

Intellectual professions and the use of AI

Checklist pursuant to
Article 13, Law 23 September 2025, No. 132
on Artificial Intelligence

Intellectual professions and the use of AI

This checklist is a **practical tool** designed to help professionals conduct a self-assessment to **verify compliance with Article 13 of Law No. 132 of 23 September 2025** (“Provisions and delegations to the Government regarding Artificial Intelligence”).

Article 13 introduces, for the first time in the Italian regulatory framework, specific principles governing the use of artificial intelligence in intellectual professions.

The questions included focus on key aspects under **Article 13 of the AI Law**: from client disclosure to the predominance of intellectual work, the protection of professional secrecy, and cybersecurity.

This checklist aims to help professionals:

- **understand** the requirements imposed by national legislation;
- **assess** their operational practices in terms of transparency, trust, and correct use of AI tools;
- **adopt** good governance and communication practices consistent with the ethical and legal principles of the profession.

Final note: Proper compliance with Article 13 may require technical expertise. Therefore, some assessments may need to be supported by qualified IT professionals.

The checklists and contents herein are the result of research, analysis,
and the experience of the 42 Law Firm team.

Use of these materials is permitted solely for personal or internal purposes; any dissemination, modification, or commercial use without authorization is prohibited.

Issues to consider

P.1	Transparency and support for professional activity
P.6	Protection of the fiduciary relationship
P.8	Protection of minors and sensitive content
P.11	Professional secrecy
P.12	Cybersecurity

Transparency and support for professional activity

question

Is AI used only as a support tool to the professional's main activity?



Article 13(1) specifies that AI must serve solely as a support tool, not as a replacement for human work, ensuring the prevalence of intellectual contribution.



examples

An architect uses an AI system to generate layout proposals or simulate natural light, but develops the final design personally.

A lawyer may use AI to analyze case law and identify precedents, but personally drafts the defense strategy and procedural documents.

Transparency and support for professional activity

question

Does the final decision always remain human in processes that affect people's rights (e.g., whether to initiate legal proceedings)?



AI must remain a support tool, with effective human oversight, the ability to intervene, and decision traceability.



examples

A lawyer uses AI to analyze case law on damage compensation but autonomously decides whether to bring the case to court based on professional judgment and the client's real interest.

A notary may rely on AI for formal checks but personally verifies the legal validity and parties' intent before signing.

Transparency and support for professional activity

question

Is the client informed that AI systems are used during the professional service?



Article 13(2) of Law 132/2025 requires clear, simple, and comprehensive disclosure to clients regarding AI tools used, in order to protect trust in the professional relationship.



examples

A lawyer using AI for legal research adds a "How we use AI" section on their website or provides an information sheet detailing which tools are used and for what purposes.

An architect explains that the initial concept was AI-generated, but the final design remains the result of personal creative work.

Transparency and support for professional activity

question

Is the AI disclosure provided before starting the professional service?



The client must be able to evaluate the use of AI before assigning the task. Ex-post disclosure violates the principles of transparency and trust.



esempi

A lawyer begins a case in September 2025 and uses AI during the process to analyze contracts. However, they inform the client only in December, upon delivery of the final work.

A doctor using AI for automated reporting explains how it works one month before the patient's appointment — this complies with transparency.

Transparency and support for professional activity

question

Which AI system is used in your professional practice (e.g., generative or predictive)?



Article 13(2) requires professionals to communicate information about AI systems used in a clear and comprehensive manner.



examples

A doctor employs predictive AI to estimate cancer recurrence risk based on clinical and biological data.

An architect uses generative AI to develop graphic concepts, keeping prompts and drafts as part of the project file.

Clarification:

- **Predictive AI:** analyzes historical data to identify recurring patterns and make forecasts about future events (e.g., clinical recurrence risk or litigation success probability).
- **Generative AI:** creates new content — text, images, designs, or models — from user-provided data or instructions, simulating human creative or linguistic processes.

Protection of the fiduciary relationship

question

Do engagement letters or contracts clearly state that final professional responsibility lies with the professional, not the AI system?



It is essential for clients to understand that responsibility always lies with the professional. This reinforces trust as required by Article 13(2).



example

A clause may state: "AI systems may be used for support or ancillary tasks. Final professional responsibility remains with the professional."

Protection of the fiduciary relationship

question

Have you established ways for clients to ask questions about AI use?



Trust requires not only information but also open dialogue, ensuring clients fully understand how AI is used and what safeguards exist.



example

A labor consultant using AI provides a contact person or technical documentation for client inquiries.

Protection of minors and sensitive content

question

If your work involves minors or vulnerable individuals, have you implemented specific notices and safeguards?



Using AI with minors under 14 requires parental consent and simplified, understandable language.



examples

A psychologist using AI for educational assessments provides illustrated notices to parents and simplified versions for children.

A family lawyer anonymizes data when using AI for child protection cases.

Protection of minors and sensitive content

question

Does the AI system process, even indirectly, sensitive content?



Processing sensitive content (judicial, health, or biometric data) requires reinforced human control and technical safeguards per Articles 9–10 GDPR.



example

A lawyer representing a sexual assault victim never uploads sensitive materials to online generative AI tools, using only encrypted, local systems with restricted access.

Protection of minors and sensitive content

question

When using AI for high-risk tasks (e.g., diagnostics), is the client informed in greater detail?



Where errors can have significant consequences, professionals must provide enhanced disclosures specifying system limits, checks, and supervision.



example

A doctor informs patients about verification steps or known system error margins.

Professional secrecy

question

Are adequate measures in place to ensure professional secrecy when using AI systems, particularly cloud-based ones?



Under ethical rules, intellectual professions must maintain confidentiality and protect all handled information.



example

Before processing, the professional anonymizes data, trains staff on data breach prevention, chooses encrypted platforms, and signs confidentiality agreements with cloud providers.

question

Have you implemented security controls throughout AI use — including testing, audits, and hardening procedures to prevent data abuse or manipulation?



Cybersecurity is a fundamental prerequisite for AI reliability. Professionals must adopt measures ensuring resilience against unauthorized access, data alteration, or model tampering.



example

A consulting firm using AI for document analysis applies a secure-by-design approach: end-to-end encryption, periodic penetration tests, and access logs to detect anomalies.

question

Have you developed an incident response plan defining roles, timing, and communication procedures in case of security breaches, model drift, or data compromise?



Incident management is integral to AI security. Systems must be continuously monitored, and professionals must be ready to promptly mitigate issues like data poisoning or intrusions.



example

A lawyer using AI for document drafting maintains an incident response playbook: upon detecting anomalous access, the system is suspended, and the IT officer notified.



For further information or to request
professional support:

info@42lf.it



www.42LF.it