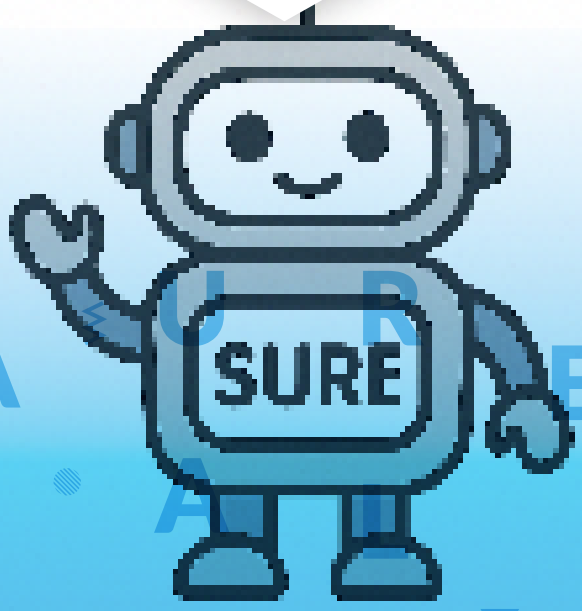
LAUREA

AMMATTIKORKEAKOULU
University of Applied Sciences



LAUREA LONG 16 | 2025

Jelte Van Barneveld, Joni Kivelä, Tommi Koivunen, Johan Mounier,
Emilia Rämö & Annemari Kuhmonen

Responsible AI in Action: A Practical Guide for SME Exporters

Co-funded by
the European Union

Abstract

In this international student project, different aspects of responsible generative AI were explored using the SURE Bot as a case example. The SURE Bot, co-developed by Laurea University of Applied Sciences and AI Think, is a foresight tool designed to support Finnish small and medium-sized businesses in export markets. At the time of the project, the bot was being developed and transformed from a proof of concept (PoC) into a minimum viable product (MVP). AI service design was used as the main methodological framework.

The bot was evaluated from ethical, secure, and sustainable perspectives, with particular attention to its usability in scenario building and strategic foresight. The concept of AI service promise was also examined. Agile teamwork supported the process. As a result, a development concept was created to strengthen the SURE Bot's value for SMEs operating in uncertain environments. The project supported the development of future-oriented professional skills.

This project was completed as part of the SURE (Performance, Resilience and Vitality through Continuous Workplace Learning) RDI initiative (ESR+), funded by the European Social Fund and the Häme Centre for Economic Development, Transport and Environment.

Keywords: generative AI, AI service design, AI service promise, responsible AI, ethical AI, secure AI, sustainable AI, scenarios, strategic foresight, SME, exports

Responsible AI in Action: A Practical Guide for SME Exporters

WHAT DOES IT really mean for a small business to use generative AI responsibly? A student team at Laurea University of Applied Sciences explored this question as part of an international project. They investigated the ethical, legal and sustainable dimensions of AI adoption. Their research focused on the SURE Bot, a generative-AI tool co-developed by Laurea UAS and the company AI Think. Designed to support strategic foresight, the SURE Bot helps Finnish export-oriented SMEs create future scenarios and prepare for change in an increasingly complex global operating environment.

As generative AI becomes a key driver of innovation and efficiency, adopting it responsibly is no longer optional. To fully benefit from these technologies, businesses must understand what generative AI is, how it is delivered, and what to consider before integrating it into daily operations.

GENERATIVE AI AND SOFTWARE AS A SERVICE: WHAT SMES NEED TO KNOW

Most SMEs rely on ready-made AI tools developed by external providers. These include general-purpose applications like OpenAI's ChatGPT or Microsoft's Copilot, as well as more specialized solutions built on top of large language models. Large language models (LLMs) are AI systems trained on vast amounts of text data, enabling them to generate human-like responses, summarize content, and support complex reasoning tasks. (Microsoft 2024.)

Generative AI refers to a form of artificial intelligence capable of producing new content, such as text, images, or music, by learning patterns from existing data. Instead of repeating stored information, generative AI generates new, original outputs in response to user prompts. (Microsoft 2024.) In this article, the term "provider" refers to companies offering such tools.

These ready-made tools are typically delivered as Software as a Service (SaaS), meaning they can be accessed online without the need for installation or technical expertise. In the SaaS model applications are hosted by the provider and made available to users over the internet, eliminating the burden of local maintenance. (Rivers 2024.)

The student team identified five key areas that SMEs should consider for responsible adoption of generative AI:

1. Evaluating the AI provider's service promise
2. Understanding how AI works
3. Ensuring ethical use
4. Securing data and systems
5. Minimizing environmental impact

This article offers practical guidance in each of these areas to help SMEs make informed choices when integrating generative AI into their strategies and operations.

AI SERVICE PROMISE – BEING CLEAR ABOUT WHAT THE TOOL CAN REALLY DO

Before choosing an AI tool, it's important for SMEs to stop and ask: *What does this tool promise to do? Can I trust that promise?* This is what we mean by a service promise, a clear and honest description of what the AI tool is designed to deliver. A well-crafted service promise sets expectations and builds trust between the provider and the user.

In practice, a service promise should be simple and easy to understand. It tells who the tool is for, what problem it solves, and what kind of benefits it offers. It also explains how the tool works and what the user needs to do. These are the basics that help SMEs decide if a tool is the right fit for their business. (Blomster, Kurtti, Määttä & Sinisalo 2020.)

WHAT MAKES A GOOD AI SERVICE PROMISE?

- Who is this for?
- What problem does it solve?
- What are the benefits?
- How can it be used?
- What does the user need to do?
  (Blomster et al. 2020.)

If a service promise is unclear or unrealistic, it can damage trust quickly. In the digital world, negative experiences spread fast. That's why companies need to be clear and honest about what their AI tool can and cannot do. And that's why it's better to promise a little less and deliver more, not the other way around. Storytelling can also help explain these promises in a more relatable and emotional way (Blomster et al. 2020, 78; Kalliomäki).

Trust is a critical enabler of successful AI adoption. Afroogh, Akbari, Malone, Kargar & Alambeigi (2024) emphasize that accuracy, reliability, transparency, and explainability are key pillars for building trust in AI systems. Without these, users are less likely to fully adopt or effectively utilize AI solutions, especially in small and medium-sized businesses where resources to verify AI performance independently may be limited.

One way to strengthen trust in practice is through transparent and user-centered tool design. When users understand what an AI tool can and cannot do, their expectations stay realistic, and confidence grows. (Afroogh et al 2024.)

A real-world example reinforces this lesson: Microsoft's Copilot was launched as a groundbreaking productivity assistant, but generated mixed user reactions when expectations were not fully met. This highlights how realistic, clearly communicated service promises are essential for credibility and adoption, especially in the rapidly evolving AI landscape. (Apple 2025; Warren 2025.)

EXAMPLE IN PRACTICE: THE SURE BOT

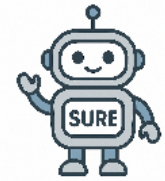
To demonstrate how the principles of responsible generative AI apply in real-world context, this article introduces the SURE Bot, co-developed by Laurea UAS and the company AI Think as a recurring example. The SURE Bot is a strategic foresight tool based on generative AI, designed specifically for export-oriented SMEs, including those with little or no previous experience in foresight or AI adoption.

WHAT IS THE SURE BOT?

- A strategic tool for SMEs to anticipate changes in the global operating environment. Identifies macro-level trends and drivers of change.
- Supports exploration of topics such as the green transition, sustainability, geopolitical shifts, and technological disruption.
- Helps build alternative future scenarios.Does not make decisions or create strategies for the user. Keeps the human insight and company vision at the center.

Accessible at: www.suremalli.fi.

The SURE Bot's service promise is clear and realistic: it supports SME users in exploring external changes and building future scenarios but does not replace human judgment or strategic planning. It is designed to be easy to use, even without technical expertise, helping users reflect on key drivers of change rather than predict the future.



Example 1: What the SURE Bot Offers

- Helps SMEs create scenarios.
- Promotes reflection over prediction.
- Supports thinking, doesn't deliver strategies.
- Easy to use, even without prior AI or foresight expertise.

For generative AI tools, the provider must be honest about what the tool can do. And the SME must ask the right questions. A clear service promise is the first step toward responsible AI use. Next, we will explore another critical aspect: knowing how the AI tool works.

AI LITERACY – KNOW WHAT YOU'RE USING

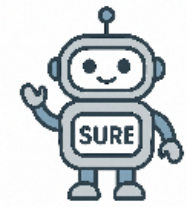
Before adopting and AI tool, SMEs must understand more than what it promises, they must know how it works. In just a few years, tools like GPT-3 have transformed how people and businesses access and use information. As

generative AI-generated content becomes more common, it's important to understand how these tools work and how to use them in a responsible way.

In this article, we use the term AI literacy as defined in the EU AI Act (Regulation EU 2024/1689). The regulation emphasizes users' ability to understand how AI systems function, how to use them responsibly, and what legal responsibilities are involved.

According to Blythe, Cuyvers & Bruynseraede (2024), the AI Act introduces a specific "AI literacy" obligation under Article 4, requiring organizations to ensure that their staff possess the necessary skills and knowledge. This includes understanding the risks, limitations, and intended use of AI tools. AI literacy is no longer a "nice-to-have", but a legal necessity for businesses operating in the European market.

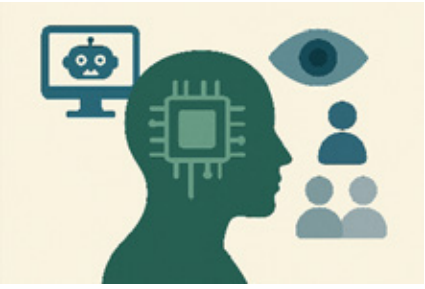
But beyond regulatory requirements, improving AI literacy also plays a crucial role in building trust in AI systems. Gillespie, Lockey, Curtis, Pool & Akbar (2023) found in a global study that individuals who understand AI are significantly more likely to trust and accept it. Their findings also showed that 82% of people want to learn more about AI, emphasizing the urgent need for AI literacy initiatives that are not only regulatory but empowering.



Example 2: How the SURE Bot Builds AI Literacy

- Shows how prompts affect responses, helping users experiment and learn.
- Clarifies what data is used and what the model is trained on.
- Emphasizes the role of human input.
- Builds user confidence, even without technical expertise.
- Encourages critical thinking over blind trust in AI.

AI literacy means more than technical skill. It is about curiosity, critical thinking, and strategic awareness. SMEs don't need in-house data scientists, but they do need staff who can ask smart questions and evaluate the tools critically.(Pinski & Benlian 2024; Deuze & Beckett 2022.)



DO YOU UNDERSTAND HOW TO USE AI WISELY IN YOUR BUSINESS?

Ask yourself:

- How does the AI create content or suggestions?
- What data does the tool rely on?
- Where is human oversight still essential?
- What risks might come from bias, errors, or over-reliance?
- Is the tool guiding or replacing professional judgement?

Under the EU AI Act (Regulation EU 2024/1689), which came into effect on February 2, 2025, all companies that build or use AI tools, whether made in-house or bought from others, must ensure their staff know how the systems work. This includes training, raising awareness about risks, and being clear about how the AI is used.

Most SMEs use tools created by others, but they still have legal duties. If your company uses AI, you are seen as a "deployer" under the law. This means you must understand who is affected by the AI, how it uses data, and whether it treats people fairly and openly.

ARE YOU READY FOR THE EU AI ACT? KEY QUESTIONS FOR SMES

- Have your employees received training on how the AI system works, including its purpose, risks, and limitations?
- Do you know who is affected by the tool (e.g. employees, customers, or partners), and is it fair and accessible for everyone using it?
- Are you confident that the tool handles personal data responsibly and fully complies with GDPR and other privacy regulations?

AI is changing how companies work. But with those changes come real risks. Misuse, bias, and unfair results can happen if tools are used blindly. Marr (2020) writes that companies must take the lead in using AI responsibly. Trust in AI depends not just on better tech, but also on clear rules that protect people and data.

In the long run, companies that understand AI will be better prepared for future changes. When AI is used in scenario planning or supply chains, you need to know how it works to get the most from it. (Marr 2020.)

To put it simply: knowing how AI works, and where its limits are, is the first step in using it wisely. That knowledge helps businesses make smart choices and adapt to change.

Next, we'll look at how to make sure those choices are also ethical.

ETHICAL AI – IS YOUR AI FAIR?

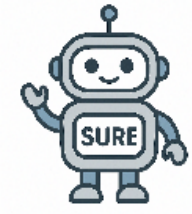
As AI tools become part of daily work, ethics is no longer just a theoretical concept. For SMEs, responsible AI means choosing solutions that do not unintentionally exclude, mislead or discriminate. Fairness, transparency, and inclusivity must be designed into AI from the start, not added later.

AI systems impact real people. The way they are designed, trained, and applied can have significant real-life consequences. Over time, AI may contribute to solving big global problems like climate change or conflict, while also improving productivity and decision-making. (Rusanen, Nurminen, Raisanen, Tarkoma & Halmetoja 2025.)

Ethical AI is a growing field focused on ensuring that technology serves the common good. This includes the entire lifecycle, from research and design to procurement, deployment, funding, and daily use. As AI begins to shape decisions that affect people's lives, the urgency of ethical thinking increases. (Rusanen et al. 2025.)

One globally recognized reference is UNESCO's (2021) Recommendation on the Ethics of Artificial Intelligence, which calls for AI systems to be understandable, just, and equitable across diverse populations. These global ethical guidelines align closely with the practical needs of SMEs aiming to adopt AI responsibly.

A key pillar of ethical AI is transparency. This means users should know how the AI system works, what data it uses, and how it makes decisions. Under The General Data Protection Regulation (GDPR), companies are already required to explain how they collect, process and share personal data (Rusanen et al. 2025). Transparency is also essential for risk management. SMEs must anticipate how AI decisions could affect users and ensure those outcomes are fair. (Vähä-Sipilä 2021.)



Example 3: How the SURE bot reflects Ethical AI

- Does not collect personal data, lowering privacy risks.
- Clearly states that it is an AI assistant.
- Avoids overpromising — offers guidance, but does not decide.
- Designed for easy to use regardless of background or digital skills.
- Brings strategic foresight tools accessible for all SMEs.

Ethical AI also means inclusion. Everyone should be able to benefit from modern AI tools, regardless of gender, geography, language or digital skills. But access is not always equal. For example, UNESCO (2023) found that men are up to four times more likely than women to possess advanced digital skills. True inclusion means recognizing these gaps, when designing, training, and deploying AI. (UNESCO 2023.)

Inclusion is not only about language interfaces or user guides. It's also about ensuring that training data reflects diverse real-world experiences. Tools that only serve majority groups risk reinforcing biases, marginalizing users, or producing flawed outcomes.

Fairness means treating everyone equally and must be a core principle in AI development. When AI systems make decisions, those decisions must be free from bias. However, bias can easily creep in if the training data is poor in quality, incomplete, or reflects only one group's perspective. Systems should avoid using pre-classified or sensitive data that might reinforce social stereotypes or discriminatory patterns. (ICO 2023.)

Ethics isn't just about good intentions. It requires clear principles and measurable action. As the AI Ethics Impact Group (Hallensleben, Hustedt & al. 2020) argues responsible AI must be backed by indicators, such as transparency, accessibility, and dataset diversity. These indicators help SMEs ask the right questions and choose the right tools.

ETHICAL AI CHECKLIST FOR SMES

Fairness
- Does the tool treat all users equally?
- What measures are in place to reduce bias?

Transparency
- Is it clear how the AI works and what data it uses?
- Do users know when they are interacting with AI?

Inclusivity
- Is the tool designed with diverse users in mind?
- Does it consider gender, age, culture, language, and access?

Next, we'll explore how to protect your business and your users through strong AI security and privacy practices.

SECURE AI – PROTECTING PEOPLE AND DATA

Today's SMEs face growing responsibilities: protecting data, maintaining trust, and reducing environmental impacts. Generative AI offers powerful ways to work smarter, anticipate change and operate more efficiently. But with these new capabilities come new responsibilities. Whether AI is used for customer service, strategic foresight, or scenario building, data protection must remain a core priority.

Using AI responsibly is no longer just an IT decision. It's about preserving credibility and brand trust. Mishandling personal or sensitive business data can lead to severe regulatory fines, legal actions, reputational damage (SentinelOne, 2024; OECD, 2024).

THE HIDDEN SECURITY RISKS SMES MUST MANAGE

While AI offers significant advantages for SMEs, it also introduces new layers of vulnerability. Many of these risks remain hidden until a breach, compliance failure, or ethical problem brings them sharply into focus. Understanding these potential pitfalls is critical for SMEs seeking to deploy AI solutions responsibly and sustainably. Below, we explore the key security risks that require proactive management.

Data breaches: A growing threat

One of the biggest risks for SMEs using AI tools is data breaches. If a tool stores or processes sensitive information and gets compromised, it can harm both the users and the business relying on the tool. That is why it is essential for SMEs to choose AI solutions that follow strong security practices, such as encryption, access control, and regular testing.

It's also important to ensure that the AI tool respects privacy from the start by using methods like data minimization and anonymization. (NTT Data 2024; Secure Privacy 2024)

Regulatory non-compliance

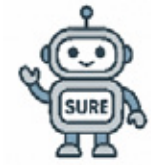
Another big challenge is compliance with regulations. In the European Union, rules like GDPR and the EU AI Act create high standards for how AI systems should treat user data (EQS Group 2025).

Supply chain and third-party risks

Many AI systems rely on third-party datasets, cloud platforms, or APIs. Weaknesses in these external components can expose SMEs to unexpected vulnerabilities.

Model security risks

Advanced AI systems are vulnerable to attacks such as model inversion, where sensitive data can be reconstructed, and data poisoning, i.e. corrupting training data. SMEs must ensure that providers have defences against these emerging threats.



Example 4: How the SURE Bot Minimizes Risks

- **Collects no personal data and avoids profiling**, minimizing GDPR exposure.
- **Does not track user activity**, reducing risks of unintended data capture.
- **Built with GDPR compliance and EU AI Act alignment**, ensuring lawful processing.
- **Emphasizes explainability**, supporting transparency and user control.

Why this matters: These design choices protect SMEs from legal liabilities, foster customer trust, and position the business for long-term credibility.

Bias, fairness, and unintended harm

There's also an ethical dimension SMEs should be aware of when choosing AI tools. These systems can influence real-world decisions. If a tool is built on biased data or lacks fairness checks, it can lead to unintended harm. This makes it essential to choose tools tested for fairness and designed to serve a wide range of users (Chaudhuri & Mohanty 2023).

The risks of "black box" AI

Transparency and explainability go hand in hand. If an AI tool gives advice or suggestions, SME users should understand how and why. If the process feels like a "black box," trust breaks down. Choosing tools that offer explainable output helps SMEs stay in control and make informed, responsible decisions (Giovine, Roberts, Pometti & Bankhwal 2022).

DATA SECURITY CHECKLIST FOR SMES

- Is the AI tool GDPR- and AI Act-compliant?
- Does it minimize data collection and anonymize where possible?Can you explain how the AI produces its outputs?
- Has the provider published a cybersecurity and privacy commitment?

As the use of AI expands, so do the safety and regulatory requirements. Today, AI is already regulated in areas like autonomous vehicles and medical devices (MDR), where safety is critical and strict oversight applies. In some contexts, AI systems may also be linked to criminal liability, especially if they contribute to decisions with serious consequences. (MedTech Europe 2022; Fraunhofer IKS 2023.)

This highlights a broader legal landscape. AI does not fall under just one set of rules. It is subject to multiple overlapping regulations, including product safety, consumer protection, data privacy, and even labour law. That's why SMEs should understand that AI security is not just a technical matter, it's a legal and ethical responsibility. Choosing safe, well-documented, and compliant tools is key to building trust and avoiding future risks.

In short, AI offers powerful benefits, but with that power comes a duty of care. SMEs must ensure that the tools they choose safeguard user data, meet legal standards, support fairness, and remain easy to understand.

Next, we will focus on how to think responsibly not only about people and data, but also the planet.

SUSTAINABLE AI – PROTECTING THE PLANET

Artificial Intelligence is transforming industries from healthcare to finance, but behind the convenience lies a hidden environmental cost. As AI models grow larger and more complex, their energy demands quadruple. Training a single large language AI bot can emit as much carbon as five cars over their lifetimes as a study from the University of Massachusetts says. (Strubell, Ganesh & McCallum 2019.)

One of the most pressing issues is the hidden carbon-cost of AI: Data centres that power these systems now account for 3–4% of global CO_2 emissions (Kamiya & Bertoldi 2024). Much of this relies on fossil fuels. (Lavi 2022; OECD 2024.) Large language models can also suffer from "stochastic parroting", vast consumption of resources without proportional value (Bender et al. 2021).

Short-lifecycle AI hardware generates significant electronic waste (UNITAR 2024). AI tools often rely on powerful chips and servers that need to be replaced after just a few years. As technology moves fast, older equipment becomes outdated quickly. This leads to growing amounts of electronic waste, which is expensive to manage and harmful to the environment if not recycled properly. For SMEs, choosing energy-efficient tools and extending the life of hardware where possible helps reduce costs and shows commitment to sustainability.

BUSINESS BENEFITS VS RESPONSIBILITY CHALLENGES OF AI

AI offers many business benefits for SMEs. It can improve operational efficiency by automating tasks and speeding up processes. It can also support better decision-making through data analysis and scenario foresight, helping businesses plan for the future more effectively. Moreover, using AI smartly can provide a real competitive advantage.

However, these benefits come with important responsibility challenges. High energy consumption associated with AI models increases environmental costs. Using AI without proper safeguards creates data privacy risks. Scenario planning based on biased data can lead to fairness issues, affecting trust and decision quality. In addition, the fast turnover of AI hardware leads to growing e-waste problems, adding pressure to find sustainable solutions.

To fully benefit from AI, SMEs must recognize and manage these responsibility challenges alongside the business opportunities. Fortunately, solutions are emerging. One approach is to locate datacentres in colder regions, where less energy is needed for cooling (VERNE 2024). Next to that the residual heat can be used for district heating. For example, the Telia Helsinki data centre uses its waste heat to warm offices and homes in the Helsinki region (Telia 2024).

Another solution is developing smaller, task-specific AI models, which use significantly less computing power (Canales Luna 2024).

EMERGING SOLUTIONS FOR SUSTAINABLE AI

As concerns over AI's environmental impact continue to grow, businesses are actively seeking smarter and more sustainable solutions. Fortunately, innovation is moving fast. New technologies and operating models are making it possible to reduce AI's carbon footprint without sacrificing performance.

Here are a few practical approaches that SMEs should be aware of when selecting or building AI solutions:

- Green data centres: Facilities in colder regions with heat recovery systems (Telia, 2024; Verne Global, 2024).
- Heat recovery innovations: Reuse of server heat for district heating.
- Task-specific lightweight models: AI models designed for efficiency (Canales Luna, 2024).

Example 5: How the SURE Bot Supports Sustainability

- Lightweight and task-specific foresight model.
- Hosted on Microsoft's sustainable Azure Platform.
- Minimized carbon footprint through efficient architecture.

AI can be a great tool for business, but it has a footprint. Here's how SMEs can support sustainable use of AI when adopting external tools:

SUSTAINABILITY CHECKLIST FOR SMES

- Is the AI model optimized and right sized for the task?
- Is it hosted on eco-friendly, efficient infrastructure?
- Does the provider minimize hardware turnover and promote e-waste recycling?
- Is energy efficiency a core design principle?

In conclusion, AI hold great promise for SMEs, but it also carries a cost. From data centres to e-waste, the environmental impact of AI must be addressed with the same care as privacy and ethics. Fortunately, sustainable solutions exist, such as relocating data centres to cold climates and reusing the heat. The real question is: can SMEs to ignore them?

KEY FUTURE TRENDS IN SECURE AND SUSTAINABLE AI

The regulatory and technological landscape around AI is evolving rapidly. For SMEs aiming to stay competitive and compliant, it's no longer enough to adopt AI tools. Future success will depend on anticipating the next wave of standards and innovations.

Understanding these emerging trends helps businesses prepare strategically, manage risks early, and seize new opportunities in a responsible way. Here are four developments SMEs should watch closely:

- **Mandatory sustainability reporting**: The new EU Corporate Sustainability Reporting Directive (CSRD) will require disclosures on AI energy use and emissions (EU 2024).
- **Security-by-design requirements**: Upcoming updates to GDPR and the AI Act will demand that AI tools include built-in security, not add-ons (Lai & Spring 2023).
- **Green AI innovations**: Investment is accelerating in energy-efficient hardware like neuromorphic chips and carbon-aware AI scheduling (Greene-Dewasmes & Tiadi 2025; Masterson & North 2025).
- **AI auditing and certification**: Independent third-party audits will become standard to verify an AI system's ethical, security, and environmental compliance (OECD 2024).

Together, these trends signal a major shift: responsible AI is no longer optional. It is becoming a baseline expectation. SMEs that proactively embed sustainability, security, and transparency into their AI strategies will not only meet regulations. They will stand out as trusted, forward-looking leaders.

CONCLUSION: FIVE PILLARS FOR RESPONSIBLE AI ADOPTION

As AI adoption accelerates, SMEs that lead with responsibility will position themselves for long-term resilience. Responsible AI is not just about legal compliance. It is about earning trust, demonstrating ethical leadership, and generating shared value for people, business and the planet.

To guide their journey, SMEs can rely on these five foundational pillars:

- **Service Promise**: Is the AI tool's purpose clear, credible and achievable?
- **AI Literacy**: Do employees understand how the tool works and where its limits lie?
- **Ethical AI**: Is the system built to be inclusive, transparent and fair?
- **Secure AI**: Is all data, personal and business, protected by design?
- **Sustainable AI**: Are the environmental impacts known, measured and minimized?

By embedding these principles throughout the AI lifecycle, from selection and deployment to monitoring and continuous improvement, SMEs can transform responsible AI into a lasting competitive advantage. A future-ready, resilient, and trusted organization starts with the choices made today.

This article was produced as part of a student project integrated into the completed SURE RDI project (Performance, Resilience and Vitality through Continuous Workplace Learning), funded by the Centre for Economic Development, Transport and the Environment for Häme (ELY Centre for Häme).

The SURE project (ESR+) supported the sustainable growth of Finnish SME exporters in a rapidly changing global environment. It helped companies anticipate future skills needs and lead continuous workplace learning through data-driven tools and responsible AI solutions.

Illustrations in this article were generated by generative AI (OpenAI ChatGPT). AI was also used to refine the language. The article adheres to the principles of responsible conduct of research and Laurea's ethical guidelines on the responsible use of AI in expert communication.

References

Afroogh, S., Akbari, A., Malone, E., Kargar, M., & Alambeigi, H. 2024. *Trust in AI: progress, challenges, and future directions*. Humanities and Social Sciences Communications, 11, Article 1568. Retrieved: 27.4.2025.

Apple, J. 2025. *Battling the Expectations and Realities of Copilot: Insights from the Ring*. Orchestry. Retrieved 4.4.2025.

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. 2021. *On the dangers of stochastic parrots: Can language models be too big?* Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 610–623. Retrieved: 20.4.2025.

Blythe, F., Cuyvers, L., & Bruynseraede, M. 2024. *EU AI Act: Are you prepared for the "AI literacy" principle?* Sidley Data Matters Privacy Blog. Retrieved: 27.4.2025.

Blomster, M., Kurtti, J-R., Määttä, M. & Sinisalo, J. 2020. Digitaalisen markkinoinnin käsikirja: opas mikro- ja PK-yrityksille. E-Kirja.

Canales Luna, C. 2024. *Sustainable AI: How Can AI Reduce its Environmental Footprint?* DataCamp. Retrieved: 2.4.2025.

Chaudhuri, S. & Mohanty, I. 2023. *The Importance of Bias Mitigation in AI: Strategies for Fair, Ethical AI Systems*. UX matters. Retrieved: 5.4.2025.

Deuze, M. & Beckett, C. 2022. *Imagination, Algorithms and News: Developing AI Literacy for Journalism*. Digital Journalism 10(10), 1913-1918. Retrieved: 30.3.2025.

EQS Group. 2025. *Artificial intelligence and GDPR – managing the data protection challenges*. Retrieved: 2.4.2025.

The EU Artificial Intelligence Act. *(Regulation EU 2024/1689).* EUR-Lex. Retrieved: 1.4.2025.

Fraunhofer IKS. Institute for Cognitive Systems 2023. *AI Act: High-risk AI systems – Requirements for autonomous vehicles and medical devices*. Retrieved 2.4.2025.

Gillespie, N., Lockey, S., Curtis, C., Pool, J., & Akbar, A. 2023. *Trust in Artificial Intelligence: A Global Study*. The University of Queensland and KPMG Australia. Retrieved: 24.4.2025.

Giovine, C., Roberts, R., Pometti, M. & Bankhwal, M. 2022. *Building AI Trust: The Key Role of Explainability*. McKinsey & Company. Retrieved: 7.4.2025.

Greene-Dewasmes, G. & Tiadi, T. 2025. *AI's energy dilemma: Challenges, opportunities, and a path forward*. World Economic Forum. Retrieved: 23.6.2025.

Hallensleben, S., Hustedt, C. & al. 2020. *From Principles to Practice. An interdisciplinary framework to operationalise AI ethics*. AI Ethics Impact Group led by VDE. Bertelsmann Stiftung. Retrieved: 31.3.2025:

ICO. 2023. *Annex A: Fairness in the AI lifecycle*. Information Commissioner's Office. Retrieved: 1.4.2025

Kalliomäki, A. publication date unknown. *Tarinallistaminen*. Tarinakone.fi. Retrieved: 6.4.2024.

Lai, C. & Spring, J. 2023. *Software Must Be Secure by Design, and Artificial Intelligence Is No Exception*. CISA. America's Cyber Defense Agency. Retrieved: 23.6.2025.

Lavi, H. 2022. *Measuring greenhouse gas emissions in data centres: the environmental impact of cloud computing*. Climatiq. Retrieved: 23 .6.2025.

Kamiya, G. & Bertoldi, P. 2024. *Energy consumption in data centres and broadband communication networks in the EU*, Publications Office of the European Union. Retrieved 24.6.2025.

Marr, B. 2020. The Intelligence Revolution: Transforming Your Business with AI. Kogan Page**.**

Masterson, V. & North, M. 2025. *Microchips – their past, present and future*. World Economic Forum. Retrieved: 23.6.2025.

MedTech Europe. 2022. *Liability challenges in AI medical technologies: MedTech Europe's perspective*. Retrieved: 24.4.2025.

Microsoft. 2024. *What is generative AI?* Retrieved: 14.4.2025.

NTT Data. 2024. *Security Risks of Generative AI and Countermeasures, and Its Impact on Cybersecurity*. Retrieved: 2.4.2025.

Pinski, M.& Benlian, A. 2024. *AI literacy for users – A comprehensive review and future research directions of learning methods, components, and effects*. Computers in Human Behavior: Artificial Humans 2(1), 100062. Retrieved: 1.4.2025.

Rivers, T. 2024. *How SaaS and AI are Building the Future of Intelligent Software*. Software Equity Group. Retrieved: 20.4.2025.

Rusanen, A.-M., Nurminen, J.K., Raisanen, S., Tarkoma, S. & Halmetoja, S. 2025. *The Ethics of AI*. University of Helsinki: Online course. Retrieved: 31.3.2025.

Secure Privacy 2024. *Compliance Challenges at the Intersection between AI & GDPR in 2025*. Retrieved: 5.4.2025.

SentinelOne 2024. *Top 14 AI Security Risks in 2024*. Retrieved: 2.4.2025.

Strubell, E., Ganesh, A., & McCallum, A. 2019. *Energy and policy considerations for deep learning in NLP*. In Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics , 645–3650. Association for Computational Linguistics. Retrieved: 15.4.2025.

Telia 2024. *Telia Helsinki Data Center serves as a radiator for thousands of homes*. Retrieved: April 2, 2025.

UNESCO 2021. *Recommendation on the Ethics of Artificial Intelligence*. Paris: United Nations Educational, Scientific and Cultural Organization. Retrieved: 20.4.2025.

UNESCO 2023. *Women in Tech – "I'd Blush if I Could"*. Retrieved: 31.3.2025.

UNITAR. United Nations Institute for Training and Research 2024. *The global e-waste monitor 2024*. Retrieved: 6.4.2025.

Verne Global 2024. *The Nordic advantage for high performance compute*. Retrieved: 6.4.2025.

Vähä-Sipilä, A., Marchal, S. & Aksela, M. 2021. *Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta*. National Cyber Security Centre Finland. Traficomin tutkimuksia ja selvityksiä 9/2021 Retrieved: 20.4.2025.

Warren, T. 2025. *Microsoft should change its Copilot advertising, says watchdog*. The Verge. Retrieved: 23.6.2025.

Authors

Jelte Van Barneveld, Joni Kivelä, Tommi Koivunen, Johan Mounier, Emilia Rämö & Annemari Kuhmonen

Figures:

1. Picture about service promise, generated by ChatGPT
2. Picture about AI literacy, generated by ChatGPT
3. Picture about Ethical AI, generated by ChatGPT
4. Picture about Secure AI, generated by ChatGPT
5. Picture about Sustainable AI, generated by ChatGPT
6. SURE Bot Icon, generated by ChatGPT

ISSN 2954-2170