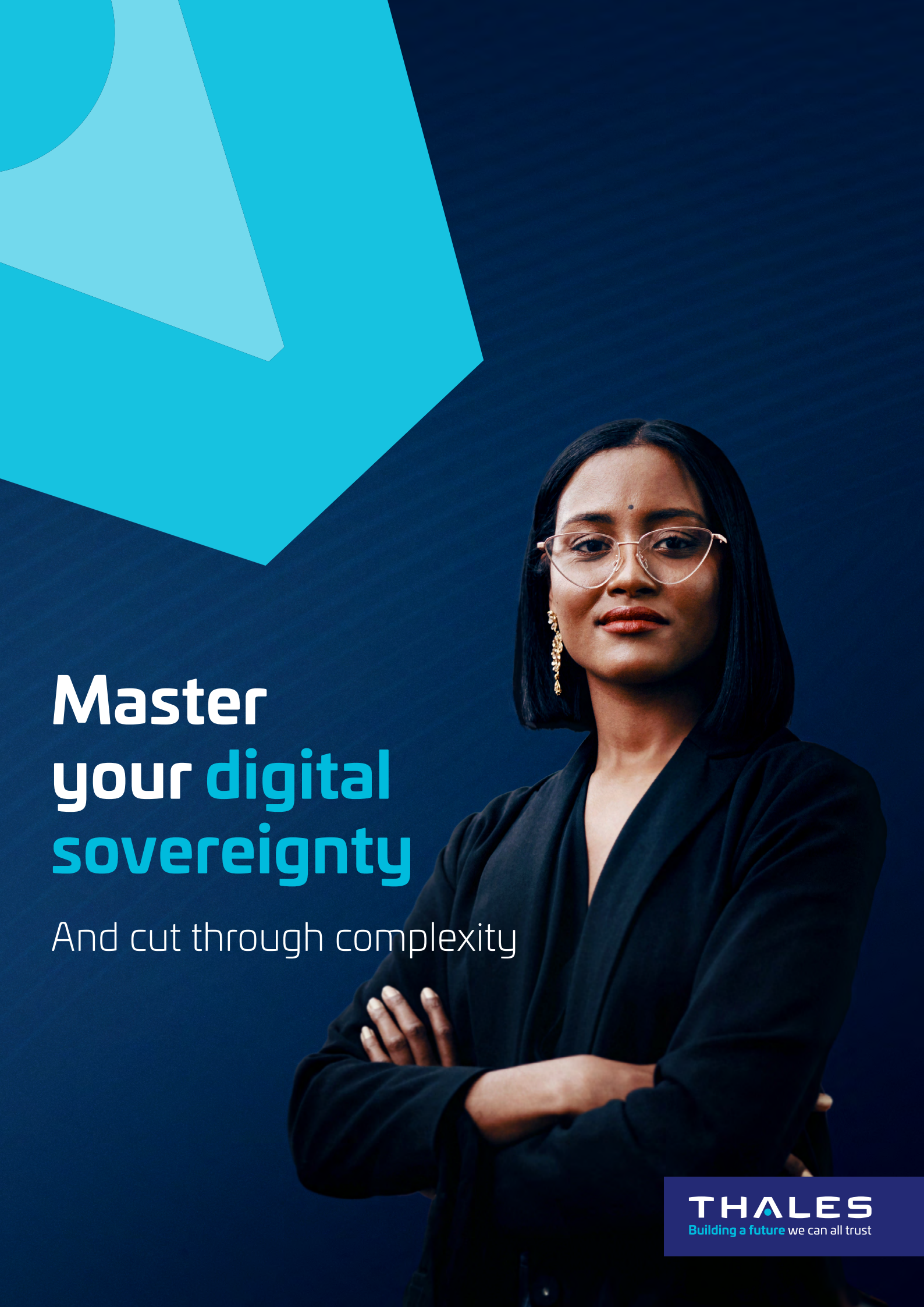
Master
your digital
sovereignty
And cut through complexity
THALES
Building a future we can all trust

# What is **digital sovereignty?**

Data residency. Data localization. Data sovereignty.

All different aspects of the same challenge: **Digital Sovereignty.**

In broad terms, digital sovereignty is having control over all your data (business', employees', customers'), so that you can protect them effectively and can be certain to comply with relevant national and regional laws. The simplest way to understand if digital sovereignty should be a concern to you, is to answer a simple question:

**Do you know where all your data is?**

If your answer is "in the cloud/hybrid IT" then your digital sovereignty could be at risk.

It has caught many organizations out. But Thales can help.

# Why digital sovereignty matters

## The weakest link in your cybersecurity. Are you aware?

**Organizations should be aiming for 100% digital sovereignty: knowing what data you hold, where it's stored, who can access it, and that it complies with all relevant legislation.**

Typically, though, organizations become aware of their digital sovereignty position in one of three ways: audits, freedom of information requests, or cyberattacks. In all these cases it can be an unpleasant surprise: noncompliance means having to pay a substantial fine, incurring much more damaging reputational harm, or even imprisonment in some European countries such as Denmark.

### Example fines

- EU GDPR could fine up to **€20 million or up to 4% of total global turnover**, whichever is higher.
- Meta, the parent company of Facebook, was fined **$1.2 Billion Euros** in May 2023 for transferring data collected from Facebook users in Europe to the United States[1].
- Equifax was fined **$700 million** by the US Federal Trade Commission in 2019 for failing to take adequate measures to protect the personal information of approximately 147 million people.

As individuals, we create much more data than ever before, and we effectively give the businesses and services we interact with license to use it. We need to know we can trust them with it..

Organizations from both private and public sectors are also going through their digital transformation and leverage third party cloud services to generate, store, process and transmit more data than ever before.

Nation states have reacted by adapting their compliance frameworks to better regulate the way citizens, consumers, business data, as well as the resilience of critical services are protected.

This is why digital sovereignty has become essential to all organizations: public services, B2C and B2B.

[1] Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules, The New York Times, 2023

# Where does digital sovereignty apply?

## Complex global requirements. Solved by Thales.

Digital sovereignty adds layers of complexity for global companies.

Across the world, 71% of countries have already passed data protection legislation, and a further 9% are drafting it. And in each country or region, the regulations around data are different, and often in conflict.

For example, 92% of the western world's data is stored in the US[2]. But the EU has different requirements around data. And many data regulations are under constant review.

[2] Waving the flag of digital sovereignty, Atlantic Council, 2019

### Example data legislation

**EU**

- EU legislations now include responsibilities and obligations for organizations when using third party IT services, such as cloud services.
- GDPR forbids the transfer of personal data to international organizations if not protected by lawful instruments such as specific technical and organizational measures.
- DORA and NIS2 are new compliance frameworks that mandate organizations to cover risks related to 3rd party ICT suppliers.

**US**

- The US EO14028 on "improving the nation's cybersecurity" mandates the use of encryption of data following attacks on US critical infrastructure.

# Where do you turn for help?

## Cloud providers are not responsible for the security in the cloud, i.e. for your data.

It is in the cloud where digital sovereignty can create a nightmare scenario for your data policies. **83% of organizations globally** are concerned that sovereignty or privacy regulations will affect their organization's cloud deployment plans[3].

That emanates from the fact that most organizations – enterprises and public sector included – are multi-cloud, with 80% of organizations[3] reporting having two or more cloud infrastructure providers, not counting platform or software-as-a-service solutions.

That means there's no holistic or overarching visibility over where data resides, and no alignment on responsibilities across all of the clouds.

The end result is that sensitive regulated data is at risk. This leaves your organizations exposed and vulnerable to breaches and penalties which could impact and disrupt your business.

[3] 2023 Thales Data Threat Report, produced by S&P Global Market intelligence

# How Thales can help you?

## Automate and simplify sovereignty and privacy compliance.

Our digital sovereignty solutions give you complete control and confidence to manage your business data, and empowers you to implement the right decisions and actions to protect yourself, no matter what cloud you use or where you operate.

We bring the relevant knowledge, tools and expertise to help you automate and simplify the complexity of meeting sovereignty requirements and control all elements of sovereignty – data, technical and operational – from a single pane of glass.

Our platform gives you the ability to decide what needs to be protected, and manage compliance across multiple environments, jurisdictions and regulations including GDPR, DORA, NIS2 and specific sovereignty requirements in different countries.

With Thales, you keep complete control over encryption and access to your data, remove dependence on your cloud providers' software and have complete visibility and control over provider operations.

**Build confidence through compliance.**
**Master your digital sovereignty with Thales.**

**Our breadth of capabilities covers:**

**Data Security solutions:**

- Discovering, assessing risk, classifying and protecting sensitive data based on specific regulatory requirements.
- Protecting sensitive data throughout its life cycle whether at rest, in motion or in use.
- Enforcing centrally defined control policies globally, while allowing for local control when required.
- Controlling encryption keys for all repositories and enforcing separation of duties with cloud providers.

**Identity & Access Management solutions:**

- Applying role-based access control for all access requests to sensitive data.
- Enhancing user privacy by reinforcing storage and proficient management of identity data.
- Standardizing secure identity verification options with robust authentication technologies.

THALES

Building a future we can all trust

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

**Decisive technology for decisive moments.**

Contact us – For all office locations and contact information, please visit
**cpl.thalesgroup.com/contact-us**