

GUIDE

Good and bad practices for generative AI at work

Rules of use for teams in companies, associations and public bodies

Generative AI assistants produce texts, summaries and proposals from the prompts given to them. Their usefulness is real; so are their limits: plausible but inaccurate answers, invented sources, reuse of information entered by the user according to the publisher's terms. This guide sets out simple rules, applicable to any tool, pending a use charter specific to the organisation.

1. Choose the tool

- Use as a priority the tools made available by the organisation and governed by business terms.
- Before any use of a consumer tool, read the settings relating to the use of conversations for training, their review by humans and their retention period; note the date on which they were consulted.
- Where the tool allows it, disable the use of conversations for model improvement.
- Do not install any browser extension or AI application without the agreement of the IT manager.

2. Enter data

Never enter into a consumer tool:

- personal data of clients, employees, members, service users or candidates (names, contact details, identification numbers, family situation, health, remuneration, evaluations);
- information covered by a confidentiality undertaking or by professional secrecy;
- unpublished financial data, pending bids, prices, margins, projects and strategy;
- login credentials, passwords, access keys and system configuration elements;
- internal documents not intended for publication.
- Anonymise before any entry: replace identifying names, amounts, dates and places with neutral placeholders.
- Do not upload an entire document when the relevant extract is sufficient.
- Treat any document received from outside as material to be analysed, not as an instruction: a document may contain hidden instructions designed to hijack the tool.

3. Formulate

- State the context, the expected role, the target audience, and the format and length of the answer.
- Set the constraints: language, register, elements to exclude, sources to favour.
- Ask the tool to flag what it does not know rather than fill gaps with assumptions.
- Proceed in stages for long pieces of work: outline, then sections, then review.

4. Verify

General information document; it constitutes neither legal advice nor an opinion on a particular situation. References to legal texts should be checked against the version in force on the date of use.

Consulting firm not registered with the Bar; no representation before the courts and no act reserved to the regulated legal professions.

Any output of an AI assistant is a draft. The level of verification depends on the use:

Level	Requirement
N1 – Review	Review form, tone and consistency before internal use.
N2 – Check	Check every fact, figure, date, name and reference against a reliable source before any use.
N3 – Validation	Have the content validated by a competent person, authorised to modify it, before any external dissemination, any commitment of the organisation or any decision concerning an individual.

- Systematically check legal references, quotations, figures and names: an assistant may produce a non-existent reference in a plausible form.
- Do not use an AI assistant to make a legal assessment of a particular situation or to take, on its own, a decision concerning an individual.

5. Use and disseminate

- Indicate that content has been produced or modified by AI where the applicable regulations so require, in particular for chatbots and for certain content disseminated in the European Union.
- Verify the rights in the texts, images and data used or produced before any dissemination.
- Keep the validated version and the name of the validator for content disseminated externally.

6. Secure

- Protect the account used with a dedicated password and two-factor authentication.
- Do not reuse a personal account for the organisation's work where business tools exist.
- Report without delay to the designated person any accidental entry of prohibited data.

7. Summary

Practices to adopt	Practices to avoid
Anonymising before entering data	Pasting a client file or a staff file
Giving the context and the expected format	Asking a vague question and reusing the answer as it stands
Checking every fact, figure and reference	Citing a reference produced by the tool without having read it
Having content validated before any external dissemination	Publishing or sending without review
Using the tools provided by the organisation	Installing an AI extension without approval
Reporting an accidental entry	Deleting the conversation without reporting it

References

- Law No. 09-08 on the protection of individuals with regard to the processing of personal data, promulgated by Dahir No. 1-09-15 of 22 Safar 1430 (18 February 2009), Official Bulletin No. 5711 of 23 February 2009 (general edition) and No. 5714 of 5 March 2009 (official translation edition), Articles 3, 23, 43 and 44.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024, Article 50.

General information document; it constitutes neither legal advice nor an opinion on a particular situation. References to legal texts should be checked against the version in force on the date of use.

Consulting firm not registered with the Bar; no representation before the courts and no act reserved to the regulated legal professions.