

AI Charter

Why We Have an AI Charter

AI transforms how we deliver value, creating opportunities for every employee to engage in more strategic, creative, and fulfilling work. As AI systems augment, improve upon, and take over routine tasks, our people can focus on what we do best: strategic thinking, creative problem-solving, building client relationships, and providing the judgment and oversight that AI requires to be effective. At the same time, it's important to understand that uncontrolled use of these technologies can expose our clients, our firm, and our colleagues to real risks, including data breaches, inaccurate content, copyright violations, and reputational damage.

The Atos AI Charter establishes a clear framework for responsible and ethical use of AI. It aligns with the Atos Group AI Policy and supports compliance with regulatory frameworks and standards including the EU AI Act, GDPR, and ISO 42001.

The charter exists to:

- Protect our clients by prioritizing data security and strengthening the quality of our deliverables.
- Protect our firm by governing the use of AI according to our values, principles, and risk profile.
- Demonstrate responsible AI practices to clients, colleagues, and external stakeholders.
- Empower our employees to innovate with AI following clear, practical guidance.
- Support regulatory compliance efforts across our business.

This charter applies to all Atos employees, contractors, and partners involved in the development, deployment, use of, or interaction with AI systems—whether for our internal operations, service delivery, or customer solutions.

Guiding Principles

The following principles should consistently guide all of our long-term thinking and day-to-day decisions and actions as we engage with AI technologies:

- **Human-Centricity:** In our work with AI systems, we prioritize human needs, values, and well-being. The AI systems we deploy should enhance human abilities, ensure human control, and deliver equitable outcomes.
- **Transparency & Explainability:** The AI systems we build and deploy should be transparent about their operations. This includes disclosing when AI is being used, explaining the logic behind decisions, and enabling users to challenge outcomes.
- **Data Protection & Privacy:** AI systems should protect personal and sensitive information, comply with relevant legal requirements, and employ robust security measures by default to prevent data breaches.
- **Security & Resilience:** AI systems should include robust protection against adversarial threats and security risks by default. This includes secure coding practices, threat modelling, and prevention measures throughout the AI lifecycle.
- **Intellectual Property:** In our work with AI systems, we respect intellectual property rights. We do not use copyrighted materials without authorization, and we work to ensure AI-generated content does not infringe on existing rights.
- **Fairness & Inclusivity:** We develop and deploy AI systems that strengthen diversity, equity, inclusion, and accessibility. We prioritize the mitigation of harmful biases, fair treatment for affected stakeholders, and accommodation of diverse needs and perspectives.
- **Environmental Responsibility:** We develop, deploy, and use AI systems with a mindset of environmental stewardship and sustainability, making thoughtful decisions wherever possible to reduce environmental cost and impact.
- **Risk Awareness:** We assess AI systems and use cases according to their potential for negative impact. We understand that higher-risk systems require stronger governance, oversight, and control measures, in line with regulatory requirements and standards.
- **Compliance:** We build and deploy AI systems in compliance with all relevant laws and regulations, including the EU AI Act, applicable data protection legislation, internal AI policies, and ethical AI standards.

Guidelines for Engaging with AI

Atos employs a range of technology and process controls to enforce policy and reduce risk related to AI, however, employee cooperation is essential for the success of our Responsible AI efforts. Atos employees are expected to follow these guidelines when engaging with AI:

- **Engage Authorized Tools**
Employees are only permitted to use AI tools and use cases authorized by Atos following our documented review and approval processes. Employees are expected to pursue innovation and client value without engaging in “shadow AI.”
- **Protect Confidentiality in AI Training and Use**
Express clients approval is required before employees use client data, personally identifiable information, intellectual property, or otherwise sensitive content with AI tools. Employees may also only use customer data for AI training if they have prior customer consent.
- **Respect Intellectual Property and Copyright**
Employees are not permitted to use prompts that directly request or indirectly suggest copyrighted characters, protected styles, or other trademarked content.
- **Systematically Verify All AI-Generated Content**
Employees are expected to rigorously review AI-generated content, cross-referencing facts and mitigating inaccuracies and biases when such content could result in business risk, detriment to people’s well-being, or other harm.
- **Inform Clients and Ensure Transparency**
Employees are expected to practice full disclosure, explainability, and clear labeling of AI-generated content, agentic AI engagement, and other use of artificial intelligence as standard practice, especially in the context of high-risk and highly regulated use cases.
- **Monitor and Report Incidents**
As a matter of standard practice and good AI governance, employees are expected to immediately report any AI issues (data leaks, meaningful inaccuracies, misuse, etc.) that might result in unforeseen costs, brand damage, or other harm to Atos or our clients.
- **Consider the Environmental Impact of AI**
Employees are expected to practice responsible, energy-efficient use of AI whenever possible as part of Atos’ commitment to environmental responsibility and responsible AI practices.