Generative Artificial Intelligence (GenAI) Policy

Version	1
Version date	July 15, 2026

1. History

Version	Date	Description
1	20/05/2026	Document creation

2. Table of contents

1. HISTORY 1
2. TABLE OF CONTENTS 2
3. INTRODUCTION 3
3.1. Preamble 3
3.2. Objectives 3
3.3. Scope of application 3
3.4. References 4
3.5. Related documents 4
3.6. Abbreviations and definitions 4
4. GUIDELINES FOR THE USE OF GENERATIVE AI TOOLS 6
4.1. Acceptable Use of Technology 6
4.2. Data Protection and Privacy 6
4.3. Verification of GenAI Outputs 7
4.4. Transparency 8
4.5. Risks Related to Third Parties and the Use of AI 8
Transmission of Data to a Third Party 8
Use of a Third-Party Application Incorporating AI Features 8
Specific Case of Microsoft Copilot 8
4.6. Compliance with Laws and Policies 9
4.7. Reporting Policy Violations 9
4.8. Responsible Use and Digital Sobriety 9
4.9. Assistance with Documentation and System Validation 9
Drafting Support 9
Execution and Automated Decisions 9
4.10. Maturity and Regulatory Watch Clause 9
5. MONITORING 10
5.1. Non-compliance 10
5.2. Appendix 11
5.3. Examples of authorized and prohibited use cases for Microsoft Copilot and GenAI 11

3. Introduction

3.1. Preamble

As a reminder, any project falling within the DDSI scope must be formalized through a Project Charter and submitted to the relevant IT committee.

When the project includes artificial intelligence technologies, regardless of their form, a specific additional section must be completed and attached to the standard Project Charter in order to go through the IT demand management process and the AI Board.

3.2. Objectives

Generative AI (GenAI) refers to artificial intelligence technologies capable of creating new content (text, audio, videos, or images) based on a human instruction.

Mayoly's objective is to ensure the lawful, responsible, and secure use of generative AI (GenAI) technology.

This approach aims to ensure regulatory compliance, the protection of sensitive data belonging to the Mayoly Group, patient/customer data, as well as transparency and traceability of uses, while promoting controlled innovation to support business activities and limiting legal, ethical, reputational, and operational risks.

It is based on the **principle of human responsibility primacy**: GenAI tools are intended to assist employees, without ever replacing their judgment, particularly for sensitive or critical decisions.

This policy and AI-related practices will be updated regularly to ensure they remain aligned with technological developments, internal projects, regulatory and organizational requirements, and the level of maturity reached by the Mayoly Group in this area.

3.3. Scope of application

This policy applies to all employees of the Mayoly Group and its affiliates, as well as to third parties (service providers, partners, etc.) using Mayoly systems or having access to data belonging to the Mayoly Group or its affiliates.

The only AI tool authorized at Mayoly is Microsoft Copilot, when connected with a Mayoly Microsoft account. It is the solution approved by the DDSI and administered for the Mayoly Group. The use of Microsoft Copilot with a personal account or without being signed in is prohibited.

Any other AI tool (e.g., Claude, ChatGPT, Gemini, Mistral Vibe, DeepSeek, etc.) is strictly prohibited in the context of professional activities at Mayoly. It is also prohibited to install an AI application on a Mayoly PC other than Microsoft Copilot, even for personal use.

This policy covers all authorized uses of Microsoft Copilot within the Mayoly environment (i.e., connected with the Mayoly Microsoft account), whether based on Microsoft 365 licenses or Microsoft Copilot for Microsoft 365 licenses, as well as their use on workstations running a version of Windows that is compatible and approved by the DDSI. As available features may vary depending on the environment, the authorized scope of use depends on the assigned licenses and the settings approved by the DDSI.

3.4. References

Table 1: Regulatory references

ID	Regulatory text
[1] EU AI Act	European regulation governing the development, placing on the market, and use of artificial intelligence systems based on a risk-based approach.
[2] GDPR	European regulation governing the protection of personal data and individuals' rights.

3.5. Related documents

Table 2: Internal references

ID	Internal text
[3] Security Policy	Overall Information Systems Security Policy
[4] Notice GenAI	The principles of this AI policy are operationally set out in the "**GenAI Notice**" intended for employees.
[5] GDPR Policy	Mayoly policy on the processing of personal data

3.6. Abbreviations and definitions

Table 3: Abbreviations

Name	Abbreviation	Meaning
Artificial Intelligence	AI	Automated system capable of producing outputs such as predictions, content, recommendations, or decisions.
Generative Artificial Intelligence	GenAI	Category of AI that produces text, audio, images, videos, code, or other content.
Information System	IS	Organized set of resources (people, data, tools, and processes) used to collect, process, store, and disseminate information within an organization.
DPO	DPO	The Data Protection Officer is the person responsible for the protection of personal data within an organization. Mayoly Group's DPO is **Karine Renault**, from **Pharmarketing.**
Personal data		Any information that makes it possible, directly or indirectly and in any form whatsoever, including partially and/or encoded/pseudonymized data, to identify the natural persons to whom it relates (e.g., name, email address, etc.).
Sensitive data		Business data that may require special attention depending on its use, context, and the user's access rights (e.g., financial or strategic data).
Microsoft Copilot environment		Refers to all generative AI features integrated into Microsoft 365 services, including Copilot Chat, Outlook, Word, Excel, PowerPoint, Teams, and SharePoint.

Name	Abbreviation	Meaning
DDSI	DDSI	Digital and Information Systems Department of the Mayoly Group.
Third party		Refers to any entity external to Mayoly and its affiliates, including digital service providers, subcontractors, integrators, partners, and consultants.

4. Guidelines for the Use of Generative AI Tools

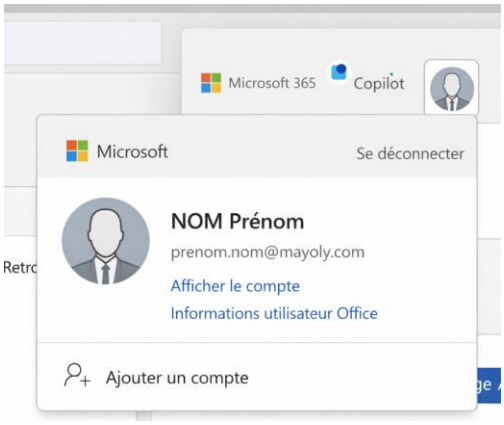
4.1. Acceptable Use of Technology

To maintain the security of our data and information systems, employees must comply with our overall Information Systems Security Policy and **use only Microsoft Copilot**, the only GenAI tool approved by the DDSI.

The use of Microsoft Copilot is authorized only when the following conditions are met:

- When signed in with a Mayoly Microsoft professional account:

In each application using Microsoft Copilot 365 (Word, Excel, PowerPoint, Teams, Outlook, etc.), as well as in Microsoft Copilot Chat via the Edge web browser, users must check, by clicking the profile icon in the top right corner, that they are signed in with their Mayoly professional account in the format *prenom.nom@mayoly.com*. The same applies to the Microsoft Copilot application installed on Mayoly computers.



- In compliance with the Mayoly Group's security and access management policies.

Employees must ensure that:

- Data processed by Copilot is accessible in accordance with existing access rights,
- No attempt is made to bypass the security, logging, or governance mechanisms implemented in the Microsoft 365 environment,
- Outputs generated by Copilot are used exclusively for a legitimate professional purpose.

Any use of Microsoft Copilot outside the Mayoly tenant scope (personal account, supplier account, unmanaged environment) is prohibited.

Employees are required to declare GenAI uses implemented in their professional activities and to report any deviation, incident, or doubt regarding the compliance of a use case. (See section 5.7)

When the need concerns professional content already accessible to the user in Microsoft 365 Mayoly, such content may be used in Microsoft Copilot or in a tool approved by the DDSI, when necessary for professional activities.

For recurring translation needs, employees who do not have access to an approved tool must request a solution validated by the DDSI or their management.

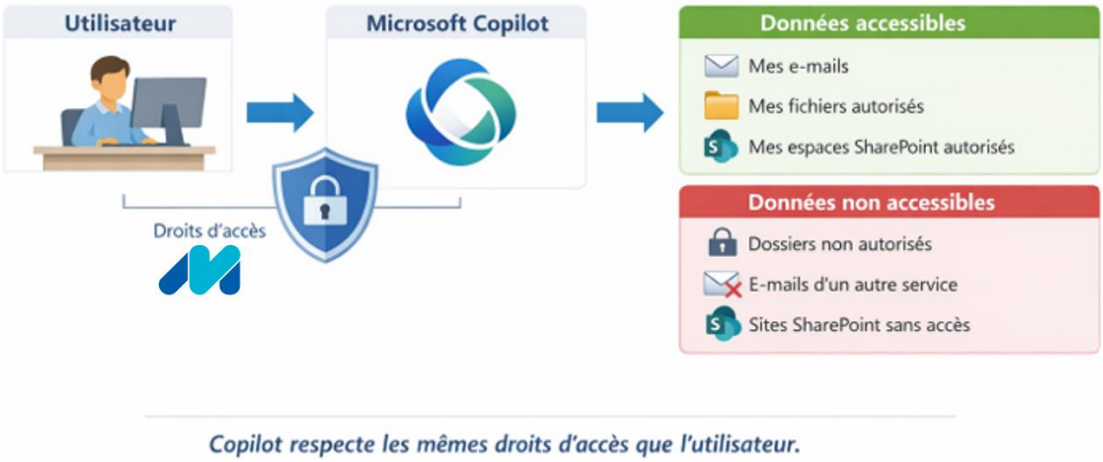
Authorized and prohibited use cases for Microsoft Copilot are detailed in the appendix **(see Appendix 8.1)**.

Any use not explicitly mentioned as authorized in this appendix is deemed prohibited or subject to prior validation by the DDSI.

4.2. Data Protection and Privacy

The use of Microsoft Copilot while signed in with a Mayoly Microsoft account takes place in a contractually and technically controlled environment. Mayoly Group business information, including personal, financial, strategic, or regulated data, **must not be entered into a public GenAI system** (ChatGPT, Claude, etc.).

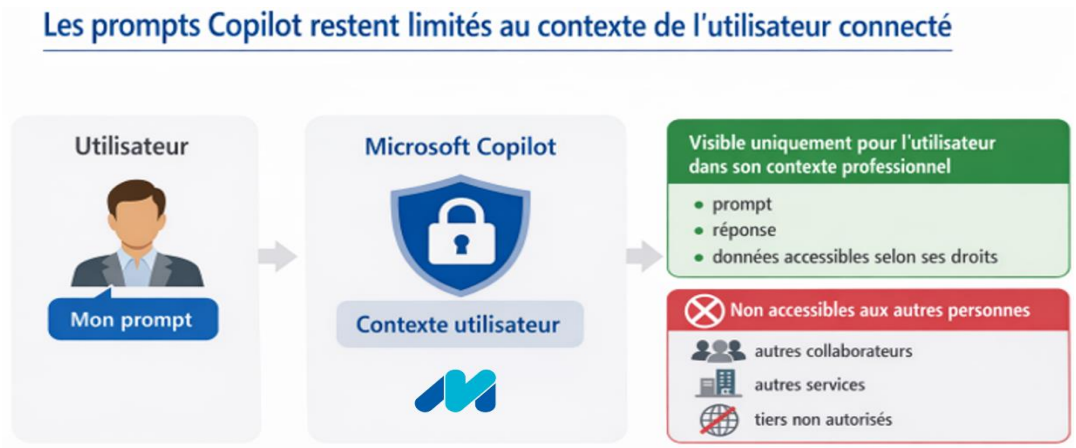
Microsoft Copilot only accesses data for which the user already has access rights within the Mayoly Group Microsoft 365 environment (for example: their own emails, documents, or SharePoint spaces they are authorized to access), in accordance with existing permissions and security rules.



In this respect, users must comply with the following principles:

- Copilot may be used with information to which the user already has access in Microsoft 365 Mayoly, when useful for their professional activity.
- The user must ensure that only the information genuinely required for the requested task is used in Copilot, in compliance with their usual access scope.
- No personal data may be processed or added in Microsoft Copilot without validation from the DPO.

It is also specified that the requests, known as "prompts," entered into Microsoft Copilot, as well as the responses generated in this context, remain linked to the personal context of the signed-in user and **are not accessible to other employees** under their usual access rights.



Microsoft Copilot must be used exclusively for professional purposes.

Any question regarding the nature of the data that may be used with Microsoft Copilot must be addressed to the DDSI support service by email at ddsi.support@mayoly.com.

As a reminder, the professional use of ChatGPT, Claude, Gemini, Mistral Vibe, DeepSeek, Microsoft Copilot Pro with a personal account, or any other GenAI service subscribed to under a personal subscription (and therefore not approved by the DDSI) is prohibited.

4.3. Verification of GenAI Outputs

To protect employees, partners, customers, and patients, and to protect the company against reputational harm, Microsoft Copilot users must verify the accuracy of outputs in order to avoid incorrect results (hallucinations), bias, and copyright infringements.

Employees remain responsible for the prior verification of content generated by Microsoft Copilot, to ensure its accuracy, legal compliance, and lawful reusability before any distribution or use in a professional context.

This verification also includes vigilance regarding potential bias, ethical impacts, and any consequences that may affect safety, compliance, health, or individuals' rights.

Content generated by Microsoft Copilot is considered **assistance content**. It must under no circumstances be used as-is for:

- Regulatory, medical, quality, pharmacovigilance, legal, HR, or similar decisions.
- External communications binding the Mayoly Group, without prior validation by a qualified person.

4.4. Transparency

In accordance with our Code of Conduct, we aim to provide our employees, third parties, customers, and patients with transparency regarding how we use Microsoft Copilot to support our work. To this end, when content has been mostly generated by AI without significant human modification OR when required by applicable law, employees and third parties must **indicate in the final material that Copilot was used.**

This transparency requirement is part of a broader approach to traceability of GenAI uses, making it possible to identify the tools used, the purposes pursued, and the associated responsibilities.

When Microsoft Copilot is used to produce content distributed outside the Group or having a regulatory, quality, or contractual impact, this use must be documented in accordance with internal traceability requirements and, where applicable, mentioned in the final materials when required by applicable regulations.

4.5. Risks Related to Third Parties and the Use of AI

The use of AI in relationships with third parties requires particular vigilance. Two situations in particular must be taken into account:

Transmission of Data to a Third Party

When a third party accesses Mayoly data as part of a service, it must be ensured that any potential use of AI technologies by that third party is contractually governed. Consequently, any engagement of a third party with access to Mayoly data must be subject to a prior review of contractual clauses and, where applicable, validation by the Legal Department in order to confirm the conditions for using or prohibiting AI.

Example: when an activity is outsourced to a service provider required to handle Mayoly data, the use of AI by that provider is prohibited until the contract and conditions of use have been reviewed with the Legal Department.

Use of a Third-Party Application Incorporating AI Features

When an employee uses, in the course of their professional activities, an application or service provided by a third party that includes AI features, such use may not take place without prior notification to the DDSI and the Legal Department. This approach aims to verify the contractual framework, terms of use, regulatory compliance, and associated risks before any activation or effective use of these features.

Example: if a CRM application used in a professional context offers AI features to assist the user, the DDSI and the Legal Department must be informed and must validatein advance in order to frame the use of these features with the supplier.

Specific Case of Microsoft Copilot

When used within **Mayoly's Microsoft 365 environment**, Microsoft Copilot is considered a solution already governed by the Group's contractual agreements and by the security mechanisms validated by Mayoly.

4.6. Compliance with Laws and Policies

All concerned parties must also comply with applicable laws, regulations, or company policies relating to the use or development of GenAI content or tools.

In particular, any use of GenAI that may affect safety, health, regulatory compliance, or individuals' rights must be subject to qualified human control and may not rely exclusively on automated processing.

4.7. Reporting Policy Violations

All concerned parties are required to report suspected policy violations, whether unintentional or intentional, to communication.cyber@mayoly.com. This will help ensure that any potential breach of confidentiality or other concerns are addressed promptly and effectively, thereby maintaining trust and the security of our data and systems.

4.8. Responsible Use and Digital Sobriety

As part of a corporate social and environmental responsibility approach, the Mayoly Group encourages the reasoned and relevant use of generative AI technologies.

Each prompt submitted to a GenAI tool mobilizes significant IT and energy resources. As such, employees are encouraged to:

- Systematically question the purpose, added value, and legitimacy of using GenAI.
- Avoid repetitive requests or requests without a clear professional objective.
- Favor structured and relevant prompts in order to limit unnecessary iterations.

The use of GenAI must therefore be part of a digital sobriety approach, in line with the Mayoly Group's CSR commitments, without compromising operational efficiency or the quality of deliverables.

4.9. Assistance with Documentation and System Validation

Generative AI is integrated progressively and in a controlled manner into validation life cycles, while maintaining a balance between innovation and regulatory compliance.

Drafting Support

The use of GenAI is authorized as an assistance tool for creating validation documentation, for example test plan drafts, test cases, or risk analyses. Any documentation generated in this way must be fully reviewed and validated by a CSV specialist, who assumes final responsibility through their signature.

Execution and Automated Decisions

- By default, AI may not be used to autonomously execute qualification tests or to decide alone on the compliance of a result (Pass/Fail) without systematic human control.
- The use of AI for automated decision-making or execution processes may be considered when:
  - The technology can demonstrate compliant repeatability and reliability.
  - The system has undergone a specific qualification demonstrating control of the risks of errors or deviations.

4.10. Maturity and Regulatory Watch Clause

The use of AI in processes directly impacting production remains subject to the evolution of the legal framework.

- As long as the European AI Regulation (AI Act) is not in force in its final version and the authorities (EMA/ANSM) have not updated GMP requirements, for example through a future Annex 22 or a revision of Annex 11, the use of AI for production-related validation is restricted to exploratory frameworks such as sandboxes.

- Any transition to automated use in production must be validated through a regulatory impact assessment and approved by Quality Assurance.

5. Monitoring

In accordance with the Group's security policies, Mayoly DDSI supervision systems could access and monitor the use of GenAI applications on any company-provided device in order to ensure compliant use of these systems.

The purpose of supervision and audit mechanisms is exclusively security, compliance, and the detection of non-compliant uses. They may not be used as a managerial monitoring tool or for individual employee assessment, except within a specific legal framework and with prior HR validation.

The use of Microsoft Copilot is subject to supervision, audit, and logging mechanisms integrated into the Microsoft 365 environment, in accordance with the Mayoly Group's security policies.

These controls are intended to ensure:

- Regulatory compliance,
- Data protection,
- Detection of non-compliant or risky uses.

5.1. Non-compliance

The user undertakes to comply with all applicable legislation relating to intellectual property, company confidentiality, the General Data Protection Regulation (GDPR), the AI Act, as well as all good practice rules. In this respect, no personal data, regardless of its form – direct, encoded and/or partial personal data – may be shared on Microsoft Copilot without validation from the DPO and is strictly prohibited under applicable legislation. For any necessary clarification, please contact the Data Protection Officer (DPO) via DDSI support at ddsi.support@mayoly.com.

Failure to comply with the rules and obligations set out in this Policy may expose the MAYOLY Group to liability, reputational harm and/or damage to the company's image.

Consequently, failure to comply with the rules set out herein, including those relating to personal data protection, may result in criminal and/or civil sanctions provided for by applicable laws and regulations, as well as disciplinary measures in accordance with MAYOLY's internal rules, up to and including dismissal.

5.2. Appendix

5.3. Examples of authorized and prohibited use cases for Microsoft Copilot and GenAI

Authorized uses (under human responsibility)	**Prohibited uses**
Rewording, correction, and stylistic improvement of professional content accessible to the user in Microsoft 365 Copilot provided by Mayoly.	Entering or processing professional content in a GenAI tool other than Microsoft Copilot connected with your Microsoft account.
Drafting internal non-regulated documents.	Automating regulatory, medical, quality, legal, or HR decisions.
Summarizing internal documents accessible according to the user's access rights.	Using Microsoft Copilot outside the Mayoly Microsoft 365 ecosystem.
Structuring ideas, outlines, or internal training materials.	Bypassing Information System security or access control rules.
Translating or linguistically adapting professional content accessible to the user using an approved tool.	Using unapproved public translation tools for professional content.
Summarizing email exchanges, notes, or professional documents accessible to the user in order to extract key points.	Summarizing professional exchanges via a personal account, personal subscription, or tool not approved by the DDSI.
Preparing presentation materials, slide outlines, or visual summaries based on professional content already available.	Producing presentations or materials intended for internal or external distribution without prior human review and validation.
Assisting with the analysis of tables or data to identify trends, summarize results, or suggest interpretation paths.	Using Microsoft Copilot to make a financial, regulatory, quality, medical, legal, or HR decision on its own.
Preparing meetings, generating agendas, taking notes, drafting minutes, and identifying actions based on information accessible to the user.	Using Microsoft Copilot to record, summarize, or exploit exchanges to which the user does not have access within their usual scope.
Drafting, rewording, or improving emails, Teams messages, or professional responses, while respecting the business context.	Sending messages, responses, or positions that bind Mayoly without appropriate verification or validation.
Searching for and summarizing internal information accessible to the user in Microsoft 365 Mayoly (documents, emails, authorized collaborative spaces).	Searching, aggregating, or attempting to access information not accessible to the user under their usual rights.
Creating simple visuals, illustrations, or supporting images for professional use, subject to human validation before distribution.	Creating or distributing misleading or unverified visuals, or visuals that may harm the Mayoly Group's image, rights, or obligations.
Organizing, classifying, and structuring notes, ideas, or work-related information to facilitate their reuse in a professional context.	Organizing or reusing work-related information for personal, unauthorized use, or use unrelated to professional activity.
Processing anonymized personal data that I am authorized to access as part of my professional activity.	Processing confidential, non-anonymized personal or HR data.

Rewording a job offer, HR email, or training material without personal data.	Analyzing emails, Teams messages, or minutes to assess engagement, loyalty, motivation, emotions, or performance.
Preparing interview templates, manager guides, or training materials.	Assisting with decisions on promotion, mobility, compensation, disciplinary action, dismissal, or succession.