INFORMATION NOTE
AND NEWS

# Overview of European digital legislation

> UNDERSTANDING THE APPLICABLE REGULATIONS

CIGREF
SEPTEMBER 10TH, 2023

Cigref
SUCCEED WITH DIGITAL

Cigref

# Overview of European digital legislation

*Understanding the applicable regulations*

*September 2023*

## FOREWORD

Since the arrival of the RGPD in the European regulatory landscape, and during the work led by Cigref between June 2016 and November 2017 to prepare its entry into force on 25th May 2018 for the benefit of our members, our association and its Board of Directors have become convinced of the importance of our involvement upstream of the drafting of European legislation. This upstream work should make it possible to guard against regulatory overzealousness on the part of the European institutions, on the one hand, and the exorbitant and asymmetrical lobbying resources that non-European technology giants know how to deploy to steer the legislative processes to their advantage, on the other. It is against this backdrop that Cigref has acquired the capacity to assess, decide and act to influence the European Commission, Council and Parliament, so as not to leave these legislative processes, which could have an impact on our members, solely in the hands of their main suppliers of digital products and services.

Of course, the game remains uneven, as we have seen once again with the European Commission's refusal to designate AWS, Google Cloud and Microsoft as gatekeepers for cloud services, despite the fact that they are clearly identified in the Digital Markets Act. We have no doubt about the intensity of the lobbying that these players had to deploy to achieve this result. We have seen this again in the current negotiations on a European cloud certification scheme, the EUCS. In an open letter addressed to the highest level of the US administration, the main organisations representing the US tech industry called for action against the proposed European certification scheme on the grounds that it "potentially threatens the economic interests and national security of the United States".

While we have not been entirely successful with the European institutions in recent years, they now know that they can count on our associations representing professional users of digital products and services. And they no longer hesitate to call on us and listen to what we have to say. Against this backdrop, it is essential that our members maintain their commitment to the various legislative texts that are still being negotiated and adopted within the European institutions, and which are presented in this Cigref information note.

We are therefore publishing this overview of European digital regulations primarily for our members. It was produced following an excellent summary by our trainee lawyer, Aliette Diéval, whose professional qualities I would like to pay tribute to and whom I would like to thank most warmly.

**Henri d'Agrain,**
General Delegate of Cigref

## TABLE OF CONTENTS

# 1 INTRODUCTION

In response to the constant evolution and development of digital technologies, the European Union has adopted a "Digital Agenda for Europe 2020-2030".

As part of this strategy, the European Commission has proposed a number of regulations aimed at regulating the role of digital services and markets and facilitating data transfers, while ensuring the confidence and security of European businesses and citizens.

# 2 DIGITAL MARKETS ACT

The aim of the Digital Markets Act is to establish fair and equal conditions of competition in order to foster innovation, growth and competitiveness, both within the single market and internationally, and to strengthen European consumers' freedom of choice.

As a tool for ex-ante regulation of the market, the regulation aims to put an end to the domination of "gatekeepers" at the entrance to the Internet. These companies, which have an annual turnover of at least €7.5 billion in the European Union and more than 45 million monthly users, are subject to various obligations and prohibitions:

- Gatekeepers are required to:
    - Allow users to uninstall applications already preinstalled on their smartphones;
    - Making instant messaging services interoperable;
    - Give application developers fair access to the ancillary functionalities and hardware of smartphones.
- Gatekeepers are prohibited from:
    - Rank their own products or services more favourably than those of their competitors: this is the end of the principle of self-preference;
    - Use, without the consent of users, their personal data collected between different services;
    - Prevent user companies from offering their products or services on different terms on other platforms or distribution channels.

## 2.1 INSTITUTIONAL CHRONOLOGY

- **December 15, 2020**: Commission proposal;
- **July 5, 2022**: Parliament's position;
- **July 18, 2022**: general orientation of the Council;
- **October 12, 2022**: publication in the OJEU (Official Journal of the European Union);
- **November 1, 2022**: entry into force;
- **May 2023**: implementation;
- **September 6, 2023**: the Commission designates the gatekeepers.

## 2.2 CIGREF'S POSITION

- Call for a review of the qualitative and quantitative criteria used to define gatekeepers in order to:
    - Adopt an approach based on market size and niche markets rather than thresholds;

    - To avoid undesirable collateral effects by considering only the share derived from the sale of digital services.

- Call for the inclusion of directly applicable measures to prohibit more unfair practices that are detrimental to users;
- Call for the list of unfair practices to be extended and made progressive;
- Call to strengthen the effective implementation of the rules by national authorities with extensive enforcement powers;
- As the Commission's designation of gatekeepers on 6 September 2023 did not include the 3 main cloud providers under the DMA, Cigref sent a letter of protest and request for clarification to the Presidency of the European Commission, co-signed by its Belgian, Dutch and German partners.

## 2.3 ADAPTATION OF NATIONAL LAW

**Digital Space Bill**: Aims to prohibit digital giants from favouring their services on their platforms. The direct application of the DMA at European level will strengthen the ability of European companies to penetrate the markets of the digital economy.

# 3 DIGITAL SERVICES ACT

The Digital Services Act aims at ensuring a safe online environment by making "intermediary service providers", i.e. platforms and search engines, responsible for protecting fundamental rights such as freedom of expression and consumer protection. To this end, the regulation provides for measures to combat the dissemination of illegal and harmful content, as well as illegal products and services online.

Replacing the e-commerce directive of 8 June 2008, the regulation puts into practice the principle that "what is illegal offline is illegal online". To achieve this, the very largest platforms and search engines, i.e. services with at least 45 million monthly users, are subject to two obligations:

- **Obligation of transparency online**: provides an internal complaints handling system, explain how algorithms work, ban targeted advertising for minors and profiling based on sensitive data;
- **Obligation to mitigate risks and respond to crises**: analyse the systemic risks generated, carry out independent risk reduction audits and grant researchers access to key data from their interface.

## 3.1 INSTITUTIONAL CHRONOLOGY

- **December 15, 2020**: Commission proposal;
- **July 2022**: Parliament's position;
- **October 2022**: general direction of the Board;
- **October 27, 2022**: publication in the OJEU;
- **November 16, 2022**: entry into force;
- **August 25, 2023**: entry into force for very large platforms and search engines;
- **January 1, 2024**: implementation.

## 3.2 ADAPTATION OF NATIONAL LAW

**Securing and Regulating the Digital Space Bill (SREN Act):**

- Ban advertising targeted at minors or using sensitive data;
- Free choice of search engine, browser and e-mail service: as a direct application of the DSA at European level, the French will no longer be able to be dictated to in terms of the tools they use online.

# 4 DATA GOVERNANCE ACT

As part of the European Data Strategy, the Data Governance Act aims at encouraging the sharing of personal and industrial data by setting up **intermediation structures**. The regulation also aims at boosting confidence in data sharing (relating to health, mobility, environment, agriculture, etc.) by making it safer, easier and compliant with data protection legislation.

There are four sets of measures to stimulate the development of reliable data sharing systems:

- Put in place mechanisms to facilitate the re-use of certain public sector data that cannot be made available as open data (e.g. health data for research);
- Guarantee the reliability of intermediaries in the sharing and pooling of data within common European data spaces in strategic areas (health, environment, energy, finance, etc.);
- Reinforcing the altruism of data: sharing data for the benefit of society (for medical research, global warming, etc.);
- Facilitate cross-border data sharing.

Finally, the Regulation has created the European Data Innovation Board to facilitate the sharing of best practices.

## 4.1 INSTITUTIONAL CHRONOLOGY

- **November 25, 2020**: Commission proposal;
- **April 2022**: Parliament's position;
- **May 16, 2022**: general direction of the Council;
- **June 3, 2022**: publication in the OJEU;
- **June 13, 2022**: entry into force;
- **September 2023**: implementation.

## 4.2 ADAPTATION OF NATIONAL LAW

**Bill to "Secure and Regulate the Digital Space"**: stimulating Europe's data economy.

# 5 DATA ACT

As part of the European Data Strategy, the Data Act aims to maximise the value of data in the economy by facilitating the availability and sharing of data between businesses, consumers and public bodies. Complementing the DGA, it specifies who can create value from data and under what conditions.

It includes an obligation for "data holders", i.e. manufacturers of connected products and providers of related services, to share data with users. However, since the RGPD and the Schrems and Schrems II rulings (invalidating EU-US adequacy rulings), cloud services must prevent international transfers of industrial data, or access to it by a third-party government, that would not be compatible with European and national legislation.

## 5.1 INSTITUTIONAL CHRONOLOGY

- **February 23, 2022**: Commission proposal ;
- **March 14, 2023**: Parliament's position ;
- **March 17, 2023**: general direction of the Council.

## 5.2 CIGREF'S POSITION

- Unfair contract terms must stop for all types of businesses, not just the smallest;
- Clear definitions are essential to guarantee legal certainty, particularly with regard to the actors in the data chain and the definition of the data covered by the Regulation, while respecting commercial secrets;
- The regulation is an appropriate means of prohibiting anti-competitive behaviour and the misuse of data, as a complement to the DMA;
- Higher ambitions are possible in terms of changing data processing service providers;
- Clear limits on data availability and fair compensation systems are essential to support innovation;
- Clear rules and strong sanctions for international data transfers must be put in place.

# 6 CYBERSECURITY ACT

Clarifying the NIS2 Directive of 14 December 2022, the aim of the "Cybersecurity Act" is to ensure a high level of cybersecurity within the EU, initially by giving ENISA a new mandate: the European Union Cybersecurity Agency will consolidate cooperation within the Union, in particular by using a network of cyber incident response teams, help Member States in their efforts to strengthen their capacities and ensure that citizens have confidence in digital Europe.

Secondly, the regulation establishes a European cybersecurity certification framework at EU level for ICT products, services and processes. The aim is to harmonise assessment methods between Member States by creating three common levels of cyber certification, leading to mutual recognition of certificates between Member States. These three levels of cyber security assurance are proportionate to the cyber risk associated with the use of the ICT product, service or process:

- Basic level of insurance: for items intended for the general public ;
- Substantial level of assurance: for objects that have passed conformity tests by conformity assessment bodies;
- High level of assurance: if the objects have been thoroughly tested.

## 6.1 INSTITUTIONAL CHRONOLOGY

- **September 13, 2017**: Commission proposal;
- **March 12, 2019**: Parliament's position ;
- **April 9, 2019**: general orientations of the Council ;
- **April 17, 2019**: publication in the OJEU ;
- **June 28, 2021**: entry into force.

# 7 CYBER RESILIENCE ACT

Complementing the NIS2 Directive of 14 December 2022, the aim of the Cyber Resilience Act is to guarantee greater security for software and hardware products in order to address two problems: the low level of cyber security and the lack of clarity in product security information.

This regulation introduces an obligation for manufacturers of connected products to ensure the security of products with a digital component from the moment they are designed: this is a duty of vigilance for the entire life cycle of the product. Manufacturers are also prohibited from supplying products with known security flaws.

## 7.1 INSTITUTIONAL CHRONOLOGY

- **September 15, 2022**: Commission proposal.

## 7.2 CIGREF'S POSITION

- Adopt an approach that is consistent with other European Union legal instruments on cyber security, in particular the NIS Directive2 ;
- Design a vulnerability compliance assessment that is better aligned with operational practices and constraints, particularly in terms of reporting vulnerabilities and their treatment;
- Strengthen provisions relating to open source software and components;
- Cover digital technologies in products, services and processes regardless of whether they are used by individual consumers or professional users.

# 8 CYBER SOLIDARITY ACT

The Cyber Solidarity Act was proposed in March 2022 in response to Russia's invasion of Ukraine: the aim is to strengthen EU-wide cooperation on preparing for, detecting and responding to large-scale cyber attacks, and to stimulate coordination both across borders and between the public and private sectors within a single Member State.

To achieve this, the regulation provides for the creation of various structures:

- **A European Cyber Shield** consisting of national and cross-border Security Operations Centres (SOCs) located throughout the EU. These regional cyber cooperation hubs will detect, mitigate and respond to threats (using AI in particular). This shield will not replace the Member States' current cybersecurity operations centres and will have to cooperate with them;
- **Cybersecurity reserve** comprising certified and trusted private companies ("trusted suppliers") ready to intervene in the event of a major incident. However, this will lead to institutional competition between the European External Action Service (EEAS) and the European Cybersecurity Agency (ENISA);
- **Cybersecurity Incident Review Mechanism** to improve the EU's cyber posture by reviewing and analysing major incidents after the event to inform future developments in the EU's approach to cyber defence.

## 8.1 INSTITUTIONAL CHRONOLOGY

- **April 18, 2023**: Commission proposal.

## 8.2 CIGREF'S POSITION

Organisation of a consultation of members.

# 9 ARTIFICIAL INTELLIGENCE ACT

The Artificial Intelligence Act is the first text in the world to regulate the placing on the market, putting into service and use of artificial intelligence systems by establishing harmonised rules within the EU: this regulation is therefore intended to become a global standard (Brussels effect). By adopting this regulation, the EU aims to stimulate research and industrial capacity, and promote investment and innovation in AI, while ensuring safety, the protection of fundamental rights and transparency with regard to the use of AI systems.

The Regulation classifies AI systems into three categories with different obligations based on a risk-based approach:

- AI systems presenting **unacceptable risks** are prohibited;
    - Examples: real-time remote biometric identification, social rating.
- **High-risk** systems are subject to transparency and traceability obligations and require human control;
    - Examples: critical infrastructure management, access to essential services.
- **Low** or minimal **risk** systems are only subject to a transparency obligation.
    - Examples: spam filters, chatbot.

## 9.1 INSTITUTIONAL CHRONOLOGY

- **April 21, 2021**: Commission proposal;
- **December 6, 2022**: general direction of the Council;
- **June 14, 2023**: Parliament's position.

## 9.2 CIGREF'S POSITION

- We need more flexible, progressive, proactive and reactive regulation.
- We need to create an independent European administrative body with a reactive regulatory remit to take account of technological dynamics and adapt the obligations and constraints of the IA Act to the current context.
- Even in the presence of "regulatory sandboxes", it must be possible to test under real conditions, in particular by spontaneously using test data sets.

# 10 E-PRIVACY REGULATION

The ePrivacy Regulation, which clarifies the GDPR, was due to come into force at the same time as the GDPR, but negotiations were blocked for four years in the Council: this explains why the 2002/58/EC Directive on privacy and electronic communications, amended in 2009 (2009/136/EC "Cookies" Directive), is still in force. However, as the latter has become obsolete, it needs to be replaced by this ePrivacy regulation in order to take account of new market players and technological and commercial developments over the last 20 years.

Article 1 of the regulation sets out the two objectives of the text:

- To protect the rights and freedoms of natural and legal persons in relation to the provision and use of electronic communications services (including the right to privacy and communications), and to protect individuals with regard to the processing of personal data;
- Guaranteeing the free movement of electronic communications data and services within the EU.

The regulation will apply to natural and legal persons within the EU, and will cover the processing of electronic communications and metadata, commercial canvassing and the use of cookies. Its implementation will allow the use of a "cookie wall", provided that the user can choose between this offer and an equivalent one that does not require consent to cookies and is provided by the same supplier.

## 10.1 INSTITUTIONAL CHRONOLOGY

- **January 2017**: Commission proposal;
- **October 20, 2017**: Parliament's position;
- **February 2021**: general direction of the Council.

# 11 EU-US MATCHING DECISION

## 11.1 PREVIOUS SUITABILITY DECISIONS

### 11.1.1 SAFE HARBOR

Adequacy decision proposed by the European Commission allowing the transfer of data between the European Union and US operators adhering to its data protection principles. This decision was invalidated on 6 October 2015 by the Schrems ruling of the CJEU.

### 11.1.2 PRIVACY SHIELD

US self-certification mechanism recognised by the European Commission as offering an adequate level of protection for personal data transferred from a European entity to companies established in the United States. Providing for the possibility of recourse to a mediator, "ombudsperso", this adequacy decision came into force on 1 August 2016 but was invalidated on 16 July 2020 by the Schrems II ruling of the CJEU.

## 11.2 NEW ADEQUACY DECISION: THE DATA PRIVACY FRAMEWORK (DPF)

The aim of this new adequacy decision is to guarantee the security and privacy of European citizens, while promoting economic opportunities for European businesses.

US organisations and companies will have to update their privacy policies to comply with this new adequacy decision within 3 months of the decision coming into force.

This new adequacy decision provides new guarantees and protections compared to Safe Harbor and Privacy Shield:

- Creation of a **two-tier appeal mechanism** through an authority whose decisions are binding:
    - The possibility of lodging a complaint with the Civil Liberties Protection Officer, who ensures that data transfers between US intelligence agencies comply with fundamental rights, including privacy;
    - The Officer's decision may be appealed to the Data Protection Review Court, which may delete data collected in breach of the US presidential decree of 7 October 2022.

- **Principle of necessity and proportionality** in access to data by US national security authorities to protect national security.

## 11.3 INSTITUTIONAL CHRONOLOGY

### 11.3.1 SAFE HARBOR

- **July 26, 2000**: Commission decision;
- **November 2010**: Parliament resolution;
- **December 2, 2010**: Council decision;
- **October 6, 2015**: Schrems ruling by the CJEU invalidating the Safe Harbor.

### 11.3.2 PRIVACY SHIELD

- **July 2016**: Commission adequacy decision: "EU-US Data Protection Shield";
- **December 2, 2016**: Council decision;
- **July 16, 2020**: Schrems II ruling by the CJEU invalidating the Privacy Shield.

### 11.3.3 ADEQUACY DECISION

- **March 25, 2022**: Joint declaration by the European Commission and the United States on the transatlantic framework for the protection of personal data;
- **October 7, 2022**: Presidential decree from US President Joe Biden providing for the implementation of the joint declaration of 25 March 2022 in national law;
- **December 2022**: launch of the process for adoption of the new adequacy decision by the European Commission;
- **July 10, 2023**: Adequacy decision by the European Commission.

# 12 LEXICON

## 12.1 THE INSTITUTIONAL TRIANGLE: THE INSTITUTIONS OF THE EUROPEAN UNION

### 12.1.1 THE EUROPEAN COMMISSION

As "Guardian of the Treaties", the Commission embodies executive power and represents the general interests of the Union. Based in Brussels, it is made up of 27 Commissioners, one from each Member State, each with a specific portfolio for a 5-year term of office. It has a monopoly on legislative initiative under the ordinary legislative procedure, proposing legislation to the Council of the European Union and the European Parliament.

### 12.1.2 THE COUNCIL OF THE EUROPEAN UNION

Also located in Brussels, the "Council", also known as the "Council of Ministers", brings together the government ministers of each Member State according to the areas on the agenda. As the embodiment of legislative power, it votes, as co-legislator with the European Parliament, on the Commission's legislative proposals under the ordinary legislative procedure.

### 12.1.3 THE EUROPEAN PARLIAMENT

Based in Strasbourg and Brussels, the 705 members of the European Parliament, elected by direct universal suffrage, represent the citizens of the Union. As co-legislator, it participates jointly with the Council in the adoption of legislative acts proposed by the Commission.

### 12.1.4 THE COURT OF JUSTICE OF THE EUROPEAN UNION

Formerly the ECJ (Court of Justice of the European Communities), the CJEU is the Union's judicial institution. Working alongside national courts, the 27 judges based in Luxembourg review the legality of EU acts and ensure that Member States comply with the Treaties by issuing binding and enforceable rulings.

## 12.2 ORDINARY LEGISLATIVE PROCEDURE

Under Article 294 of the Treaty on the Functioning of the European Union, the co-decision procedure is the ordinary legislative procedure. This procedure is based on the principle of parity between two co-legislators who jointly adopt the European Commission's proposals: the European Parliament and the Council of the European Union.


## 12.3 ACTS OF THE EUROPEAN UNION

### 12.3.1 REGULATIONS

It is a legal act of the European Union of general and mandatory scope, directly applicable as soon as it enters into force, in order to guarantee simultaneous and uniform application of European legislation in all Member States.

### 12.3.2 DIRECTIVE

It is a legal act of the European Union requiring transposition by the Member States to which it is addressed so that it can be binding on them in terms of the result to be achieved.

### 12.3.3 SUITABILITY DECISION

Under Article 45 of the GDPR, the European Commission may declare that a third country or international organisation ensures an adequate level of protection for personal data, thereby allowing the transfer of such data between the European Union and the third party concerned.

To do this, it proposes an "adequacy decision" to the Council and the European Parliament in which it assesses the level of data protection, taking into account in particular respect for human rights and fundamental freedoms under the third country's national legislation, as well as the existence and effective operation of independent supervisory authorities responsible for ensuring compliance with data protection rules.

# ABOUT CIGREF

Serving the economic growth and competitiveness of our members, large French companies and public administrations, users of digital solutions and services, through digital success.
Cigref is a network of major French companies and public administrations whose mission is to develop its members' capacity to integrate and master digital technologies. Through the quality of its thinking and the representativeness of its members, it is a unifying force in the digital society. Cigref was founded in 1970 as a not-for-profit association under the law of 1901.

To achieve its mission, Cigref relies on three areas of expertise that make it unique.

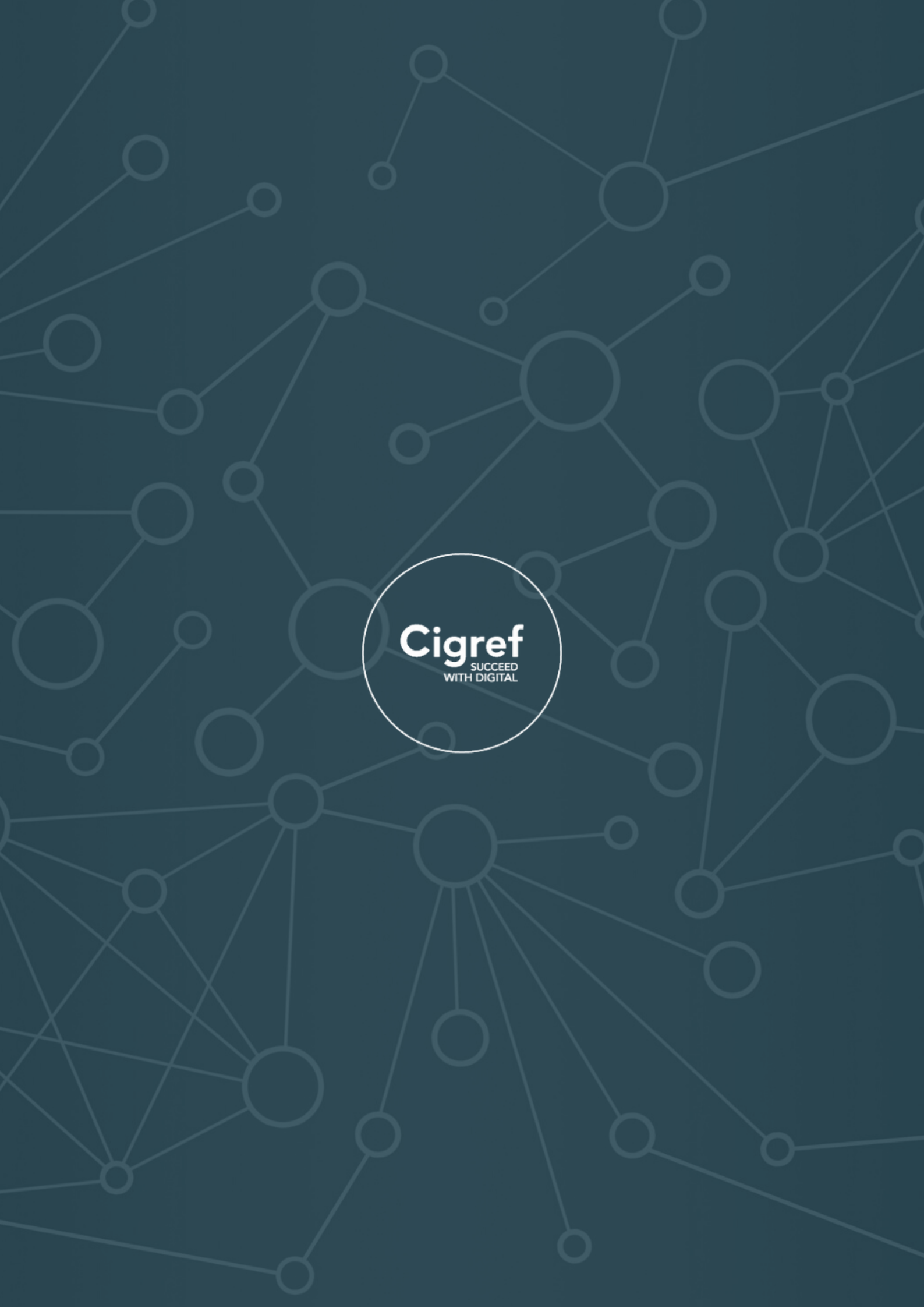
**Membership**
Cigref embodies the collective voice of France's major companies and public authorities on digital issues. Its members share their experiences of using technologies within working groups to bring out the best practices.

**Intelligence**
Cigref participates in collective discussions 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 issues, the foundation of skills and know-how that underpin digital technology.

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

# CONTACT US

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


Cigref
SUCCEED
WITH DIGITAL