MEMO

June 2026

The protection of sensitive non-personal data: a competitiveness issue for European organisations

Cigref
SUCCEED WITH DIGITAL

Cigref Memo

The protection of sensitive non-personal data

A competitiveness issue for European organisations

June 2026

EDITORIAL

Major economic transformations have always been based on the control of a strategic resource. In the past, these were energy, raw materials or industrial infrastructure. Today, data has become one of the main resources for creating value. It underpins business processes, feeds artificial intelligence models, accelerates innovation and now determines an increasing proportion of organisations' competitiveness. This development opens up considerable opportunities. It also reveals new vulnerabilities.

As businesses and public authorities rely on globalised digital infrastructures, the protection of their most sensitive data is no longer solely a matter of cybersecurity. It is becoming a question of governance, law, strategic autonomy and, more broadly, industrial policy. Non-personal data, which often embodies organisations' know-how, innovation capabilities or competitive advantages, remains insufficiently addressed by current legal frameworks. Cigref has sought to tackle this issue pragmatically.

The protection of sensitive data can no longer be viewed as a purely technical matter. Encryption mechanisms, security architectures and certifications are essential building blocks, but they are not sufficient to address the challenges posed by extraterritorial legislation, the global concentration of digital infrastructure or new forms of economic rivalry. The issue is now as much a legal, economic and geopolitical one as it is a technological one.

Europe now has a historic opportunity to build a coherent framework. Developments surrounding the Data Act, the Cybersecurity Act and future European certification schemes offer an opportunity to strengthen trust without stifling innovation. However, this ambition must be underpinned by a detailed understanding of the operational realities faced by organisations. This is precisely the purpose of this briefing note.

It does not claim to provide definitive answers. It sets out the current situation, highlights the limitations of existing mechanisms and makes recommendations based on users' experience. Its aim is to contribute to the public debate and to inform the choices that will need to be made in the coming years, both by Cigref members and by European legislators.

The protection of sensitive non-personal data extends far beyond the digital sphere alone. It is integral to Europe's ability to preserve its freedom of action, protect its industrial and scientific heritage, and create the conditions for growth based on innovation rather than dependence. Cigref hopes that this contribution will support this collective ambition.

Henri d'AGRAIN,
General Delegate of Cigref

ACKNOWLEDGEMENTS

Our thanks go to Vincent NIEBEL, Group Director of Information Systems at EDF, and Laurent TRELUYER, Deputy Managing Director in charge of Information Systems at the CNAF, who led this working group in 2023–2024, as well as to all those who took part and contributed (in alphabetical order):

Daniel ACHHAB – SOCIAL AFFAIRS MINISTRIES

Chantal ALARIO – ENGIE

Cédric ALEGRE – PIERRE FABRE

Patrick ARMUSIEAUX – MSA

Laurent AVET – BNP PARIBAS

Xavier BACHIMONT – GRDF

Véronique BARDET – PIERRE FABRE

Bruno BATISSE – MICHELIN

Pascal BEAUJOUAN – KLESIA

Aurélie BERGE – BPCE GROUP

Jade BERNARDIE – MINISTRY OF THE ARMED FORCES

Nathalie BERTIN DE ALBUQUERQUE – EDF

Yves BILLON – MINISTRY OF THE ECONOMY, FINANCE AND INDUSTRIAL AND DIGITAL SOVEREIGNTY

Elsa BINET – COVÉA

Philippe BORONAT – AIR FRANCE-KLM

Bertrand BOTREL – PIERRE FABRE

Sébastien BUECHER – MINISTRY OF THE ARMED FORCES

Ségolène CAILLIEZ-BARON – EDF

Michel CAPEL – FAYAT

Florence CARIN – PIERRE FABRE

Sylvain CARON – UNIBAIL-RODAMCO-WESTFIELD

Adrian CARRETERO - MSA

Alfonso CASADO – SAINT-GOBAIN

Nicolas CAUDRON – BANQUE DE FRANCE

Jean-Fabien CHALANÇON - AG2R LA MONDIALE

Sylvain CHAUVIERE – AIR LIQUIDE

Gabriel CHENEVOY – SNCF

Claudio CIMELLI – MINISTRY OF NATIONAL EDUCATION, HIGHER EDUCATION AND RESEARCH

Philippe CLERICE – MINISTRY OF THE INTERIOR

Laure DASSONVILLE – MINISTRY OF ECOLOGICAL TRANSITION, ENERGY, CLIMATE AND RISK PREVENTION

Bruno DELCROIX – BNP PARIBAS

Laurent DELISLE – THALES

JULIEN DESMETTRE – VEOLIA

Laurent DEVAUX – SERVIER

Nathalie DIONNET – CAISSE DES DÉPÔTS

Olivier DJOMBY – ESSILORLUXOTTICA

Laurent DUCOURAU - FAYAT

Philippe EBERT – DASSAULT AVIATION

Karim EMBAREK – IDEMIA

Apollonie EPIN – CIGREF

Damien ERNST – EURO INFORMATION / CRÉDIT MUTUEL

Marie-Anne FERRÉ – MSA

Hugues FOSSEY – SODEXO

Jean-Baptiste FOUAD – SFR

Tsiporah FRIED – MINISTRY OF THE ARMED FORCES

Gwendoline GANGLOFF – CAISSE DES DÉPÔTS

Emmanuel GARNIER – ORANO

Ludivine GAUTHIER – COVÉA

Jeremy GIBBONS – AIR LIQUIDE

Stéphane GIRARD – TDF

Emma GOLDITÉ – SAINT-GOBAIN

Baptiste GRIGY – THALES

Valérie HACHETTE – SAFRAN

Luc HAEFFLINGER – ENEDIS

Fanny HAMON – MINISTRY OF THE INTERIOR

Badr-Eddine HEDDADJI – FRANCE TRAVAIL

Elisabeth HUMBERT-BOTTIN – GIP MDS

Jean HUOT – VINCI

Elyes IGHILAZA – BNP PARIBAS

Hanane JABRANE – ENEDIS

Stéphane JACQUOT – SOCOTEC

Sonia JDAINI – CAISSE DES DÉPÔTS

Christophe JOUAULT – ENEDIS

Carole JOURNEL – ADP GROUP

Ibtissam KAABOUCH – ENGIE

Agathe LADAVIÈRE – CIGREF

Stéphane LAPALUT – AIR FRANCE-KLM

Frédéric LAU – CIGREF

Antoine LE DEVENTEC – TERRENA

Laurent LE SAOUT – ENEDIS

Thomas LEFAURE – MICHELIN

Jérôme LÉGER – CRÉDIT AGRICOLE SA

Yoann LEGER – FRANCE TRAVAIL

Donovan LEVERT – SUEZ

Ambre LUONG – SERVIER

Patrick MAHU – FRANCE TRAVAIL

Romain MELET – AIR FRANCE-KLM

Patrick MÉNEZ – AXA

Pascal MERCHEZ – BPCE GROUP

Emmanuel MERCIER – MSA

Gino MEUL – AVRIL GROUP

Jean MIGUET – SODEXO

Chloé MINET – LVMH

Karl MINVIELLE – RATP

Xavier MOQUIN – FAYAT

Gauthier MULLER – HAGER GROUP

Philippe NETZER-JOLY – ARKEMA

Vincent NIEBEL – EDF

Frédéric NOVELLO – SNCF

Julie OLIVIER – EDF

Chiraz OUELHAZI – CAISSE DES DÉPÔTS

Marie-Christine PARENT – MINISTRY OF THE ECONOMY, FINANCE AND INDUSTRIAL AND DIGITAL SOVEREIGNTY

Laetitia PAYSAN-TEBOUL - ORANGE

Franck PERILLIER – EMERIA

Olivier PERNAUDET – MINISTRY OF THE ARMED FORCES

Nicolas PERRIN – BANQUE DE FRANCE

Vincent PERTUY – EDF

Eric PINAULT – OPMOBILITY

Valentine POYLO – SNCF

Josué PRISER – EDF

Ghislaine RAHAL – DASSAULT AVIATION

Camille RAPOPORT – MICHELIN

François RAYNAUD – EDF

Jean-Christophe RENDER – ORANGE

Manuel ROCHA – ENEDIS

Camille SAGE – COVÉA

Katty SAINT-GELAIS – MICHELIN

Eric SANCHEZ – BPI FRANCE

Emmanuel SARDET – CRÉDIT AGRICOLE SA

Olivier SAVORNIN – COHESITY

Nicolas SCHMITT – BNP PARIBAS

Sébastien SCHNEIDER – BPI FRANCE

Selim SOUAID – FRANCE TRAVAIL

Laurent THOMAS – BANQUE DE FRANCE

Fabrice THORINIUS – COVÉA

Nadine TIGRETT – VEOLIA

Laurent TRELUYER – CNAF

Eric VAUTIER – ADP GROUP

Martine VELASCO – BANK OF FRANCE

Pierre-Sébastien VERDIER – ENEDIS

Jennifer VERGER – ALLIANZ

Céline VERGNES – ACCOR

Laurent VERHOEST – TRANSDEV GROUP

Florent VERRIERE – EDF

Mathieu VIRELY – MICHELIN

Arnaud WOELFFEL – AIRBUS

Isabelle ZABLIT-SCHMITZ – MINISTRY OF SOCIAL AFFAIRS

Lilia ZOUAGHI – EDF

Jean-Jacques ZWALD – CRÉDIT AGRICOLE SA

We would also like to extend our warmest thanks to all those who contributed to our working group's discussions:

- Loane BEDOUET, Policy Officer, Directorate-General for Enterprise (DGE)
- Natacha CLARAC, Director, ATHENORA
- Olivier HUBAC, Project Director, Strategic Information and Economic Security Department, Directorate-General for Enterprise
- Jean-Claude LAROCHE, Policy Officer to the Chair of ENEDIS
- Nicolas MARGUET, Adviser to the Deputy Director for Expertise, ANSSI
- Juliette PERON, Adviser to the Director-General, ANSSI

This document was compiled and drafted by Aymeric BOURDIN, Head of Mission at Cigref.

EXECUTIVE SUMMARY

The data paradox: between value driver and systemic vulnerability

In today's digital economy, data has established itself as a critical and indispensable intangible asset. It is the essential fuel that powers artificial intelligence, guides executives' decision-making and shapes industrial value chains.

However, this central role exposes organisations to a major strategic paradox: they must circulate this data to create value, whilst operating in an environment of complex threats where economic intelligence and information gathering have become systemic risks. Faced with increased reliance on cloud infrastructures often located outside our borders, European companies' most valuable assets find themselves exposed to risks of exploitation by criminal or state actors.

It is to address this challenge that Cigref launched, in 2023, a collective intelligence initiative involving numerous senior executives and sector experts. The aim of this initiative is to go beyond mere technical analysis to offer in-depth strategic reflection and a common framework for major public and private organisations.

The limitations of current approaches: the legal and technical blind spot

One of the key findings of our work is the identification of a legal 'blind spot' concerning non-personal data. Whilst the European regulatory framework has been heavily structured around personal data and privacy, companies' industrial and strategic data remain subject to regulatory uncertainty that undermines their competitiveness.

The report demonstrates that traditional safeguards are now proving insufficient in a globalised environment:

- **The failure of traditional legal safeguards:** contractual clauses, trade secrets and intellectual property rights are necessary but ineffective in the face of non-European laws with extraterritorial reach (such as Section 702 of the US FISA Act). These criminal and intelligence laws are forcibly imposed on third-party hosting providers, taking precedence over private law agreements.
- **The inherent vulnerability of 'in-process' encryption:** from a technical perspective, whilst encryption effectively protects data at rest and in transit, data currently in use must necessarily be decrypted into plain text in the processor's random access memory in order to be processed. It is at this precise moment that a structural vulnerability arises when dealing with a cloud operator subject to foreign laws.
- **The limits of technological promises:** homomorphic encryption is still not commercially mature, whilst confidential computing merely shifts trust towards chip manufacturers and proprietary architectures that cannot be properly audited.

The rule of law and the ambition for a European regulatory framework

This observation leads to an uncomfortable but fundamental conclusion: to date, there is no genuine, purely technical shield. Ultimate data security does not lie in the strength of cryptographic protection, but in the legal status of the operator controlling the infrastructure. The only guarantee of true immunity is therefore of a legal nature, resting on the choice of providers subject exclusively to European law.

Although France has charted a pioneering course through the SecNumCloud certification and the 'Cloud at the Centre' doctrine, the strictly domestic nature of these measures creates complex regulatory fragmentation for multinational companies. The challenge now is to extend this momentum to a continental scale. The entry into force of the European Data Act in September 2025, combined with the ongoing negotiations on the revision of the Cybersecurity Act (CSA 2) and the Cloud and AI Development Act (CADA) in 2026, represents a historic opportunity to consolidate the protection of our information assets.

Cigref's vision: balancing security and economic performance

In the face of these geopolitical challenges, Cigref is not calling for excessive regulation, but rather for an approach based on incentives, stakeholder accountability and respect for business realities. Our proposals are structured upon four pillars:

1. **A flexible definition of sensitive data:** Allowing organisations the freedom to define their own scope of sensitivity under their own responsibility, based on a detailed analysis of their business risk.
2. **A matrix-based approach to certification:** Seamlessly reconciling the technical protection levels of CSA 2 with the legal safeguards against extraterritoriality provided by the CADA within the future EUCS framework.
3. **Economic support for demand:** Redirect public funding and introduce tax incentives (tax credits, accelerated depreciation) to help corporate clients absorb the additional costs of trust-based services (estimated at between 15% and 20% compared with hyperscalers).
4. **Realistic transition pathways:** Introduce phased timetables of 3 to 5 years (and up to 10 years for the most critical assets), aligned with contract renewals, so as not to compromise the technological capabilities of European organisations.

By publishing this briefing and news update, Cigref positions itself as a proactive force advocating for balanced regulation, making data security not only a factor in building trust, but also a cornerstone of Europe's economic strength.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

TABLE OF [INSERTS]

INTRODUCTION

Data has become one of organisations' key strategic assets. It underpins business processes, supports innovation, feeds artificial intelligence models and plays a direct role in the competitiveness of both businesses and public administrations. The flow of data is now an essential prerequisite for economic performance, but also a source of exposure to new risks.

The widespread adoption of cloud services and digital solutions operated by third-party providers is profoundly transforming the conditions under which these information assets are managed. Whilst these technologies offer considerable benefits in terms of agility, resilience and innovation, they also raise growing concerns about the ability of European organisations to protect their most strategic data against risks of interference, interception or unauthorised access, resulting in particular from foreign legislation with extraterritorial reach.

In recent years, the European Union has launched several major initiatives aimed at strengthening data governance, developing a European cloud market and improving cybersecurity. At the same time, France has introduced ambitious measures, such as the SecNumCloud certification and the 'Cloud at the Centre' doctrine. These developments reflect a shared commitment to strengthening digital trust. However, they leave one significant question unanswered: that of the protection of organisations' sensitive non-personal data.

Indeed, whilst personal data now benefits from a particularly well-structured legal framework, industrial, scientific, commercial or technological data – which nevertheless constitute an essential part of companies' information assets – remain covered by fragmented and often indirect measures. Existing mechanisms – contractual clauses, trade secrets or intellectual property – meet certain needs, but do not offer protection that is fully adapted to the challenges posed by the extraterritorial nature of certain legislation or by new data processing models.

It is against this backdrop that, as early as 2023, Cigref brought together a working group comprising numerous large companies, public authorities and experts to share their experiences, identify the difficulties encountered and develop a joint analysis of the issues at stake.

This briefing note has a twofold objective. Firstly, it aims to clarify the concepts of non-personal sensitive data and the 'trusted cloud' by analysing the legal, technical and organisational measures currently in place to protect these assets. Secondly, it sets out proposals designed to contribute to French and European discussions on the evolution of regulatory frameworks, with a view to reconciling data protection, innovation, competitiveness and strategic autonomy. Going beyond mere cybersecurity issues, this brief thus calls for the protection of sensitive non-personal data to be regarded as a major issue concerning industrial policy, economic sovereignty and competitiveness for European organisations.

1 CURRENT MECHANISMS FOR THE PROTECTION OF SENSITIVE NON-PERSONAL DATA

Until the enactment of the SREN Act, no clear and single definition of sensitive non-personal data was provided for in legislation. In reality, the GDPR only addressed sensitive data in relation to personal data, defined as 'any information relating to an identified or identifiable natural person'.

However, the SREN Act (Article 10 bis A) identifies two categories of sensitive non-personal data, the content of which is deemed critical to national sovereignty or security:

- Data constituting secrets protected by law, within the meaning of Articles L. 311-5 and L. 311-6 of the Code of Relations between the Public and the Administration.
- Data necessary for the fulfilment of the State's essential missions, in particular:
    - safeguarding national security,
    - the maintenance of public order,
    - the protection of people's health and lives.

Although this data is not personal, it is subject to enhanced levels of protection when hosted by the State or its operators, in particular via certified cloud services (e.g. SecNumCloud).

As detailed in Article 31 of the Act set out below, this data is defined in two ways: on the one hand, according to its content, and on the other, according to its impact in the event of disclosure.

Definition of sensitive data under the SREN Act

Chapter III: Protection of strategic and sensitive data in the cloud computing market (Articles 31 to 32)

Article 31

I. – Where State administrations, their operators, the list of which is annexed to the draft Finance Bill, and public interest groups comprising the aforementioned government departments or operators, the list of which is laid down by decree of the Council of State, use a cloud computing service provided by a private service provider for the implementation of IT systems or applications, they shall comply with the provisions of this Article.

If the IT system or application in question processes data of a particularly sensitive nature, as defined in (II), whether personal or otherwise, and if a breach of such data is likely to result in a threat to public order, public security, the health or life of individuals, or the protection of intellectual property, the State administration, its operators and the bodies referred to in this (I), shall ensure that the cloud computing service provided by the private service provider implements security and data protection criteria guaranteeing, in particular, the protection of data processed or stored against any access by public authorities of third countries not authorised by the law of the European Union or of a Member State.

II. – The following are classified as particularly sensitive data within the meaning of (I):

1° Data constituting secrets protected by law, in particular under Articles L.311-5 and L.311-6 of the Code of Relations between the Public and the Administration;

2° Data necessary for the performance of the State's essential functions, in particular the safeguarding of national security, the maintenance of public order and the protection of people's health and lives.

Consequently, there is no specific French or European protection mechanism designed to safeguard companies' sensitive non-personal data. Companies' sensitive non-personal data is therefore protected only indirectly through various mechanisms.

1.1 CLAUSES FOR THE PROTECTION OF SENSITIVE NON-PERSONAL DATA

In France, particularly due to the principle of freedom of contract (Article 1102 of the Civil Code), the protection of sensitive non-personal data may be addressed through contractual clauses. These clauses may provide for the restriction or prohibition of data transfers outside the EU (see the model Standard Contractual Clauses of 4 June 2021[1]). The company may, within the limits of the law, put in place any data protection mechanism it deems necessary.

[1] European Commission's model contract clauses of 4 June 2021[1] on the transfer of sensitive personal data outside the EU

This means of protection is particularly useful for agreements concluded between parties of equivalent economic standing, enabling them to negotiate on an equal footing. However, it has its limitations when contracts are standard-form contracts or when there is little negotiation between the parties.

1.2 TRADE SECRETS

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) establishes a harmonised European legal framework to combat the unlawful acquisition, use and disclosure of such information. It was transposed into French law by the Act of 30 July 2018 on the protection of trade secrets (codified in Articles L151-1 to L154-1 of the Commercial Code).

A trade secret is defined by three cumulative criteria: information known to a limited number of people; information having commercial value by virtue of its secret nature; and information which is subject to reasonable protective measures, having regard to the circumstances, taken by its rightful holder to maintain its secrecy. Trade secrets are subject to specific protections, and their disclosure may result in the civil liability of the infringer. Furthermore, the court may, without prejudice to the award of damages, order – including by way of a penalty payment – any proportionate measure likely to prevent or put an end to such an infringement.

The main weakness lies in the very nature of these laws. Trade secrets are a form of civil and commercial protection that enables a company to take legal action against a competitor, a former employee or a third party who has stolen or disclosed a secret, such as manufacturing processes, customer lists or algorithms. However, non-European laws with extraterritorial reach fall within the remit of state sovereignty, criminal law and intelligence. These laws therefore impose obligations to seize or monitor data on grounds of national security or criminal investigations.

The crux of the matter lies in the hierarchy of law and in international practice, where an American company ordered by its government (via a warrant from the FBI or the NSA) to hand over data cannot simply reply that it has no right to do so because the information constitutes a trade secret under European law. For the US justice system, in fact, a government order takes precedence over trade agreements or private-law secrets.

1.3 INTELLECTUAL PROPERTY

Whilst intellectual property (Articles 112-3 and L.341-1 et seq. of the Intellectual Property Code) provides a legal framework for defending ownership and commercial use of data covered bypatents, copyright or registered trademarks, it proves ineffective in the face of digital security challenges.

In conclusion, neither contractual clauses, nor trade secrets, nor intellectual property constitute a technical or legal barrier that can be invoked against extraterritorial legislation. They offer no protection against the access to or seizure of data by a foreign authority in the context of legal or intelligence proceedings imposed on a third-party hosting provider.

Legislative/regulatory focus on personal data	Existence of + or – indirect protection mechanisms	Difficulty in seeing binding legislation emerge
• The 2016 Regulation merely defines non-personal data as the counterpart to personal data • Existing legislation does not provide a strict framework for sensitive non-personal data	• **Contractual mechanisms** - Liability clauses - UP clauses - Security clauses • **Regulatory mechanisms** The Trade Secrets Protection Act 2018. • **EU legislation** In particular, the Data Act governing requests from foreign courts	• **At European level** through the EUCS ambitious goals but disagreements between Member States • **At national level** Chapter 3 (Articles 31 and 32) of the SREN Bill adopted in April 2024, which aims to regulate, through specific conditions, the cloud hosting of data belonging to government departments and state-owned operators.

Figure 1: Overview of the provisions governing non-personal data

2 ATTEMPTS BY PUBLIC AUTHORITIES TO PROTECT SENSITIVE DATA

2.1 AT EUROPEAN LEVEL

2.1.1 THE DATA ACT

The Data Act is a regulation that applies to all types of data generated by smart products and digital services within the EU, across all sectors. It establishes obligations and prohibitions applicable to a wide range of stakeholders.

This framework covers, amongst other things, data confidentiality, fairness, transparency of actions and interoperability. That said, its purpose is to regulate access to and use of data rather than to ensure a specific level of protection, particularly for non-personal data.

2.1.2 THE EUCS (EUROPEAN UNION CYBERSECURITY CERTIFICATION SCHEME FOR CLOUD SERVICES)

This proposed cybersecurity certification scheme for cloud services, which aims to establish a harmonised framework at European level, was provided for in the Cybersecurity Act, which came into force in 2019. For several years, our professional organisations have been advocating that beneficiaries of this certification scheme should be guaranteed immunity from non-European legislation with extraterritorial scope concerning sensitive and strategic data and the associated processing, in particular that relating to trade secrets, intellectual property and commercially sensitive data. It appears, however, that this position – shared by various French stakeholders – has continued to be strongly opposed by several European Union Member States throughout the 2019–2024 term, leading to France's relative isolation on this issue. We have therefore noted that the latest version of the Cybersecurity Act, published by the Commission on 20 January 2026 and currently under negotiation between the Council and the Parliament, adopts an approach that distinguishes so-called non-technical risks and refers the handling of these risks to the Cloud and AI Development Act (CADA), thereby tending to relegate the EUCS to a secondary role.

2.2 AT NATIONAL LEVEL

2.2.1 THE MILITARY PROGRAMMING ACT

In 2023, this draft bill aimed to require Operators of Vital Importance (OVIs) to put in place technical and organisational measures to ensure the protection of sensitive data within their Information Systems of Vital Importance (ISVIs). Cigref had considered that the Military Programming Act was not the appropriate vehicle for introducing this obligation, particularly because the legislative framework governing operators of vital importance was not designed to ensure the protection of operators' sensitive data , but rather to enable them to continue operating in the event of a threat to the nation's vital interests.

2.2.2 THE 'CLOUD-AT-THE-CENTRE' DOCTRINE

In its circular of 5 July 2021 on the doctrine governing the State's use of cloud computing**,** the Government has made integration into the cloud a prerequisite for any new digital project within the State; and, since that date, the digital services of government departments must be hosted either on one of the State's two internal inter-ministerial clouds or on cloud services provided by commercial providers that guarantee strict security criteria.

These provisions apply in particular to any digital product handling data of a particularly sensitive nature, whether personal or not, the breach of which is likely to result in a threat to public order, public security, people's health and lives, or the protection of intellectual property. The commercial cloud service selected must comply with the SecNumCloud certification or a European certification guaranteeing at least an equivalent level, particularly in terms of cybersecurity, and must be protected against any unauthorised access by public authorities of third-country governments.

2.2.3 THE ACT TO SECURE AND REGULATE THE DIGITAL SPACE (SREN ACT)

During the debates on the SREN Act, the possibility of using this legislative framework to extend the regulation of sensitive data beyond public sector bodies alone was raised.

The government and MPs from the ruling coalition ultimately undertook not to impose obligations on businesses to secure their sensitive and strategic data, in response to requests from certain parliamentarians. They stated at the time that they would address this issue through other instruments, notably the transposition of the NIS2 Directive.

This raised the question of whether the transposition of the NIS2 Directive could serve as a means of guaranteeing two important aspects for businesses: protection against cybercrime and protection against economic espionage. Ultimately, only the aspect of protection against cybercrime has been incorporated into the legislation currently being transposed through the Act on the Resilience of Critical Infrastructure and the Strengthening of Cybersecurity, which is still in the process of being transposed into French law, even though it should have come into force as early as October 2024. The text overlooks the aspect of legal protection against foreign state interference and economic espionage, thereby confirming the persistence of a legal vacuum regarding companies' strategic data.

Following the concluding joint committee meeting, the Senate finally adopted the final version of the SREN bill, which was subsequently passed by the National Assembly on 10 April 2024.

'The following are classified as particularly sensitive data:

1. *Data constituting secrets protected by law, in particular under Articles L. 311-5 and L. 311-6 of the Code of Relations between the Public and the Administration;*
2. *Data necessary for the fulfilment of the State's essential functions, in particular the safeguarding of national security, the maintenance of public order and the protection of people's health and lives.*

In this regard, it is worth comparing the provisions of the SREN Act with the Data Governance Act (DGA) and the Data Act.

Criterion	SREN Act (France)	Data Governance Act (EU)	Data Act (EU)
Main purpose	Cybersecurity, regulation of platforms and protection of individuals (minors, citizens)	Establishment of a framework to facilitate the voluntary sharing of data, particularly between the public and private sectors	Regulation of access to, use of and sharing of data, including non-personal data
Sensitive non-personal data	Not explicitly defined	Recognises certain industrial data as strategic, but without a dedicated legal category	Grants operational status to industrial data (e.g. connected machines, IoT), but does not include a 'sensitive' category in the strict sense
Protection of trade secrets	Indirectly, through the Trade Secrets Act	Encourages trust mechanisms (intermediaries, conditions for re-use)	Provides for restrictions on data access where this compromises a trade secret
Inter-company data sharing	Hardly addressed (outside the scope)	Provision for a framework for sharing with neutral intermediaries	Establishes a right of access to data generated by connected products for users, including business users
Cloud hosting	Limited, non-binding measures	Encourages localisation within the EU for certain public uses	Involves data portability, but with few guarantees of immunity
Interoperability / portability	No specific measures	Encourages, without making it mandatory	Mandatory in certain cases, to prevent vendor lock-in
Supervision / sanctions	CNIL and ANSSI, but they are not heavily involved with non-personal data	Establishment of data mediation authorities in each Member State	Provides for oversight mechanisms, but these remain vague (2025–2026)

Figure 2: Comparison between the SREN Act and European legislation

The SREN Act, adopted in France in 2024, is primarily aimed at strengthening digital security, providing a clearer regulatory framework for platforms and protecting citizens online, particularly minors. However, with regard to the protection of companies' sensitive non-personal data,it has some significant shortcomings, particularly in the following areas:

- **The definition of sensitive non-personal data**: the SREN Act does not provide a clear and precise definition of 'sensitive non-personal data'. This lack of a specific legal framework prevents adequate protection of strategic data such as, for example, trade secrets, research data or proprietary algorithms.
- **Regulation of the transfer of such data outside the EU**: unlike personal data governed by the GDPR, the SREN Act does not strictly regulate the transfer of business data to third countries. This therefore gives rise to increased risks of such data being intercepted or misused by foreign actors.
- **Data protection in the cloud**: as the law does not impose strict rules on the choice of secure cloud infrastructure for hosting sensitive non-personal data, companies may host their critical data with providers subject to extraterritorial laws.
- **Sanctions or remedies in the event of a strategic data breach**: as there is no specific mechanism for monitoring, sanctioning or alerting in the event of breaches involving non-personal but critical data, the lack of regulation prevents a rapid response in the event of theft or compromise.
- **Interoperability and transparency in algorithmic data processing**: the law does not impose any transparency or audit requirements on algorithms processing sensitive non-personal data, such as those used in industrial AI tools. As a result, companies may be exposed to bias, vulnerabilities or misuse without any real oversight.

3 PROTECTIVE MEASURES IMPLEMENTED BY COMPANIES

3.1 DEFINITION OF SENSITIVE DATA

Data can be defined as raw material derived from multiple sensors and sources: figures, sounds, images, text, geolocation, etc. The explosion in networks, satellite data streams and digital infrastructure has generated an overabundance of information, sometimes referred to as 'infobesity'.

As a critical intangible asset, data is no longer merely a by-product of digital activity. It is the fuel for industrial value chains and artificial intelligence. This central role presents organisations with a paradox: they must circulate this data to create value, whilst protecting it from a threatening environment where economic intelligence and strategic data capture have become systemic risks.

Organisations find themselves faced with a growing volume of data that must be collected, stored, structured, analysed and shared. Without these steps, data remains unusable and loses its operational value. Given this, is all data sensitive?

3.1.1 VARYING LEVELS OF SENSITIVITY

Within organisations, not all data carries the same level of sensitivity. A distinction is made between:

- Open data, accessible to all, or even published on the internet.
- Sensitive data, subject to access restrictions.
- Classified data, covered by legal secrecy provisions, requiring enhanced protection and strictly controlled access.

This hierarchy determines the methods of storage and distribution, and imposes specific technical and legal standards.

3.1.2 DATA PROTECTION AND RESILIENCE

Multiple and evolving threats

The data ecosystem is vulnerable at every stage of the data lifecycle: collection, processing, storage and use. As a result, threats are constant and rapidly evolving: data theft, intrusions, tampering, manipulation and compromise.

Ensuring data protection therefore requires constant vigilance. This sometimes leads to the creation of siloed ecosystems for sensitive data. However, these closed environments can restrict the flow of data, which is essential in systems that operate on a continuous flow basis. Hence the use of hybrid architectures to meet unclassified needs.

3.1.3 THE CENTRAL ROLE OF CYBERSECURITY

Cybersecurity aims to guarantee the integrity, availability and confidentiality of data. It is thus becoming a fundamental pillar of modern information systems.

To strengthen this protection, cybersecurity tools are increasingly incorporating artificial intelligence. This enables:

- The automation of threat detection;
- Anticipation of attacks;
- Rapid adaptation to new forms of cyberattacks.

With information systems becoming increasingly open to the outside world, isolation is no longer a viable option. It is therefore necessary to develop active cyber defence strategies and implement security by design.

3.2 PROTECTING DATA 'IN USE'

Against a backdrop of digital transformation accelerated by the dominance of the SaaS (Software as a Service) model, the question of where data is processed has become central. Whilst many software vendors are gradually phasing out their on-premises versions in favour of exclusively SaaS models, businesses are automatically seeing an increasing proportion of their data processed directly on cloud providers' infrastructure. This massive migration to outsourced environments makes the protection of data 'in use' critically important, and now constitutes a key vulnerability in modern architectures.

To properly understand this level of exposure to the risks of extraterritorial interference, it is important to distinguish between the three fundamental states of data: at rest, in transit and in use. Whilst current technologies offer robust solutions for the first two states, the third is now the critical vulnerability in cloud architectures, including in so-called 'trusted' environments.

3.2.1 RELATIVE CONTROL OVER DATA AT REST AND IN TRANSIT

The protection of data stored or circulating on networks relies on tried-and-tested encryption standards (AES, TLS), which are now widely adopted in the industry. In this context, information security no longer depends on the robustness of the algorithm, but on the governance of encryption keys.

Provided an organisation retains exclusive control over its keys, using schemes such as Bring Your Own Key (BYOK) or, better still, Hold Your Own Key (HYOK), and stores them in hardware security modules (HSMs) that it administers, it can theoretically guarantee that no third party – not even the hosting provider itself – will be able to access the intelligible content of stored or transferred files. Although complex to implement, this protection is technically feasible and widely used in large organisations that manage highly sensitive data.

3.2.2 THE STRUCTURAL VULNERABILITY OF DATA 'IN THE PROCESS OF BEING PROCESSED'

The paradigm shifts radically once the data needs to be processed. For an application, an algorithm or a database to process information, it must be decrypted in the server's random access memory (RAM) and processed in plaintext by the processor (CPU).

It is at this precise moment – the moment of computation – that a 'window of opportunity' for interference arises. In a public cloud environment, even a secure one, data decrypted in memory becomes potentially accessible to the service provider and, by extension, to a foreign authority with legal powers to compel that provider to disclose it.

3.2.3 THE LIMITATIONS OF CURRENT TECHNOLOGICAL SOLUTIONS

Faced with this risk, the digital ecosystem puts forward two types of technological response which, on closer analysis, do not currently provide a sufficient level of protection for the most sensitive data.

Homomorphic encryption: still a long way off and hypothetical

Homomorphic encryption, which would theoretically allow computational operations to be performed directly on encrypted data without ever revealing it – neither in memory nor to the processor – represents a sort of 'Holy Grail' of confidentiality, which has been talked about for many years. However, this technology remains at an embryonic stage, essentially a laboratory concept. The additional computational costs it entails – slowing down processing by several orders of magnitude – currently render it incompatible with the performance requirements of industrial information systems, confining it to niche use cases.

The Illusion of Confidential Computing

Several major cloud providers (hyperscalers), notably AWS, are actively promoting Confidential Computing based on secure enclaves (TEEs – Trusted Execution Environments). This approach promises to isolate data in memory, making it inaccessible even to the hypervisor administrator (the cloud provider).

However, as highlighted by the French National Cybersecurity Agency (ANSSI) in its technical note on the subject, published on 1 October 2025[2] , this technology offers no guarantee of security against a state actor or a hosting provider compelled to cooperate. Confidential Computing merely shifts trust: instead of trusting the system administrator, the customer must place their trust in the processor manufacturer and in the implementation of the enclave.

However, these technologies present two major shortcomings for European organisations:

1. **The lack of genuine auditability**: the internal workings of the processors and firmware managing these enclaves constitute a proprietary 'black box', often designed by the very same technology firms subject to extraterritorial jurisdictions.

[2] https://messervices.cyber.gouv.fr/documents-guides/anssi-technical-position-paper-coco-v1.0.pdf

2. **The persistence of physical control**: a cloud provider compelled by a legal order, such as a FISA warrant, retains physical and software control of the host infrastructure. Recent history in cybersecurity has shown that perfect isolation between the processor and the administrator is a promise regularly undermined by hardware vulnerabilities, notably side-channel attacks.

Consequently, it seems that viewing Confidential Computing as a safeguard against extraterritoriality is a risky gamble. As long as data must be decrypted to be processed on infrastructure controlled by a third party subject to foreign legislation, the risk of strategic compromise remains, however sophisticated the cryptographic enclave may be.

3.2.4 THE PRIMACY OF LAW OVER TECHNOLOGY

An analysis of the three states of data reveals an uncomfortable but particularly formative situation for any strategy to protect sensitive and strategic data: to date, there is no genuine technological shield.

Whilst encryption effectively protects data at rest and in transit, the absolute necessity of decrypting the information in order to process it creates a vulnerability that cannot be eliminated by technical means alone. Neither homomorphic encryption, which is still too immature, nor confidential computing, which is too dependent on hardware trust, allows us to completely eliminate the risk of interference.

Consequently, the ultimate security of data does not lie in the strength of the cryptographic armour, but in the legal status of the operator holding the infrastructure's keys. As long as processing takes place on the servers of a provider subject to coercive extraterritorial legislation, data protection remains conditional. The only guarantee of genuine immunity is therefore of a legal nature: it rests on the choice of a provider whose articles of association and location place it exclusively under the protection and obligations of European law.

3.3 CORPORATE PRACTICES REGARDING THE CLASSIFICATION AND PROTECTION OF SENSITIVE DATA

The management of sensitive data is a major strategic issue for businesses. Based on an analysis of feedback from four French and international industrial groups, we can observe specific practices, similarities and differences in approach, as well as the main expectations expressed regarding the regulatory framework.

3.3.1 PRACTICES REGARDING THE CLASSIFICATION OF SENSITIVE DATA

3.3.1.1 Increasing formalisation of classifications

All the companies analysed have implemented a formal data classification system, structured around several levels of sensitivity. Although the nomenclatures vary (secret / confidential / internal / public or public / confidential, etc.), they all aim to clearly distinguish critical data requiring specific protective measures.

3.3.1.2 Freedom of definition and regulatory standardisation

Several organisations have expressed reservations about regulatory definitions that are too vague or too restrictive. The very term 'sensitive data' is considered too broad. These organisations are calling for the ability to define the scope of sensitivity themselves, under their own responsibility, based on risks and business contexts.

3.3.1.3 Distinction between data and processing

Particular attention is paid to the distinction between the intrinsic sensitivity of data and the critical nature of the associated processing operations. Confusion between the two can lead to unnecessary or disproportionate constraints, to the detriment of operational agility.

3.3.2 STRATEGIES FOR PROTECTING SENSITIVE DATA

3.3.2.1 Risk-based, tiered protection

Organisations implement multi-layered protection strategies, combining:

- Internal measures: classification, mapping, access control, staff awareness-raising;
- Contractual measures: specific clauses depending on the type of data and the profile of the suppliers;
- Regulatory measures: use of certified service providers (notably SecNumCloud) for critical data.

Some companies go so far as to strictly limit the processing of sensitive data to local infrastructure within the country, in order to avoid any exposure to extraterritorial legislation.

3.3.2.2 Regulated multi-cloud and hybrid architecture

Two companies describe a hybrid approach to hosting: a combination of cloud and on-premises storage, depending on the level of sensitivity. The use of multi-cloud is permitted, but governed by rigorous governance and precise risk mapping.

3.3.3 REGULATORY CHALLENGES AND OBSTACLES ENCOUNTERED

Whilst the SecNumCloud certification is regarded in France as a benchmark for technical and legal robustness, its implementation is currently hampered by what many organisations perceive as a mismatch between the requirements of the framework and the reality of the digital services market. This friction is evident both in terms of governance within large organisations and the economic viability of providers.

3.3.3.1 Regulatory fragmentation incompatible with the continental scale of businesses

The first limitation lies in the strictly domestic nature of the certification. Large organisations, whose operational scope extends well beyond France's borders, find themselves unable to implement a

consistent data protection policy. The lack of mutual recognition or extension of this standard forces these companies to manage increased regulatory complexity, artificially segmenting their information systems where business logic would require unified governance across the scope of their European operations.

3.3.3.2 An untenable economic equation in the face of the hegemony of hyperscalers

Beyond this territorial constraint, it is the very economic rationale of the 'trust' offering that is most often called into question. The SecNumCloud framework, due to its maximalist nature, imposes particularly high barriers to entry on service providers, resulting in significant costs for compliance, maintaining operational standards and monitoring certification. However, these massive investments must be recouped in a 'niche' market, the narrowness of which stands in stark contrast to the breadth of the global market. For customers of these services, these costs translate into prices that are 15% to 20% higher than those charged by hyperscalers, for solutions with reduced and incomplete functionality.

Indeed, in an ecosystem where three non-European players command over 70 per cent of the market thanks to overwhelming economies of scale, the fragmentation of the so-called 'sovereign' French offering raises questions. The coexistence of nearly a dozen qualified providers in such a narrow market segment – and solely at a national level – does not allow for the critical mass required for sustainable competitiveness to be achieved.

It therefore seems unrealistic to assume that public procurement alone, whilst vital, can suffice to ensure the long-term viability of this national industrial base for the 'trusted cloud'. Without an expansion of the addressable market or a review of business models, there is a high risk that these trusted offerings will remain on state life support, unable in the long term to compete with international standards in terms of innovation and price.

3.3.3.3 The need for harmonisation and proportionality

European harmonisation of the rules is considered essential to avoid distortions of competition. Businesses are calling for an approach based on the proportionality of requirements, taking into account the actual level of risk associated with the data and its processing.

3.3.3.4 Awareness-raising and cultural adaptation across business units

Another key challenge identified concerns raising awareness amongst business units. Despite the formalisation of internal policies, effectiveness depends largely on staff engagement. Training programmes, validation processes and labelling tools are being rolled out to empower teams at every stage of the data lifecycle.

Expert opinion

What is the purpose of Data Security Posture Management?

DSPM (Data Security Posture Management) is an emerging discipline in cybersecurity that places data – rather than infrastructure – at the centre of protection. In a world where data is widely dispersed across multi-cloud environments, SaaS, hybrid environments, microservices and forgotten workloads, this approach finally provides complete visibility over sensitive data, its exposure and the associated risks.

DSPM fulfils four key functions: locating sensitive data, classifying it according to its criticality (PII, PCI, PHI, etc.), identifying risks of exposure or unauthorised access, and accelerating recovery in the event of an incident. These functions are becoming critical in the face of the explosion in shadow data: organisations are accumulating unsupervised, poorly protected or forgotten data, often stored in the cloud, which is the source of the majority of data breaches.

The complexity of cloud and microservices architectures makes reliable manual mapping almost impossible. DSPM provides a structured solution through automated discovery, AI/ML classification, permissions auditing and continuous monitoring. It constantly assesses misconfigurations, dangerous access, potential escalation paths and accidental public exposure.

A modern DSPM solution follows a continuous cycle:

- discover and classify all data, wherever it is located (on-premises, in the cloud, SaaS, backups),
- detect at-risk data by identifying policy breaches,
- automatically rectify issues and adjust policies to prevent them from recurring.

This challenge is compounded by regulatory pressure, particularly the obligations to report incidents promptly. Without clear visibility into the location of sensitive data and how it is protected, compliance is impossible.

Finally, DSPM plays a key role in cyber resilience, as it enables restorations to be prioritised according to data sensitivity, improves incident response and enhances platforms such as Cohesity Data Cloud through integration with specialist partners (Cyera, Big ID, Dasera). These integrations provide continuous classification, improved risk intelligence and optimised protection strategies.

Olivier Savornin – Group Vice President Europe at Cohesity.

The challenges of data protection
Case study of an international group

"A multinational company must comply with the applicable regulations in all the countries where it operates.

In this context, the (cyber) security of the company's data, as well as that of its suppliers, subcontractors and customers, is a priority. Indeed, the group's critical data varies in nature depending on the context and the country. This is why rules are defined at the appropriate level to manage risks.

Large teams are therefore set up to define requirements and recommendations, to determine the criticality of data by data type, to implement these measures and to ensure compliance (both regulatory and internal).

A proliferation of regional regulations creates complexity, and these can be counterproductive if they are not harmonised. It is therefore necessary to dedicate resources to this task."

Whilst these challenges highlight the need for an organisation to take charge of its data protection, each organisation will adopt a specific method of classification and protection. Here is an example of a three-tiered approach used by a Cigref member company.

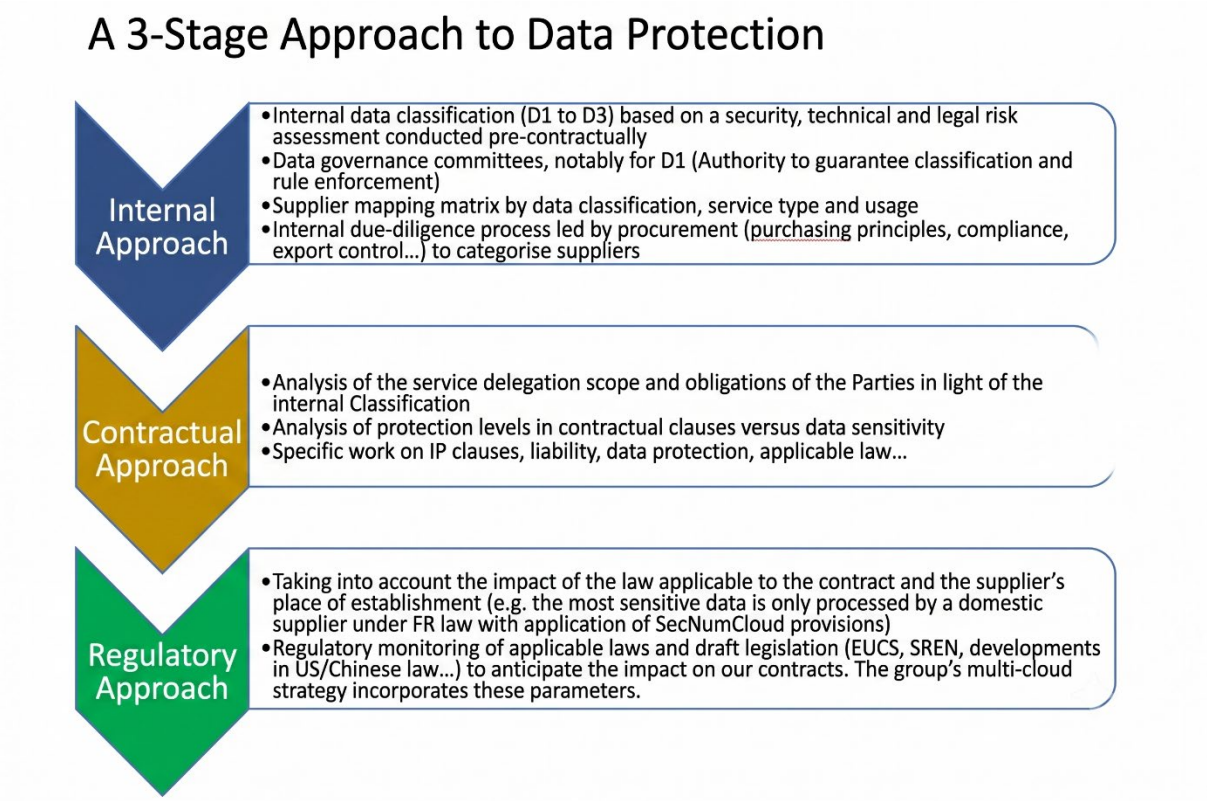

Figure 3: Example of an approach to data protection.

Three-stage diagram for data protection:
- Internal approach: classification of data sensitivity, establishment of governance committees and supplier compliance audits.
- Contractual approach: adapting contracts (intellectual property, liabilities) to the sensitivity level of the data being shared.
-Regulatory approach: selecting suppliers subject to protective local laws (e.g. highly secure French cloud services) and monitoring international legislation.

3.4 CHALLENGES ENCOUNTERED

Whilst the companies surveyed demonstrate a clear commitment to effectively protecting their sensitive data, whilst maintaining agility, competitiveness and operational security, their practices converge on several points: classification by sensitivity level, a tiered approach to protection, caution regarding extraterritorial laws and a desire for European harmonisation.

However, they also face obstacles: a lack of regulatory clarity, insufficiently mature solutions that are immune to extraterritorial laws, high costs and a gap between theory and operational constraints.

The definition of sensitive data at European level does not yet seem clear or precise enough for the majority of companies in the working group, who stress the need for a single, clarified definition.

Furthermore, some participants identified a difficulty in instilling a culture of classification across all business units, particularly those not based in France. The problem for a multinational company is that each country may devise its own definition or classification of sensitive data.

For some participants, educational initiatives are essential to increase the company's overall maturity regarding sensitive data. Training and awareness-raising programmes on the proper use of data can therefore be put in place. Each business unit must take ownership of the issue of data classification and define a framework, ensuring that all those who handle this type of data are aware of it and implement it. The IT department, for its part, must provide user-friendly classification tools: MIP (from Microsoft), for example.

One company also highlights a growing concern: in an increasingly digital world, there is a risk that non-sensitive data could be cross-referenced to uncover confidential information.

One participant believes that Article 19 of SecNumCloud does not provide genuine protection against unfair practices and points out that its implementation is extremely costly.

3.5 CROSS-CUTTING RECOMMENDATIONS

The participation of Cigref member companies in the working group has led to the identification of five best-practice recommendations:

1. Clarify regulatory definitions, in particular those of 'sensitive data' and 'trusted cloud'.
2. Adapt regulatory requirements to the actual criticality of the data, using a risk-based approach.
3. Promote a clear European certification scheme, recognised across the single market.

4. Strengthen the secure offering, particularly in relation to PaaS components and integrated services.
5. Support businesses in building their capabilities through guides, awareness-raising initiatives and operational tools.

4 CIGREF'S PROPOSALS FOR A MECHANISM TO PROTECT NON-PERSONAL SENSITIVE DATA

4.1 A COHERENT STRATEGY FOR THE PROTECTION OF SENSITIVE DATA IN THE FACE OF EXTRATERRITORIAL LAWS

Cigref's position as set out during the hearing at the National Assembly on 13 September 2023

4.1.1 BACKGROUND AND GENERAL FRAMEWORK

For several years, Cigref has been advocating for robust legislation offering businesses a range of legally binding tools enabling them to significantly improve the protection of their sensitive and strategic non-personal data, as well as the associated processing operations. The aim is to provide them with regulatory support designed to limit the legal and economic risks associated with the exposure of sensitive non-personal data, thereby contributing to the digital resilience of the economy.

Cigref has also highlighted that French and European cloud service providers need, above all, a solid customer base to support their growth and close the gap with their North American counterparts, rather than direct public funding. With this in mind, it recommends channelling public expenditure towards incentive mechanisms, particularly of a fiscal nature (accelerated depreciation, tax credits, etc.), in order to encourage the adoption of cloud solutions classified as 'trusted', both in France and across Europe.

4.1.1 European regulatory framework: a cornerstone

The Data Act, which became fully applicable on 12 September 2025, has provided an essential foundation for the implementation of consistent national provisions.

Article 32 of the Data Act (formerly Article 27 in the draft phase), in particular, makes two major contributions. First, it provides for compliance not only with European law but also with national legislation on the protection of **sensitive non-personal data**, giving the French legislator valuable leeway in transposing and adapting the regulation.

Second, it incorporates a broad definition of sensitive data, including trade secrets, commercially sensitive data, and elements protected under intellectual property law. This approach is much better aligned with the realities of the businesses represented by Cigref than the one initially proposed in draft Articles 10 bis and 10 bis A of the SREN bill.

Thus, whilst this European framework marks a historic step forward by harmonising the protection of organisations' intangible assets, it nevertheless leaves businesses facing a major challenge: the lack of operational guidelines and harmonised technical standards to translate these legal requirements into practical day-to-day IT security measures.

4.1.2 CONDITIONS FOR SUCCESS: CERTIFICATION AND SUPPORT

The use of cloud solutions compliant with these Data Act requirements presupposes the existence of a certified European offering. This is why Cigref attaches for a long time strategic importance to the development of the European Cloud Certification Scheme (EUCS), calling for it to include an optional label that is explicitly incompatible with obligations arising from non-European extraterritorial legislation.

Such a scheme should precede any national legislation imposing potential obligations on businesses regarding the use of qualified service providers.

It should also facilitate the emergence of a credible, trustworthy offering capable of standing up to functional comparison with the solutions offered by the hyperscalers (Microsoft, Google, Amazon), which account for over 70 per cent of the public cloud market in Europe.

4.1.3 ECONOMIC SUPPORT AND TRANSITION

Cigref warns of the additional costs that such obligations could entail for French businesses. To prevent them from losing competitiveness compared with their European counterparts, it has recommended that these new requirements be accompanied by incentives, particularly tax incentives. Aware of the slow pace at which the market is rebalancing, Cigref has also advocated the introduction of a transition period of 3 to 5 years, accompanied by deadlines for entry into force that may be specified by regulation

4.1.4 LIMITATIONS OF THE INITIAL DRAFT ARTICLES 10 BIS AND 10 BIS A (NOW ARTICLE 31)

Public-sector organisations and those entrusted with public service missions encountered difficulties in identifying the data covered by Articles L.311-5 and L.311-6 of the Code of Relations between the Public and the Administration, due to varying legal interpretations of the initial draft Articles 10 bis and 10 bis A of the SREN bill. Furthermore, these draft articles were interpreted as placing the responsibility for classifying and managing sensitive data primarily on cloud service providers. This posed problems both in terms of technical feasibility and the proper allocation of responsibilities between clients and service providers.

In light of these factors, it became essential for Parliament and the Government to establish a more coherent legal framework aligned with European developments. This led to the consolidation and adoption of Article 31 in the final SREN Law, which entailed:

The withdrawal of the initial draft Articles 10 bis and 10 bis A to allow for the drafting of a new, more protective and balanced text;

The rewriting of the provisions to remove ambiguities and bring them strictly into line with Rule R9 of the ‘cloud-at-the-centre’ circular;[1]

The explicit alignment of these national provisions with Article 32 (formerly Article 27 in the draft phase) of the European Data Act.

4.2 PROPOSALS ON THE EUROPEAN CLOUD SERVICES CERTIFICATION SCHEME (EUCS)

4.2.1 PROTECTION OF SENSITIVE DATA IN THE EUROPEAN ECONOMY AND THE POSITION OF EUROPEAN USERS ON THE EUCS

The European Union economy's technological dependencies on the US cloud industry have systemic effects on the legal status of sensitive and strategic non-personal data held by European businesses and public administrations.

Indeed, on 16 July 2020, the Court of Justice of the European Union (CJEU) handed down a landmark ruling invalidating the Privacy Shield, the agreement governing the transfer of personal data between the European Union and the United States. This ruling highlighted the practices of US intelligence agencies, which access the personal data of European citizens via US cloud service providers. When hosted by US service providers, this data is subject to legislation – notably Section 702 of the Foreign Intelligence Surveillance Act (FISA) – which allows the United States to collect data on a mass scale, a priori and without a court warrant, without providing the safeguards of proportionality required by European Union law. Recital 184 of this judgment emphasises that these laws do not comply with the minimum safeguards required by the EU, as the surveillance programmes resulting from them are not limited to what is strictly necessary.

In declaring the Privacy Shield invalid, the CJEU primarily emphasised the protection of personal data. However, Section 702 of the US Foreign Intelligence Surveillance Act (FISA) is not limited to personal data and also extends to non-personal data. It allows access to any type of sensitive or strategic data. This exacerbates concerns regarding the security of European economic information. The fact that the Data Privacy Framework (DPF) now provides certain assurances regarding the confidentiality of personal data is one thing, but it says nothing, however, about the protection of the confidentiality of sensitive and strategic non-personal data held by European businesses and public administrations.

4.2.2 TOWARDS A HARMONISED APPROACH TO THE CSA2 AND THE CADA

Changes to the European regulatory landscape, marked by the publication on 20 January 2026 of the revised version of the Cybersecurity Act (or CSA 2) by the European Commission, necessitate a clarification of Cigref's approach. The history of work on the European Cloud Security Certification Scheme (EUCS) shows that, following diplomatic and industrial offensives from outside Europe in late 2023, the Commission had removed any requirement for legal immunity from the 'High+' level in CSA1, relegating the handling of interference risks to the future Cloud and AI Development Act (CADA).

However, from the perspective of user organisations, a service provider's exposure to data seizure orders or unilateral interruption mechanisms (kill switches) directly compromises the confidentiality and availability of data and associated processing operations. This constitutes a structural operational security vulnerability rather than a geopolitical consideration. Moreover, Article 80-1(v) of the draft CSA 2 requires any certified service to 'withstand any event' that compromises confidentiality. This

obligation of result creates an insurmountable compliance impasse for providers subject to coercive foreign laws or non-disclosure orders (gag orders), rendering the current version of the EUCS legally deficient and vulnerable to censure by the Court of Justice of the European Union (CJEU).

Cigref would first like to draw the Commission's attention to the key issue of considering the relationship between the Cloud and AI Development Act (CADA) and the Cybersecurity Act 2 (CSA 2). It would indeed be ineffective to deal separately with vulnerabilities relating to cybersecurity techniques and threats relating to legal issues concerning access permitted by non-European legislation with extraterritorial effects. In order to simplify the work of the beneficiaries of these certification schemes – that is, all public and private organisations in Europe – we propose to the Commission a framework for seamless reconciliation between these two pieces of legislation.

Indeed, CSA 2 defines three so-called 'technical' levels of protection – *Basic, Substantial* and *High* – whilst the CADA proposes four levels of assurance. Cigref therefore advocates the introduction of a matrix-based approach to European security certification schemes, capable of offering each organisation the necessary flexibility according to its needs regarding the protection of its sensitive and strategic data, whether personal or not. Thus, depending on its own risk analyses, a company could require a 'Substantial' baseline combined with 'assurance level 3', or a 'High' baseline combined with 'assurance level 2'.

In particular, Cigref calls on the European Commission to promote such a matrix-based architecture, flexibly linking the CSA 2 protection levels and the CADA assurance levels, for the development of the European cloud security certification scheme, known as EUCS.

Alignment with a managed transition pathway (CADA / NIS 2):

Furthermore, noting the Commission's new paradigm—which seeks, during the 2024–2029 legislative term, to bring about a 'structural non-compliance shock' for the most critical sectors—Cigref emphasises the need to establish sustainable operational conditions for information systems. Achieving this ambition of the Commission requires several conditions to be met. Firstly, a realistic and phased timetable must be put in place, spanning 3 to 10 years depending on the criticality of the assets. Secondly, the text must focus its requirements on the timing of contract renewals. And finally, a fast-track mechanism must automatically exempt any service that has technically validated its resilience via the framework of Title III from Title IV of CSA2. In conclusion, European public funding support must be redirected towards the needs of client companies, to actively cover the costs of migration and technological replacement.

CONCLUSION

The protection of sensitive non-personal data is now a strategic imperative for the competitiveness and long-term viability of our organisations. The starting point for this report was to address a major legal blind spot: given our growing reliance on cloud infrastructures outside Europe, our members' non-personal information assets remain significantly exposed to legislation with extraterritorial reach, without any legally binding safeguards, unlike personal data, which benefits from a structured framework.

Our collective analysis has demonstrated that current safeguards remain inadequate. On the one hand, traditional legal mechanisms such as trade secrets, intellectual property or contractual clauses prove ineffective in the face of injunctions from foreign state authorities. On the other hand, technological analysis reveals that whilst data at rest and in transit can be encrypted, data 'in the course of processing' is subject to a structural vulnerability that neither confidential computing nor homomorphic encryption can mitigate.

This finding highlights the primacy of law over technology. The security of data and its processing relies largely on the legal status of the cloud provider and the legislation to which it is subject.

In light of these findings, Cigref calls for the establishment of a European regulatory framework that is ambitious, coherent and incentivising. Our recommendations centre on the need to adopt a flexible definition of 'sensitive data', leaving it to the discretion of companies based on their own risk analysis. Furthermore, we advocate for a seamless integration between the Cybersecurity Act 2 (CSA 2) and the Cloud and AI Development Act (CADA) within the EUCS certification scheme. This matrix-based approach should make it possible to combine technical security requirements with appropriate legal immunity safeguards.

Finally, this legitimate quest for protection must not undermine the competitiveness of our businesses in a context where the market is dominated by North American hyperscalers. The development of cloud service providers offering the highest levels of assurance regarding the confidentiality, integrity and availability of sensitive and strategic data held by European organisations will require economic support, notably through tax incentives, as well as realistic transition periods. It is only by doing so that Europe will be able to build a trusted digital space, where the security of data and the associated processing will be regarded as one of the drivers of our continent's economic prosperity.

Cigref is a network of major French companies and public administrations whose mission is to develop its members' ability to integrate and master digital technologies. Through the quality of its thinking and the representativeness of its members, Cigref is a unifying force in the digital society. Cigref was founded in 1970 under the French law of 1901, and does not engage in any profit-making activities.
To achieve its mission, Cigref relies on three core businesses that make it unique.

Membership
Cigref embodies the collective voice of France's leading companies and government agencies on digital issues. Its members share their experience of technology use within working groups, to help identify best practices.

Intelligence
Cigref participates in collective reflection on the economic and societal challenges of information technologies. Founded nearly 50 years ago, Cigref is one of the oldest digital associations in France, and draws its legitimacy from both its history and its mastery of technical subjects, the foundation of skills and know-how that underpin the digital world.

Influence
Cigref promotes and respects the legitimate interests of its member companies. As an independent forum for exchange and production between practitioners and players, it is a benchmark recognized by its entire ecosystem.

www.cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr


Cigref
SUCCEED
WITH DIGITAL