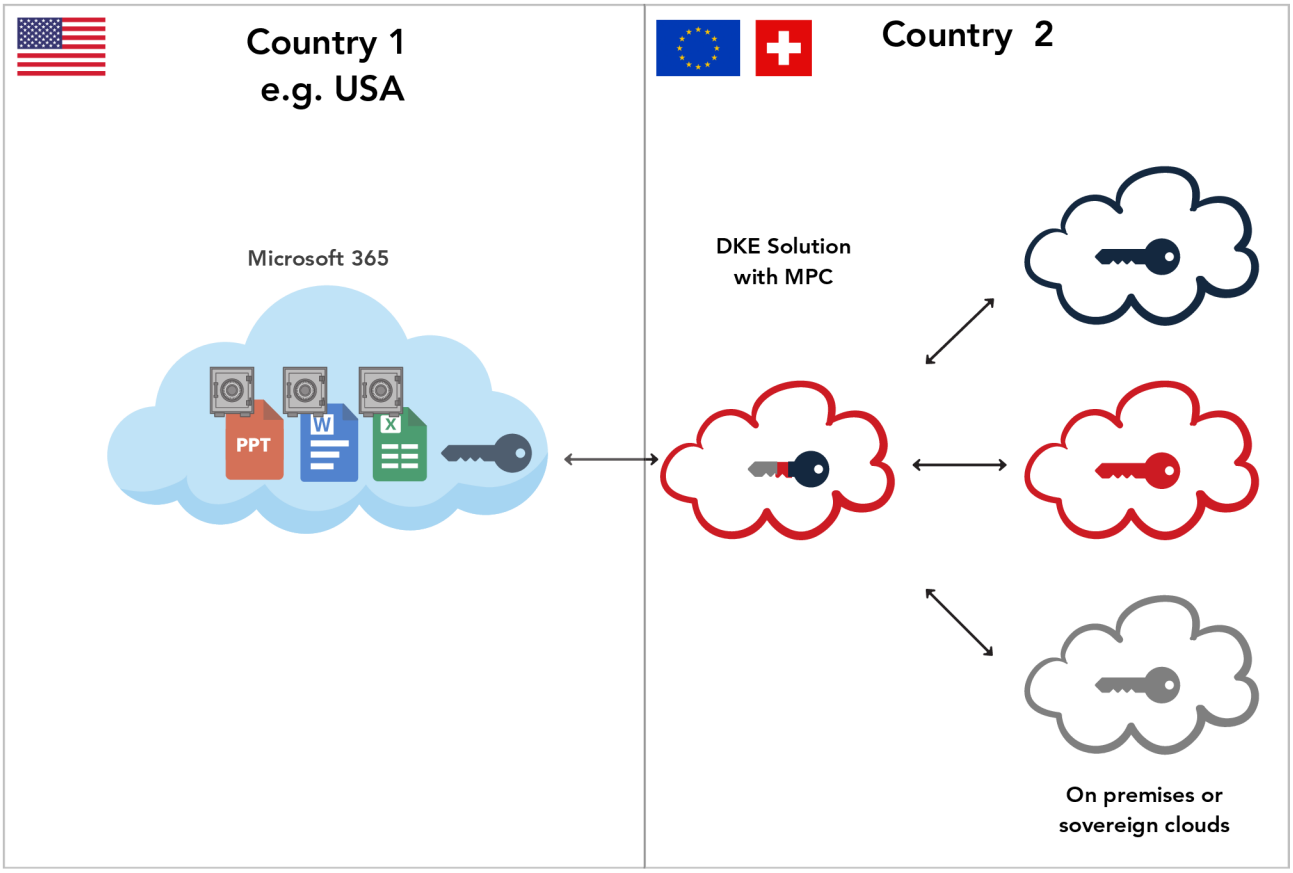
1- On-Premises or Cloud based Key Management: The 2nd key is hosted on an organisation infrastructure (Hardware HSM) or another cloud service (Cloud HSM).

2- Third party Key Management Services: Engaging a trusted European provider to host and manage the second key (Managed HSM).

3- Using a MPC (Multi Party Computation) service
See below.

Innovation with MPC (Multi Party Computation)

This type of solution can enable the same level of trust (ex FIPS 140-3) as an HSM. This way of securing encryption keys present an economic advantage and also simplifies operations.
This innovation will ease the adoption of DKE.

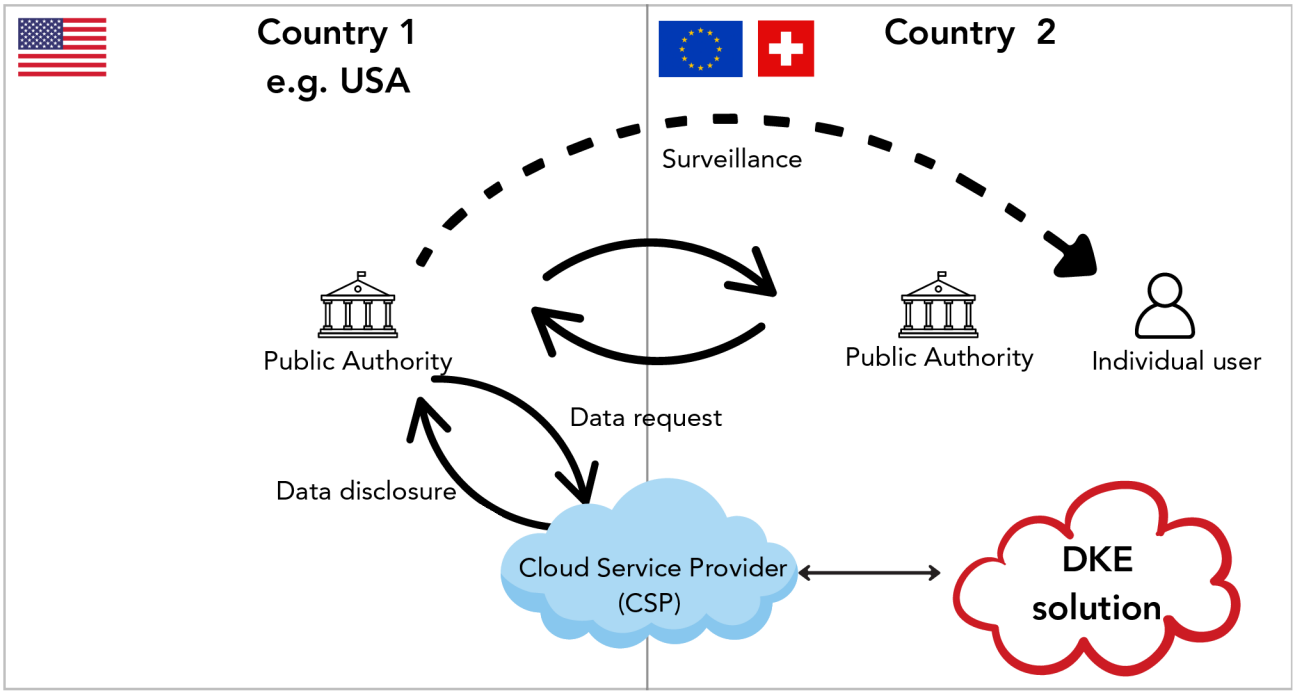


DKE solutions enabled with Multi Party Computation (MPC) presents an opportunity to address the security and data sovereignty risks of cloud services.

DKE and Extraterritorial Data Access Laws

How efficient are DKE solutions to mitigate the risk of Extraterritorial Data Access Laws?

Case 2 updated - Extraterritorial Data Access Laws (e.g. US Cloud Ac, FISA) and Double Key Encryption



The GDPR and equivalent national laws usually consider technical measures as relatively efficient risk mitigation actions. Among them, encryption is perceived by privacy regulators as a very protective mechanism, provided that the Cloud Service Provider (CSP) does not control the encryption keys. In this context, the CSP does not have "possession, custody, or control" over the data, which may block the application of certain extraterritorial data access laws such as the US CLOUD Act.

Double Key Encryption is therefore a change of paradigm in cloud security because it can prevent the CSP from getting access to data. Therefore, the same would apply to the foreign public authorities who could request such data from the CSP.

It is however to be noted that both foreign laws and public authorities' practices can change and one may imagine a future, possibly in a short-term horizon, where CSPs would prohibit the use of Double key encryption solutions.

It is therefore critical, as a minimum effort, to combine Double key encryption solutions with an appropriate contractual review and negotiation with cloud service providers and a strategic thinking around a potential shift towards alternative sovereign cloud solutions.

Double Key Encryption services associated with relevant contractual and organisational measures enable today a very satisfactory level of data protection as per EU and Swiss regulations while using foreign CSPs. Some organisations may also use this set up as a temporary solution while anticipating in parallel the deployment of alternative sovereign cloud services.

Conclusion

EU and Swiss organisations must be ready for change - legal and cyber foundations in place and a plan to enhance data sovereignty with controls such as independent encryption.

As US policy changes potentially impact data sovereignty, European and Swiss organisations must plan ahead, review their regulatory posture and proactively secure their cloud environments.

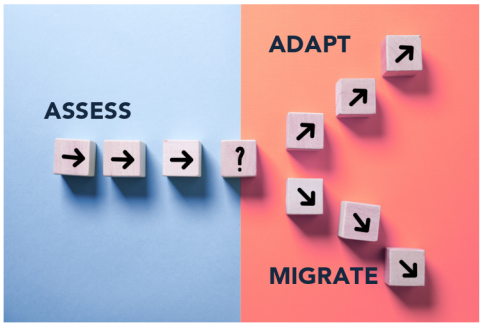
In the short to medium term

Organisations using US cloud services must ensure they have established the foundation of legal and cybersecurity controls according to their sector and specific requirements.

Extra measures to ensure sovereignty are now recommended to protect their sensitive data and pre-empt changes in the regulatory environment.

An example of such measure is the the adoption of Double Key Encryption (DKE) with M365, which is also an appropriate measure to prevent sensitive data breach in case of ~~the~~ cloud platform compromise.

> ***Cloud services, such as Microsoft M365 are now so embedded in most organisations that substituting for a EU/Swiss data service is very challenging on a short or mid-term horizon.***



In the long term

European and Swiss organisations should actively monitor the regulatory landscape and start to assess sovereign cloud alternatives for their specific needs.

They will need to approach data sovereignty from an holistic perspective, taking into account data protection but also operational and technological aspects.

Considering how cloud services are deeply embedded, organisations will need to map their use cases to alternative sovereign solutions. These solutions can be considered initially as continuity planning in case of rapid regulatory change until a strategic decision is required.

In the short and medium term, independent encryption solutions offer a clear opportunity to manage data risks and data sovereignty.
However, managing risks associated with operational and technological sovereignty require a more profound analysis of available local cloud solutions and of each organisation specific use cases.

Artes Juris CS

Get ready for cloud regulations changes
An integrated cyber and legal approach

Short term
Enhance data sovereignty on your existing US cloud services

1 Know your cloud posture
- Perform cyber technical posture review
- Review of existing cloud contracts and related agreements, including Data Processing Agreements (DPA)
- Identify Legal and cyber risks

2 Adapt your control requirements
- Update governance frameworks
- Update transfer impact assessments and compliance actions required by applicable laws
- Update technical controls such as encryption, data residency controls

4 Implement and monitor
- Apply changes : Policy, Process, People, Technology
- Test and validate: cyber and legal aspects
- Establish continuous monitoring

3 Design controls
- Change to legal and privacy documents (Standard Contractual Clauses, DPAs, etc.)
- Design cyber controls such as DKE
- Develop implementation plan
- Advise on regulatory communication

Mid and Long term
Consider sovereign cloud alternatives

Analyse use cases → **Discover available sovereign solutions** → **Perform Proof of Concept**

Our accelerators

- Data sovereignty discovery
- Cloud security posture assessments
- Blueprints for cloud security enhancements
- Managed cloud security assurance services
- Notification on Cloud and AI legal changes
- Predefined legal packages with pragmatic outcomes
- International network of trusted law firms (US, Canada, China, etc.)
- Managed legal services (contract drafting, regulatory analysis, criminal law procedures)

About the Authors

CS CYBERSHERPA Security by Design

ARTES JURIS

Jean-Loup Ravinet

Cybersecurity and Risk Leader, expertise in Cloud and Network security transformations

Matthias Traussnig

Swiss Attorney at Law, CAS Digital Finance Law specialising in business law and emerging technology law

Omar Guemmi

Cloud Security and AI Specialist, Microsoft Cybersecurity Architect Expert ISO27001 Lead Implementer

Aurélien Rocher

Associate Professor, University Lumière Lyon 2, with solid expertise in digital and company law both in Switzerland and in the EU

Book your appointment - Stay ahead of cloud regulatory changes

Artes Juris

Etude d'avocats à Genève

Rue de Candolle 34

1205 Genève

www.artes-juris.ch

info@artesjuris.com

CS CYBERSHERPA Security by Design

Rue de Genéve, 100

1004 Lausanne

contact@cybersherpa.ch

Important notice

This document reflects a general point of view provided for informational purposes only and intended to stimulate reflection. It shall not, under any circumstances, be considered as legal advice nor create an attorney-client relationship. The firms and authors disclaim any liability for decisions made based on this information without appropriate legal consultation. These comments reflect a perspective based on Swiss, French, and/or European Union law as of the date indicated.