

CIGREF MEMO

> RECOMMENDATIONS ON GENERATIVE AI

> FROM OUR GENERATIVE AI TASKFORCE

Cigref
SUCCEED
WITH DIGITAL

2023



Cigref

Cigref memo

Recommendations on generative AI

July 2023



Intellectual property rights

All Cigref publications are made available to the general public free of charge, but are protected by the intellectual property laws in force.

TABLE OF CONTENTS

1 INTRODUCTION	2
2 RECOMMENDATIONS FOR USE AND GOOD PRACTICE	3
2.1 Experiment with generative AI tools.....	3
2.2 Acculturate employees	3
2.2.1 Define your communication strategy	3
2.2.2 Train	4
2.2.3 Organise	4
2.2.4 Involve human resources.....	4
2.3 Identify use cases and performance improvements.....	5
2.4 Put in place processes to industrialise use cases with generative AI systems	5
2.5 Raise awareness of the need for careful, reasoned use	6
2.6 Include an environmental impact assessment from the outset	6
2.7 Take stock of solutions and suppliers	6
3 RISKS RELATING TO GENERATIVE AI SYSTEMS	7

1 INTRODUCTION

When the ChatGPT (Chat Generative Pre-trained Transformer) application was made available to the general public in November 2022, it created a media storm in the field of artificial intelligence technologies and generated a veritable craze. ChatGPT made visible the dynamics of artificial intelligence research that has been developing for several years now, the consequences of which have been predicted and documented. It is now clear that generative AI tools will have a major impact on public administrations and businesses in a wide range of sectors, with systematic effects on their productivity and performance.

This is why Cigref has launched a Task Force, led by Baladji Soussilane, Vice-President Digital & IT of the Air Liquide Group, and facilitated by Marine de Sury, Cigref's Mission Director, bringing together more than forty of its members to exchange practices and pool experiences. The purpose of this memo is to list the various recommendations put forward by Cigref so that its members, and potentially other organisations, companies, government departments, academies or associations, can tailor them to their own context and challenges.

Companies are reacting in different ways to the use of generative AI tools. Some prefer to prohibit, at this stage, any internal use of company data or the opening of accounts using employees' professional email addresses, in order to prevent the exfiltration of strategic or sensitive data. On the other hand, others are taking advantage of the opportunity to create an appetite for these new technologies and generate business opportunities. To do this, they share private generative AI tools in SaaS mode or hosted internally, set out guidelines indicating what can and cannot be done (for example, prohibiting the use of company documents on public tools) and put in place a "control tower" to regulate usage.

Some players are offering services that ride the "Generative AI" wave, requiring documents to be uploaded for analysis and offering no guarantee as to how the information contained will be used. The same applies to ChatGPT-type tools when they train LLMs (Large Language Machines) with conversations/corpus of company data.

Whatever their position, all organisations are unanimous in saying that the biggest risk is to miss out or fall behind the transformation brought about by generative AI. **Risks and security need to be managed in parallel, not as a prelude to thinking about opportunities.**

The first part of this memo lists the recommendations for use and good practices concerning the use of generative AI systems that it is important to share internally. Generative AI is already shifting the boundaries of productivity and creativity, and therefore offers real opportunities to be seized. However, they also present risks that need to be identified in order to better protect against them. This is the subject of the second part of this document.

2 RECOMMENDATIONS FOR USE AND GOOD PRACTICE

2.1 EXPERIMENT WITH GENERATIVE AI TOOLS

For the majority of companies and public administrations, it is essential to seize generative AI tools as soon as possible, to embark on a process of **learning, experimentation and appropriation**, so as to be able to implement them with the desired level of security, and develop appropriate and relevant uses for them. Then, practical experience enables us to put in place processes for validating use cases and to better control the associated costs.

Many companies recommend starting experimentation on a small scale and favouring the use of several "small use cases" of generative AI rather than one large all-purpose model, mainly because of the agility, modularity and speed with which solutions evolve. It would be a shame to invest too early in a technology or in-house development that would be out of date a few weeks later.

Testing generative AI systems helps to **identify their potential, but also their limits**. In order to learn how to handle them with care, organisations rely on men and women to verify or participate in the validation of results, whenever important decisions are taken on the basis of AI systems.

2.2 ACCULTURATE EMPLOYEES

As a first step, organisations recommend **assessing the maturity of** all their teams with regard to data and AI, in order to best adapt the communication and training to be implemented. Indeed, companies and public administrations are unanimous on the importance of raising awareness, acculturating and training people in the use of generative AI tools. The executive committee is the primary target, and many organisations keep them regularly informed of progress on the various projects involving these tools.

2.2.1 DEFINE YOUR COMMUNICATION STRATEGY

The general public's infatuation with the best-known generative AI systems, ChatGPT, DALL-E, Midjourney and GitHub Copilot, is leading companies and public administrations to acculturate all employees in all these tools and systems, by informing, demystifying and encouraging use, as well as widely sharing rules of conduct and ethics, sometimes called "do's and don'ts", using appropriate communication channels and formats adapted to the target audience. One company, for example, has set up an alert dedicated to AI-type sites, via the company proxy, which reminds employees of the rules as soon as they are about to use one of these tools.

In the same way, it would be interesting to quickly impose **specific rules on subcontractors**, in particular to guarantee that they themselves do not use public AI, for example on development.

Several organisations are presenting generative AI concepts to different levels of the organisation (CxO, business, support, controls), adapting the messages, challenges and objectives to the target.

Given the scale of the data sets used to train AI, companies are organising themselves **to ensure their quality and visibility at scale**.

2.2.2 TRAIN

Several organisations have set up training courses on generative AI systems, the new tasks/missions involved (e.g. prompt engineering¹), the risks, etc., or are directing their employees to online resources to raise awareness.

Teams launching data and AI projects need to be certain of the quality, origin and reliability of the data, and to understand the semantics and governance in place. All levels are affected. Data is often collected at the operational level, which is why it is so important to ensure that operational staff in particular understand the issues surrounding data (quality, completeness, etc.). AI models must be ethical and explainable. Finally, the product generated must provide value and meet the needs and strategy of the company or public administration.

Upstream training should also be integrated into academic and retraining courses.

2.2.3 ORGANISE

Some companies have set up a **cross-functional, multi-disciplinary committee**, also known as the "AI Tower", or "Generative AI committee", to monitor and validate the various use cases for generative AI and LLM in the company, as was done for data, and to keep recommendations and answers to FAQs (frequently asked questions) up to date. This multi-disciplinary committee often brings together staff from the cybersecurity, legal, product and information systems teams. It is a good practice for **building collective skills** and ensuring good visibility of internal actions. It also ensures that **the rules of conduct are kept up to date**. It is important to validate that the choice of suppliers and models are adapted to the uses (geographical location, immunity to extraterritorial laws), that the licences allow commercial use, and finally, that the service levels are compatible with the requirements, in short to measure the impacts before going into production.

One company, for example, has set up a multi-disciplinary task force, tasked with technology watch, working on use cases, demonstrators, risks and legal aspects, as well as awareness-raising and training. In this way, maturity is progressing collectively, by including different business lines, each of which is trialling its own approach.

2.2.4 INVOLVE HUMAN RESOURCES

Several companies have involved human resources in **identifying the new roles and missions** emerging with generative AI use cases (supervisors of bots and AI decisions, prompt engineers, etc.).

¹ Prompt Engineering is the process of designing and creating prompts, or input data, to drive AI to perform a specific task. This involves selecting the right type of data and formatting it so that the model understands and uses it. The aim is to create high-quality data to enable the AI to make accurate predictions and take the right decisions.

Human resources departments are also seeking to **identify the professions that will be impacted** by AI in order to anticipate the adjustments that need to be made or prepare for retraining. Indeed, while the message from those involved in these technologies is reassuring and emphasises the role of the super assistant (or co-pilot) in giving 'super powers' to employees, the efficiency gains promised by these technologies mean that we need to anticipate the possible consequences for a wage bill that has been relatively unaffected until now.

2.3 IDENTIFY USE CASES AND PERFORMANCE IMPROVEMENTS

All the firms in the market are trying to sell "their approach" to identifying good use cases, but players remain cautious about using these firms. Some organisations prefer to go it alone in their search for the "golden use cases" that could give them a major competitive advantage. This is why they choose either a top-down or a bottom-up approach.

Top-down approach: Some companies and public administrations are organising strategic reflections on the value chain and the possible uses of generative AI to generate use cases with generative AI systems. The idea is to work on business lines, customer offerings and business models.

Bottom-up approach: other organisations encourage employees to come up with ideas through experimentation. They then seek to identify those with high added value. To do this, some of them set up a multi-disciplinary task force (legal teams, AI factory, DPO) which identifies promising use cases, then analyses and finally tests them with the stakeholders concerned. Sharing feedback and ongoing experiments is a good way of stimulating serendipity among teams.

2.4 PUT IN PLACE PROCESSES TO INDUSTRIALISE USE CASES WITH GENERATIVE AI SYSTEMS

Companies that have set up a multi-disciplinary task force, with the benefit of monitoring and learning from the use cases currently being implemented, are establishing/constructing a framework to delimit the implementation of PoCs and to anticipate their successful industrialisation.

For example, one company has asked its developers to indicate their intention to use a generative AI tool, even before the first line of code is written, in order to assess the security of the project. Another systematically checks the quality and suitability of the data used before starting up. Yet another is seeking to determine indicators/criteria to assess the benefits, whether quantitative or qualitative, with the aim of making them sustainable throughout the organisation. Finally, one organisation has set up an internal ethics committee to assess the ethics of each project, analyse the potential for bias or erroneous results, and define the scope and functionalities of the product to be created, as well as the associated legal framework.

2.5 RAISE AWARENESS OF THE NEED FOR CAREFUL, REASONED USE

Most organisations are in favour of careful, reasoned use of these tools when it comes to handling sensitive data - financial, commercial, strategic, R&D and trade secrets - in order to guarantee confidentiality. This means informing employees of the potential risks depending on the classification of the data. Similarly, a certain amount of caution must be exercised when it comes to exploiting the results produced by these generative AI tools, to guard against analysis and processing errors, which are clearly not that uncommon. It is also essential to check that the processing of personal data is compliant with the RGPD when this type of tool is used for this purpose. Finally, particular attention needs to be paid to intellectual property and copyright issues, as some of these artificial intelligences may have been trained on extremely vast datasets without any robust guarantees in this area.

2.6 INCLUDE AN ENVIRONMENTAL IMPACT ASSESSMENT FROM THE OUTSET

Organisations are seeking to minimise the environmental impact and therefore to measure the CSR (Corporate Social Responsibility) impact of implementing AI. However, in the absence of collective maturity on the subject, they are rather powerless, even if they try to monitor and control the use of resources (storage, computing, for example). At this stage, suppliers are content with responses linked to their overall environmental policy.

2.7 TAKE STOCK OF SOLUTIONS AND SUPPLIERS

First of all, organisations are looking to identify the different players, test solutions in this fast-moving, teeming environment and compare them for benchmarking purposes. They study the risk of dependence on generative AI systems and the associated general terms and conditions of sale, in order to adapt them to their needs, if necessary. Data sensitivity is an important criterion in the choice of supplier. Companies identify existing models that are relevant to their use cases and adapt them with their data for their own cases. For example, some organisations have chosen to use LLM systems on a company instance without any link to the public version. Some companies choose suppliers who agree to work in synergy with their ecosystem.

Open source solutions, which are making very rapid progress, are of course among the solutions being evaluated. They are identified as solutions that do not take ownership of either customer data or results. However, companies first analyse the associated licence, and check who owns it. They also ensure that they can use these solutions for commercial activity.

Others are looking at the extent to which generative AI tools are subject to laws outside Europe and therefore potentially vulnerable to economic intelligence activities. An open source model hosted internally is a possible recourse for more sensitive use cases. On this subject, the CSF "*Numérique de confiance*" (Digital Trust) aims to help European solutions to mature, so as to ensure that users have a real choice.

Finally, some organisations are looking to identify solution providers who themselves use generative AI tools, and to analyse how these tools are used.

3 RISKS RELATING TO GENERATIVE AI SYSTEMS

During the workshop, we tried to identify the risks and listed them in the diagram below.

Risks associated with generative AI systems



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