HUX AI
Empowering humanity, shaping tomorrow

RESEARCH INTERNSHIP REPORT

AI Governance Toolkit for SMEs

AUTHORS
ASLI DİLARA ŞEN, BUSE NAZAN TASHKIN, DENİZ ALBAYRAK,
ECE SÜLÜNGÜR, ENES BAŞBUĞ, TOLGA ARSLAN, ZEYNEP ÖNAL

ADVISOR & MENTOR
DUYGU ÇAKIR

ADVISOR & EDITOR
MERVE AYYÜCE KIZRAK

PUBLISHED
NOVEMBER 2025

Licensing Notice

Please cite this work as:
Şen, A. D., Tashkin, B. N., Albayrak, D., Sülüngür, E., Başbuğ, E., Arslan, T., and Önal, Z., "AI Governance Toolkit for SMEs," HUX AI, 2025, licensed under CC BY-NC 4.0 via Wikimedia Commons.

Legal Notice

The views and analyses expressed in this report are those of the individual authors and contributors. They do not represent the official position of HUX AI. This publication is for informational purposes only and does not constitute legal or commercial advice.

Table of Contents

Table of Contents

Executive Summary

Artificial intelligence (AI) is redefining how organisations innovate and operate by presenting opportunities to work in a more intelligent way, identify opportunities, and have a better understanding of their customers. For small- and medium-sized enterprises (SMEs), these innovations are thrilling, but they are also putting additional pressure due to limited resources (e.g. people and technical capacity) to use AI applications in an ethical and compliant way. Responsible AI requires not only the technology but also clear and actionable means of incorporating transparency, fairness, and accountability in the use of that technology. The AI Governance Toolkit for SMEs aims to provide clear and actionable ways to do this, offering simple instructions, adaptable templates, and actionable steps that can help organisations use AI systems in a responsible, confident, and sustainable way.

The toolkit includes:

- **Readiness test/self-assessment** to provide a clear understanding for the company's leaders on where they stand in the AI Governance process and guide them on where to begin.
- **3 Templates on policy implementation, risk assessment and transparency & accountability.** Each template aims to create a space for company leaders to reflect on their actions, particularly on issues such as data processing, regulatory compliance, risk analysis, bias detection and responsibilities in the AI Governance process. All templates consist of some questions to be answered and an explanation of significant concepts for a smooth implementation of the toolkit and understanding AI governance.
- **Quick implementation manual** aiming to create tailored guidance for the company leaders on literacy and implementation of each template.
- **Environmental impacts for SMEs** section that will cover the Carbon Emission calculation of the company. This section is deemed essential for SMEs to take into consideration while utilization of AI has been associated with unsustainability.
- **Use cases** aiming to showcase AI governance risk in various industries. Companies may review the prepared use cases that most resemble their own AI system and/or the industry they are currently operating in to understand the potential risks posed by AI in governance.

Abbreviations

AI	: Artificial Intelligence
AIA	: Artificial Intelligence Act
FAQ	: Frequently Asked Questions
API	: Application Programming Interface
HR	: Human resources
SMEs	: Small and Medium Enterprises
NIST	: National Institute of Standards and Technology
GDPR	: General Data Protection Regulation
DPA	: Data Processing Agreement
MFA	: Multi-Factor Authentication
ESG	: Environmental, Social, and Governance
GPAI	: General-purpose Artificial Intelligence
IoT	: Internet of Things
DPA	: Data Processing Agreement
OECD	: Organisation for Economic Co-operation and Development
HITL	: Human-in-the-loop
DPIA	: Data Protection Impact Assessment
FRIA	: Fundamental Rights Impact Assessment
EIA	: Environmental Impact Assessment
CEO	: Chief Executive Officer
COO	: Chief Operating Officer
CTO	: Chief Technical Officer

Addressee List

AI Governance Owner	: Typically, CEO or COO
Technical Lead	: Typically, CTO or Senior Engineering Head
Business Lead	: Typically, Operations or Product Manager
Legal & Compliance Lead	: Internal Counsel or External Advisor

Annex I: AI Governance Dictionary

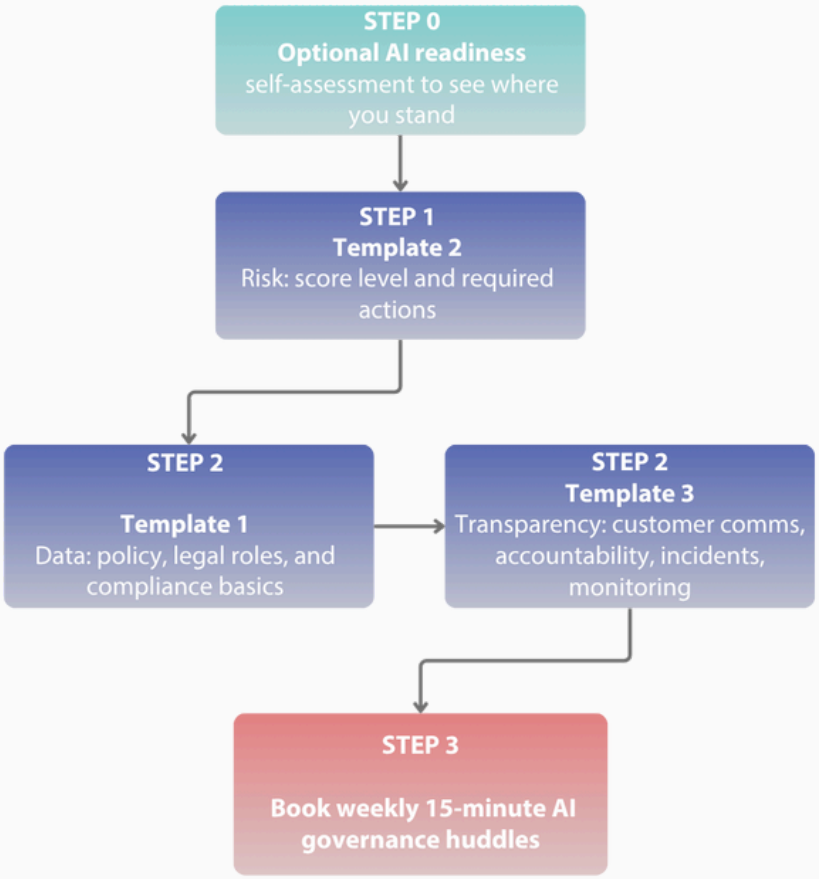
Disclaimer: *This is general guidance; it is not legal advice and does not guarantee regulatory compliance. It should be adapted to the regulations you are subject to, your jurisdiction, and your industry.*

Quick Self-Assessment: Do You Need AI Governance?

This quick AI Readiness Test aims to help SMEs evaluate their status or level of preparedness for adopting AI. The test covers key areas, including data, governance, and risk.

Answer the 20 self-assessment questions in the AI Governance Readiness Test as Step 0.
Step 1: Start with Template 2: Reflective AI Risk Awareness Checklist.
Step 2: Use the risk colour to prioritise Template 1 and Template 3.
Step 3: Book weekly 15-minute AI governance huddles.

*Please visit the **Interactive Quick Implementation Manual***



Template 1
Data & AI Responsibility Policy Template

For the sake of convenience, this toolkit selected the General Data Protection Regulation (GDPR), the Data Act, and the AI Act as regulatory frameworks. However, it is essential to remember that this is a guideline and should not be considered a comprehensive approach.

Policy owner: _____

Effective date: _____

Next review: _____

Type of Data Being Processed (A2):

- ☐ Personal Data
- ☐ Sensitive Data
- ☐ Product Data

Following Processing Principles (A3):

- ☐ Yes
- ☐ No

Business Definition (B1): _____

Risk Category (B2): _____

Regulatory Compliance Checklist Completed (D):

- ☐ Yes
- ☐ No

A. Data Protection Guidance

A1. Do Data Protection Laws (eg., GDPR) Apply to my Business?

- Do you collect, process, hold, or use the data of your customers or employees?
  - If yes, the data protection law applies
  - If no, the data protection law does not apply

A2. Knowing the Type of Data Being Processed

Regulation may pose different compliance procedures and additional obligations to companies. Thus, companies should be able to differentiate between different types of data. Some data types are presented below. These may include separate data classes, and in some cases, they may overlap.

Table 1: Types of data collected, processed, and/or used *(adapted from GDPR & Data Act categories)*

Personal Data (GDPR) *Data that is related to an identified or identifiable person, such as*	**Sensitive Data (GDPR)** *Personal data that reveals specific information*	**Product Data (Data Act)** *Data generated by the connected product (IoT) could be personal or non-personal*
• Contact details *(name, email, phone)* • Account data *(username, password hash)* • Usage/analytics *(page views, clicks, device info, IP address)* • Customer service interactions *(chat/email transcripts)* • Employee data *(HR records, performance data)*	• Healthcare history • Biometrics of the person • Ethnicity • Religion • Sexual orientation 1. Avoid processing unless it is strictly necessary. 2. Follow Article 9 of the GDPR conditions to process	• Non-personal; purely technical or environmental information (soil temperature detector) • Personal data; fitness tracker linked to user account • Sensitive data; smart watch revealing heart rate (health data falls under a special category)

A3. Are you Following "Processing Principles"?

A company must follow at least these principles when handling data. Failing to comply with any of these principles could result in legal problems. However, confirming your compliance always requires a formal, legal audit.

- **Lawfulness, fairness, transparency:** Have a clear lawful basis (e.g., consent; ensure it is freely given, specific, informed, and unambiguous; contractual basis, etc.); be open with people.
- **Purpose limitation:** Collect for specific, stated purposes only.
- **Data minimisation:** Collect only the necessary data for the determined purpose.

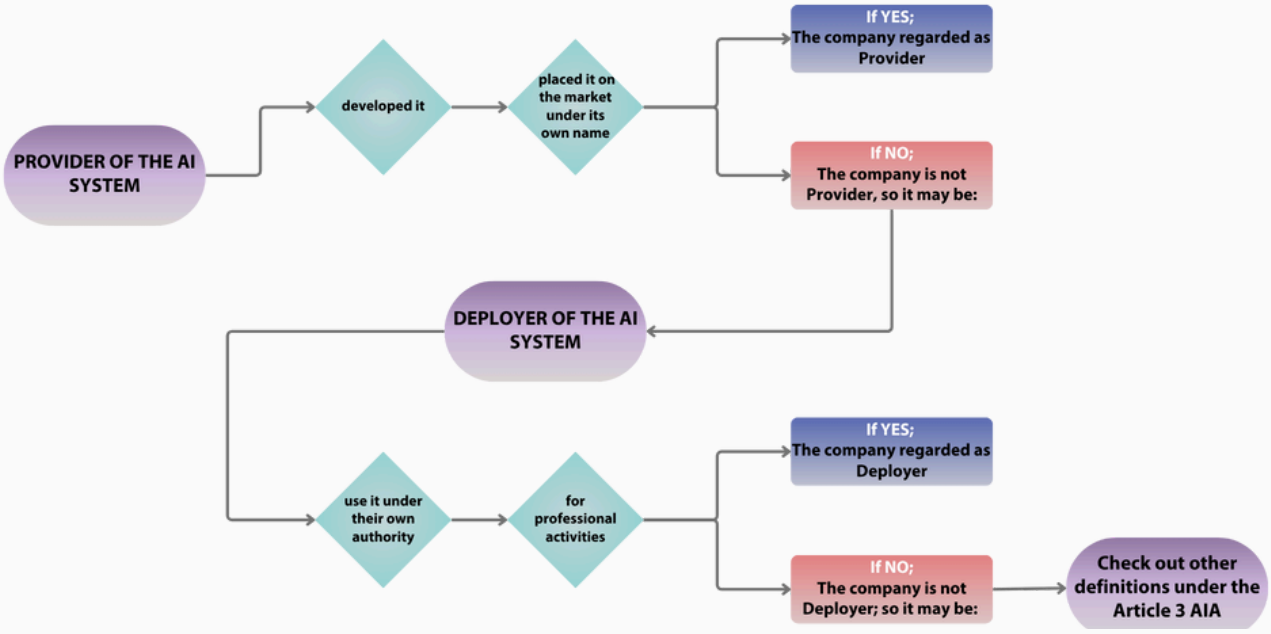
- **Accuracy:** Keep data accurate and up to date.
- **Storage limitation:** Don't keep it longer than necessary & be aware of retention periods.
- **Integrity & confidentiality:** Keep it secure (e.g. access controls, encryption, logging).
- **Accountability:** Document decisions and be able to show compliance.

B. EU AI Act Guidance

B1. Which Definition Does my Business Fall Under?

As each definition imposes various obligations on companies, it is crucial to start by understanding your company's relationship with the AI system in use. By checking the flowchart, you can help you to decide which definition your company fall under the AI Act:

Figure 1. Example of decision flow for determining whether a company is an AI provider or deployer under the EU AI Act.

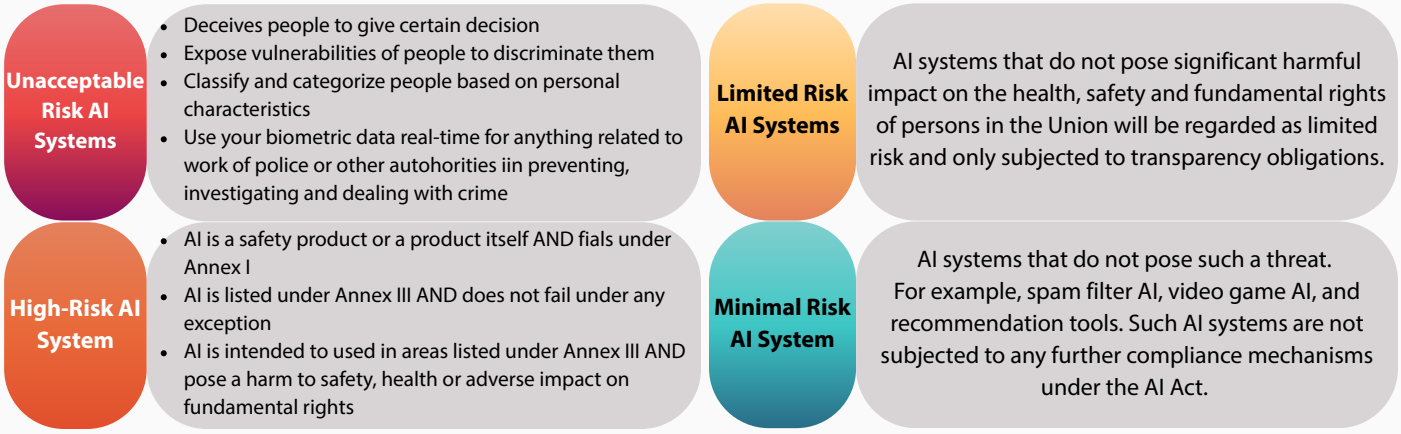


B2. Which Risk Category Does my AI System Fall Under?

The AI Act employs a risk-based approach to classifying AI systems. While unacceptable risk categories prohibit the use of AI systems in the EU market, it is essential to understand what practices can be considered unacceptable risk. Hence, this falls outside the scope of this governance toolkit.

Moreover, minimal risk AI systems are not subject to compliance measures, whereas limited risk AI systems that pose a **significant harmful effect** must fulfil transparency requirements. Given that the main focus of the Act is on categorisation, compliance mechanisms and provider/deployer obligations of the high-risk AI systems, the company has to pay more attention when they have a high-risk AI system.

Figure 2. Categorisation of AI systems into unacceptable, high, limited, and minimal risk under the EU AI Act.



Annex II: High-Risk AI Classification & Governance provides more on the High-Risk AI classification and compliance mechanism under the AI Act.

C. Escalation to Legal Leaders

Some procedures can be more complex to follow, or they might be required to fulfil additional requirements. Those issues should escalate to Legal & Compliance Leads.

Such as:

- If the AI system will be used in third-party countries, then international data transfer/third-party sharing rules (data processing agreements, check of adequacy decisions) will be relevant.
- If there are any detected cybersecurity risks, the company should ensure **minimum security** precautions under GDPR.
- Where data processing results in a potential high risk to customers' rights and freedoms, controllers must carry out a data protection impact assessment (DPIA).
- When the AI system is classified as high-risk, a fundamental rights impact assessment (FRIA) must be carried out.
- When the AI system is classified as high-risk, the obligations of providers and deployers must be checked under the AI Act.
- There is confusion in the classification of general-purpose AI (GPAI) models as "general-purpose AI models with **systemic risk**".

Significant effect *refers to any decision or outcome that substantially impacts an individual's rights, responsibilities, opportunities, access to services, employment, health, or financial stability.*

Minimum security, *precautions can be role-based permissions, Multi-Factor Authentication (MFA), encryption (technical); least-privilege, quarterly access reviews (Organisational); restrict access to offices/servers/devices; no personal data on personal devices (Physical).*

Systemic risk, *"a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole" (art. 3 (65) AIA)*

D. Guidance for Trustworthy AI Use

This section provides practical guidance to help SMEs foster trustworthy and transparent AI use. The following points draw on widely recognised ethical and governance principles from global frameworks, but are illustrative in nature. They are intended to support awareness and responsible decision-making rather than to prescribe or guarantee legal compliance. Organisations are encouraged to treat these as reference points and consult professional legal advisors for jurisdiction-specific requirements.

- **Complied with Data Processing Principles** *(see processing principles)*
- **Record-Keeping:** Document what personal data you hold, where it came from, who you share it with, how long you will keep it, and the technical procedure of AI systems.
- **Data Protection by Design & by Default:** Privacy should be established as an integral part of data protection and implemented effectively. Personal data should not be made accessible by default.
- **Explainability & Understandability:** The processing process should be rendered comprehensible to ensure transparency and accountability.
- **Human Oversight:** Established humans must be present if autonomous decision-making is involved or if an AI system is at high risk.
- **Risk Category of AI System:** Different obligations for different risks, so the risk category of the AI system should be established as a priority step.
- **Awareness by Customers:** Data subject rights should be informed, e.g. access, correction.
- **Cybersecurity Measures Installed:** MFA, encryption, Data Breach Response Plan.
- **Management of DPIA + Fundamental Rights Impact Assessment (FRIA):** Render someone accountable for the impact of AI systems on the company, customers, and essential rights.
- **Seek Legal Advice:** When there is confusion, additional requirements, and conflict within processes.

Template 2 Reflective AI Risk Awareness Checklist

Risk management for SMEs is essential, as they generally have less capacity and a greater compliance risk. This template helps teams detect, assess, and mitigate risks related to AI during the AI life cycle, support responsible use, legal compliance, and long-term trust.

Owner: _____
Last updated: _____
Risk Evaluation Score (B): _____

A. AI System Inventory

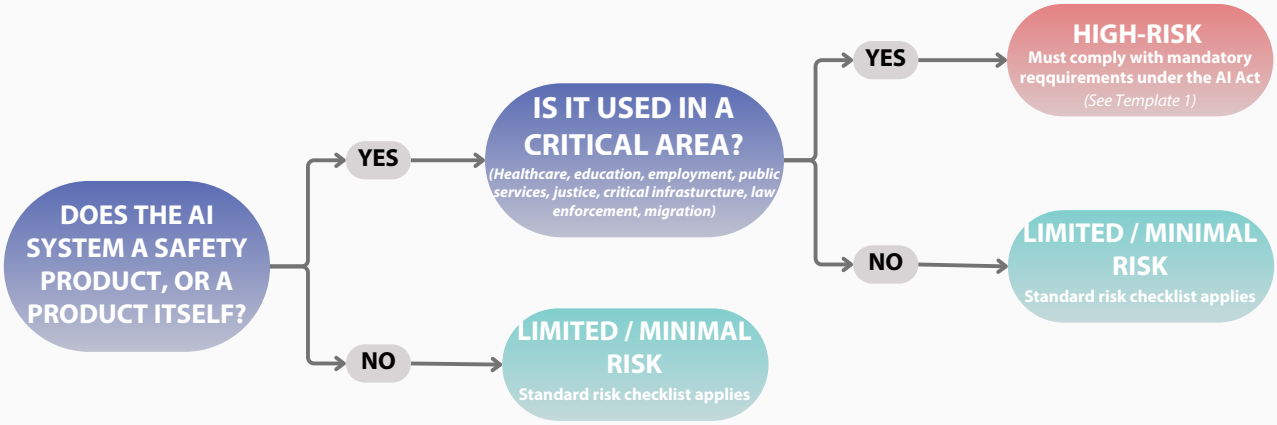
The AI inventory table below has descriptions for the SME's AI systems, including their purpose, data sources, individuals affected, level of risk, and governance, to facilitate risk assessment, accountability, and compliance.

Table 2. AI system inventory and risk assessment checklist.

ID	System/ Tool	Purpose	Data used	Affected people	Risk Category*	Risk Areas**	Decision owner
1	Customer Support Chatbot	Automate FAQ answers and triage; HITL for refunds/escalations	Chat transcripts; prior ticket metadata; account tier; device info (no payment numbers, no special-category data)	Customer support agents	L	T, E, L/C	Customer Service Lead
2	Automated Hiring Algorithm	Screen and rank job applicants using predictive models	CV data; education and employment history; behavioral assessment data; potentially inferred sensitive attributes	Job applicants	H	T,E,L/C,B	Head of HR

**The level of risk is categorised as Minimal (M), Limited (L), High (H) or Unacceptable (UnA) risk based on the AI Act. For better understanding, see Figure 2. To determine the risk category, refer to Figure 3.*
***Risk Areas covers the following aspects: technical (T), business (B), legal/compliance (L/C), or ethical (E).*

Figure 3. Flowchart for determining the AI system's risk category under the AI Act.



B. Reflective Risk Awareness Questions

(30 prompts for self-assessment)

The following reflective questions are designed to help teams self-assess areas of potential risk awareness during AI use. The responses are indicative only and should not be interpreted as a formal compliance evaluation.

Domains: Data, Automation, Oversight, Bias/Harm, Security, Regulation, Transparency.

Data Sensitivity

- Does the system use personal data?
- Does it use sensitive data?
- Has more data than necessary been processed?
- Has personal data been obtained without relying on any of the lawful bases? (e.g. consent, contract, legal obligation, vital interests, public task, or legitimate interests)
- Are prompts/outputs stored by the vendor?
- Are there cross-border data transfers?
- Is data used beyond its initial purpose?
- Does the system process children's data or significantly affect children's rights?

Decision Automation

- Do decisions have a significant effect on people?
- Are decisions solely automated?

Human Oversight

- Does the system make decisions without providing an appeal after they are made?

- Is the system deployed without a comprehensive human audit procedure (either before or after deployment)?
- Is the system operating without a specified oversight mechanism for detecting and correcting hallucinations or mistakes before they have caused a significant effect on people?

Bias & Harm

- Does the system operate without clearly defined intended uses and boundaries?
- Does the system run without clear goals or limits?
- Does the system run without properly checking for bias across different groups?
- Does the system operate without thorough bias testing across relevant groups?
- Can errors in the system lead to physical, financial, or psychological harm?
- Does the system rely on datasets that are used in the same context and have the same characteristics as the affected population?

Security & Resilience

- Are system activities not being recorded or not reviewed regularly?
- Before launching the AI system, do we skip testing for possible attempts to trick or confuse it?
- If an update fails, is there no clear way to return to a safe version?
- Can administrators log in without extra verification or approval steps?

Regulatory & Contractual

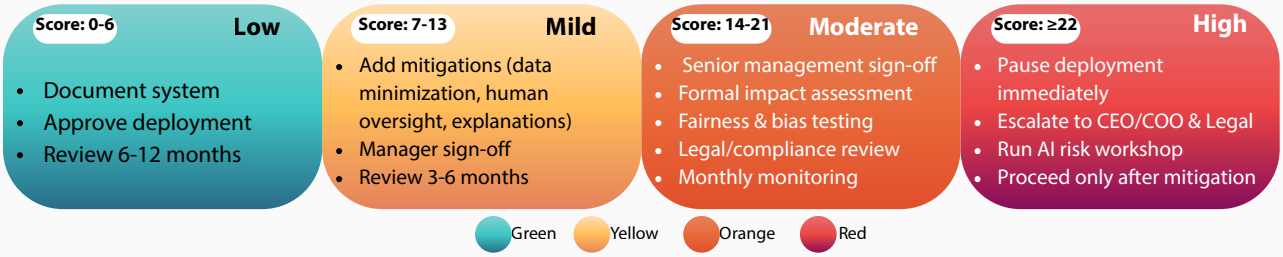
- Does the system operate without a privacy notice and AI disclosure in place?
- Do vendor relationships proceed without a Data Processing Agreement (DPA) in place?
- Does the AI system put in place without an impact assessment?
- Does the organisation continue without a breach response plan (72-hour internal clock)?
- Do staff carry out their responsibilities without receiving appropriate training?
- Does the program work without a specified review schedule (e.g., quarterly or twice a year)?

Transparency & Explainability

- Does the system interact with users or display AI-created content without clearly informing that the interaction or content is generated by an AI system?
- Does the system deliver results or decisions without providing plain-language explanations that an average user can easily understand?
- Does the system make or support decisions in ways that users or affected individuals cannot reasonably understand, question, or challenge?

C. Risk Awareness Matrix and Example Actions

Figure 4. Risk scoring framework and Illustrative actions for AI systems.



Escalation Triggers

- A change in the system's purpose or application that impacts the AI system's risk scoring.
- The vendor updates the model: new version, refreshed training data, or significant parameter adjustments.
- A serious incident occurs, such as a biased finding, user harm, a privacy leak, or a security breach.
- Legal, regulatory or policy changes; new laws, regulator guidance, or internal policy updates that affect your controls. *(See Template 1)*

Template 3 Transparency & Accountability Framework

For SMEs, the transparent and accountable use of AI is an essential element for earning customer trust and achieving long-term competitiveness. For SMEs with limited budgets and shifting compliance demands, acting responsibly with AI is more than good ethics. It is essential for maintaining stable operations and earning lasting customer confidence. This section will provide a practical checklist example to help SMEs build transparent and sustainable AI systems by helping companies assess their AI processes, manage incidents, and align with ethical standards.

Owner: _____
Effective date: _____
Review date: _____

Customer Communication Provided (A):

- ☐ Yes
- ☐ No

Internal Accountability Provided? (B):

- ☐ Yes
- ☐ No

Incident Response Plan Ready? (C)

- ☐ Yes
- ☐ No

A. Customer Communication

It is good practice for SMEs to enhance transparency within the AI process to build and maintain customer trust. Therefore, explaining the design and implementation process of an AI system, the purpose of the data being processed, and how the outputs are made is encouraged to support responsible AI use. The following points provide suggested areas for consideration when aiming to strengthen transparency and user communication.

- Are customers informed when they interact with AI? *(AI Disclosure)*
- Have the customers consented to the privacy terms and conditions? *(Privacy Notice)*
- Can the decision made by AI (e.g. recommendations) be explained? *(Explainability)*
- Does the interaction with the AI system use plain language? *(Accessible Language)*
- Can users have a chance to opt out of AI-based profiling at any time? *(User Choice)*
- Is there a framework that allows users to challenge or request a review of AI-generated decisions? *(Appeal Mechanism)*

B. Internal Accountability

Mechanisms for internal accountability can help SMEs strengthen transparency and resilience against external audits. To improve clarity in decision-making, it is recommended that AI-related roles and responsibilities are clearly outlined and regularly reviewed. Accountability extends beyond documentation; it supports integrity and ethical awareness.

The following questions serve as a self-assessment guide, allowing organisations to reflect on how responsibilities are assigned, documented, and monitored.

- Are the responsibilities of the AI governance procedure formally assigned *(Addressee: AI Governance Owner)*?
- Are all the AI systems regularly documented and kept up-to-date *(Addressee: Technical Lead)*?
- Can authorized staff intervene with the decision making by AI system, where necessary *(Addressee: Business Lead)*?
- Are compliance and performance audits performed regularly *(Addressee: Legal & Compliance Lead)*?
- Has the organisation ensured that all relevant employees have completed training on AI ethics and risk management *(Addressee: HR / Compliance Lead)*?

C. Incident Response Plan

Having a structured incident response approach can help companies investigate and communicate AI-related risks in a timely and responsible manner.

To improve clarity in decision-making, it is recommended that AI-related roles and responsibilities are clearly outlined and regularly reviewed. Accountability extends beyond documentation; it supports integrity and ethical awareness.

This model aims to help organisations consider appropriate timelines and effective actions while maintaining accountability.

C1. AI Incident Response Matrix (Impact x Urgency)

AI incidents may be assessed through a transparent evaluation process that considers impact and urgency.

This assessment relies on three general factors:

1. Count of impacted individuals: potentially impacted users, employees, and stakeholders.
2. Disruption to operations and finances: planned disruption to operations or other technical activities.
3. Reputational or regulatory considerations: potential loss of public trust or risk of violating laws or regulations.

Table 3. Incident types, examples, and actions required based on their urgency level in AI governance.*

IMPACT → / URGENCY ↓	CRITICAL REGULATORY BREACH OR SEVERE BIAS	HIGH LARGE NUMBER OF USERS OR SIGNIFICANT HARM	MODERATE LIMITED BUSINESS OR CUSTOMER IMPACT	LOW MINOR ISSUE, NO MATERIAL RISK
IMMEDIATE NEEDS CONTAINMENT	**P1** Activate incident response team; regulator notified within 24h	**P1** Suspend feature; notify affected users; initiate retraining	**P2** Apply fix and log event	**P3** Monitor; include in quarterly report
HIGH ADDRESS in 1-2 DAYS	**P1** Governance owner approval; internal communication required	**P2** Conduct model audit technical root-cause analysis	**P3** Schedule corrective update	**P3** Track issue for trend analysis
MODERATE ADDRESS WITHIN 1 WEEK	**P2** Document in AI risk registery; review by Technical Lead	**P2** Apply internal correction; no user notification required	**P3** Minor fix; verify in next audit	**P3** Record only
LOW FLEXIBLE HANDLING	**P3** Document for oversight; review in annual meeting	**P3** Monitor performance metrics	**P3** Log and archive	**P3** Close without further action

**This matrix serves as an illustrative model only and should be adapted to the organisation's internal governance and context.*

Incidents are then classified by impact *(Critical → High → Moderate → Low) and urgency (Immediate → High → Moderate → Low).*
Each category assigns a priority level (P1–P4) with a matching response action.

This structured approach helps ensure that serious incidents are addressed without delay, while lower-risk issues are managed efficiently and recorded for future reference.

Using such a framework allows SMEs to respond appropriately, use their resources effectively and remain accountable at every stage of incident management.

C2. Ensuring Post-Incident Transparency

After SMEs have taken appropriate steps they deem necessary to enhance transparency in their use of AI, users and affected stakeholders should be clearly informed. The following questions are suggested prompts for communicating lessons learned and restoring user confidence.

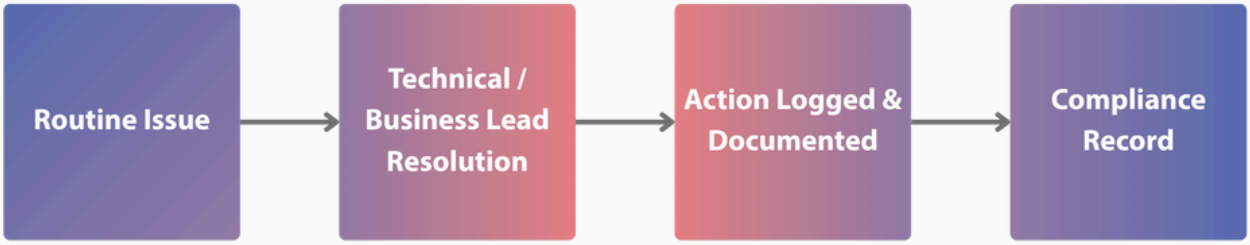
- What was the incident?
- How it was addressed, and
- What safeguards were put in place to prevent recurrence?

This reinforces organisational accountability and helps restore confidence in AI systems, which will maintain customer trust.

D. Escalation and Approval Process

Daily Operations: Routine, low-risk matters are resolved directly by the Technical and Business Leads. All actions must be logged and supported with technical documentation so there is a transparent and traceable record for compliance.

Figure 5. Escalation workflow for daily operations.



Policy Changes: Drafted by the Leads, legally reviewed, and only take effect once the Governance Owner gives formal approval.

Figure 6. Escalation and approval workflow for policy changes.

Quick Implementation Manual

Getting Started

- Answer the optional 20 questions of the **AI Readiness Test.**
- Start with this order: Template 2 → Template 1 → Template 3.
- **Gather:** list of tools, privacy notice, contracts, security controls, and any impact assessments.
- **Team:** AI Governance Owner, Technical Lead, Business lead, Legal & Compliance Legal.

Step-by-Step

Week 1

- **Day 1–2:** Complete AI inventory and assign an owner per system.
- **Day 3:** Run risk assessment and score each system.
- **Day 4:** Draft Template 1 (purposes/retention table).
- **Day 5:** Review; set access controls, enable logs; schedule reviews.

Week 2

- **Day 6–7:** Implement transparency (website/chatbot notice; privacy notice add-on).
- **Day 8:** Training for relevant staff (policy + incident drills).
- **Day 9:** Set up monitoring (dashboards, log checks, monthly metrics).
- **Day 10:** Document everything (owners, decisions, dates); book next scheduled review.

Tips: Start with the highest-risk systems; keep decisions short (bullets) and save them; iterate quarterly.

Common Mistakes to Avoid:

- Over-engineering before shipping v1.
- Under-communicating (no AI disclosure/notice update).
- Copy-pasting controls that don't fit your risk.
- Set-and-forget after launch.

When to Seek External Help:

- **Legal triggers:** High-Risk AI (credit, employment, eligibility, safety, biometric/emotion), cross-border transfers or children's data, data breach/potential notification, complex vendor contracts.
- **Technical triggers:** Tests for bias and stability, checks for data safety, and reviews to find weak points in the system. Regular monitoring keeps it working well.
- **Maturity evolution:** Work starts with basic tasks, moves to testing and reviews, and finishes with full reports and standards in place.
- **Cadence update:** Weekly or monthly checks for results and logs, quarterly updates for policies and training, and a yearly review for plans and goals.

Try the **Interactive Quick Implementation Manual**

Important Notice: *The Quick Implementation Manual provides an illustrative framework to help SMEs explore responsible AI management practices.*

The suggested steps and timelines are for general awareness and learning purposes only and may not fit every organisational context. Following these steps does not imply or guarantee compliance with any law, regulation, or standard.

Users are encouraged to adapt the materials to their own needs and consult professional advisors for legal or technical matters.

Environmental Framework

AI now plays a big role in driving innovation and supporting sustainable growth across companies of all sizes. Yet the growing computational demand behind AI systems also places visible pressure on the environment. Training and operating models require considerable amounts of energy, which could lead to higher carbon emissions if not properly managed.

Using AI responsibly and efficiently can help ensure technological advancement remains aligned with environmental goals. This framework aims to raise awareness and encourage organisations to take practical steps toward balancing sustainability with AI practices, as well as reducing avoidable energy use while maintaining their innovative capacity. It also provides a practical tool for self-assessment: Each checklist item represents an action that can be verified and documented. Checking a box indicates that the company has completed or reviewed that step, allowing teams to track progress, become aware of the environmental impacts of AI use, identify gaps, and plan improvements.

Owner: _____

Effective date: _____

Indirect Environmental Impact? (A):

- ☐ Yes
- ☐ No

Direct Environmental Impact? (B):

- ☐ Yes
- ☐ No

Estimated Total Carbon Emission (kg CO2): _____

A. For SMEs Using AI Tools

Indirect environmental impact

This table supports SMEs in assessing if their reliance on external AI solutions or cloud-based platforms could lead to indirect environmental effects. Each question reflects a measurable aspect of AI usage and infrastructure.

Table 4. Checklist for assessing indirect environmental impacts of AI use in SMEs.

Evaluation Question	Notes
Are the AI services you use (e.g., ChatGPT, Azure AI, Google Cloud) hosted on data centres powered mainly by non-renewable energy sources?	Check the provider's sustainability or energy mix report.
Does your organisation track the estimated electricity consumption (kWh) of AI integrations?	Even rough estimates can indicate energy exposure.
Is AI used frequently for high-volume or repeated automated tasks that could be optimised or reduced?	Overuse of APIs increases indirect energy demand.
Have you included AI-related energy use or emissions in ESG or sustainability reporting?	Helps quantify indirect Scope 3 emissions.
Do employees receive training or guidance on environmentally efficient AI usage?	Awareness contributes to lower digital energy use.

- *If more than one question has "Yes" as an answer, this indicates that your organisation may have indirect environmental impacts through its AI-related activities.*

B. SMEs Developing or Deploying AI Systems

Direct environmental impact

This table helps SMEs evaluate whether their AI-related operations generate any direct environmental impact, using measurable indicators such as energy consumption and carbon emissions.

Answer each question according to your organisation's current practices.

Table 5. Checklist for assessing direct environmental impacts of AI development and deployment in SMEs.

Evaluation Question	Notes
Do you measure the total electricity consumption (kWh) during model training or inference?	Use internal logs or metering tools.
Has your model training produced an estimated carbon footprint greater than 200 kg CO_2e per project?	Estimate with tools like $MLCO_2$ Impact Calculator or similar.
Are multiple GPUs or high-TDP hardware (>300 W each) used for extended training sessions?	High TDP increases direct energy impact.

Evaluation Question	Notes
Is training performed on grids primarily powered by non-renewable energy sources (coal or gas)?	Check the cloud provider region data.
Do you store large datasets or trained models for long periods without active use?	Storage energy adds to the overall footprint.
Do you share updates on CO_2e estimates and energy efficiency progress with your management or other key stakeholders on a regular basis?	Supports transparent environmental tracking.

- *Answering "Yes" to two or more questions indicates that your organisation is likely to create direct environmental impact through its AI activities.*

Practical Note:

The environmental footprint of AI projects may be explored using open, publicly available tools that estimate energy use and carbon intensity. These tools are shared here as illustrative examples to raise awareness and support initial understanding of potential environmental impacts.

While such tools can offer indicative insights, their results may vary in accuracy and reliability depending on methodology, data quality, and hardware settings. Therefore, they should be interpreted as approximations rather than precise measurements.

The following table presents a comparison of commonly referenced open-source and corporate tools for informational purposes only.

Table 6. Illustrative examples of carbon footprint estimation tools for AI

Tool	Type / Source	Measurement Method	Advantages	Limitations	Best Use Case
ML CO_2 Impact	Open-source web tool	Estimates CO_2 emissions based on hardware type, runtime, and region	Quick and easy for academic citation, intuitive interface	Not real-time; relies on fixed coefficients and assumptions	Quick CO_2 estimation for papers or reports
CodeCarbon	Python package (Open source)	Tracks hardware power usage + regional energy intensity	Integrates with MLOps pipelines, logs emissions per run	Accuracy depends on proper GPU/region setup	Real-time tracking during training or inference

Tool	Type / Source	Measurement Method	Advantages	Limitations	Best Use Case
Green Algorithms	Academic framework / web tool	Considers CPU, GPU, RAM, data center location, etc.	Cited in scientific publications; broad coverage	Not ML-specific; focuses on general computation	Cross-infrastructure or research-level carbon analysis
CarbonTracker	Python module	Predicts emissions from training time and hardware power	Can estimate emissions before training is completed	Optimized for model training only	Planning and optimizing deep learning training runs
Experiment Impact Tracker	Python library	Logs hardware energy consumption and emissions	Offers detailed per-run logging and reproducibility	Complex setup; requires manual input	Research labs needing granular experiment tracking
Deloitte AI Carbon Footprint Calculator	Corporate tool (proprietary)	Evaluates model training, data size, hardware, and energy source	Professional-grade verification and reporting	Closed source; enterprise license required	Corporate sustainability and AI governance reporting

C. Reducing the Footprint: Practical Direction

SMEs may consider practical actions to increase awareness of and potentially minimise the environmental footprint of their AI activities.

- **Parameter efficiency:** Whenever possible, use smaller and simpler models. Methods such as adapter layers, pruning, or knowledge distillation can improve results without the need to increase model size.
- **Data efficiency:** Cut down on unnecessary training by improving how data is chosen and prepared. Clean, relevant, and well-structured datasets created through filtering, active learning, or organised training steps help lower energy use during model development.
- **Reporting and transparency:** Monitor and disclose estimated CO_2e emissions from major AI projects, integrating these metrics into broader environmental, social, and governance (ESG) reports.
- **Awareness and decision-making:** Before training large models, question whether simpler or existing alternatives can meet the company's needs.
- **Lifecycle view:** Every stage, training, adaptation, deployment, and inference consumes energy and can be optimised for sustainability.

Use-Case Examples

A. E-Commerce Company

Company Definition
An online store based in Luxembourg that sells organic dietary products, vitamins, and herbal teas in Europe. The company's growth strategy relies on personalisation and automated arrangement.

AI Solution
The main focus is on employing a recommendation engine for supplement offers. Notwithstanding this, the company uses AI for product suggestions, personalised emails, discounts, and a support chatbot.

Risks
Since the company effectively uses personal data like health conditions for product suggestions, customer data might be exposed in an unfavourable situation. Security might be weak. Besides, suggestions from the AI might be biased or hard to understand. The system could make users spend more than they want.

Annex III: Check E-Commerce Company in Detail.

B. FinTech Company

Company Definition
A small fintech company based in the European Union, employing around twenty-five people. The company develops AI-driven software that helps partner banks and small businesses make financial decisions securely and efficiently.

AI Solutions
The company's core systems include FraudGuard, which detects irregular payment activities and flags potential fraud before transactions are processed, and CreditRisk Support, which assists credit officers in evaluating loan applications consistently. Human analysts always make the final decision. Future improvements aim to include multilingual explanations, adaptive risk scoring, and full traceability in line with ISO/IEC 42001.

Risks
Since the systems handle sensitive financial and personal data, improper use or technical failure could result in privacy breaches, biased or opaque decisions, and regulatory non-compliance.

Errors in automated scoring or fraud detection could harm clients and partner banks, making transparency, fairness, and robust human oversight essential.

Annex III: Check FinTech Company in Detail.

C. HR Tech Company

Company Definition

A human-resources technology SME that builds AI-powered tools for hiring and employee-performance management. The company has about 40 employees, serves mainly medium-sized clients in the UK and EU with some partnerships in the US, and operates under the EU AI Act (employment use cases are high-risk) and UK/EU GDPR, with NYC Local Law 144 applicable for certain US clients.

AI Solutions

Models assist with ranking job applicants and flagging early performance/engagement signals. Automation speeds shortlisting, but all hiring and evaluation outcomes are reviewed and approved by human managers (no fully automated rejections).

Risks

Potential algorithmic bias or unfair impact on candidates; incorrect or opaque outputs; over-reliance on automation; unauthorised access to sensitive personal data; and non-compliance with the EU AI Act, GDPR, and relevant equality/bias-audit rules, which could harm individuals and erode client trust.

Annex III: Check HR Tech Company in Detail.

D. Legal Company

Company Definition

A legal company that has specialised in various fields of law, including labour law, consumer protection law and contract law. This company is located and functions in the European Economic Area.

AI Solutions

The IT department in the law company has developed a legal chatbot with the goal of efficiently managing repetitive and simple enquiries, including answers to factual questions, providing legal information to search and identifying case references.

Risks

AI systems that provide answers/explanations that are incorrect. The chatbot may generate responses that are discriminatory biases. Unauthorised access to the sensitive data shared by clients could cause damage to the company.

Annex III: Check Legal Company in Detail.

Annex I

AI Governance Dictionary

General Data Protection Regulation (GDPR)	*The Regulation that provides legal obligations and guidance on data protection and data privacy requirements.*
Data Protection Impact Assessment (DPIA)	*The data processing results in potential high-risk to the rights and freedoms of users, then DPIA must be carried out by controllers. The assessment aims to identify the potential risk to user's fundamental rights, and to minimize such risk prior to the impact.*
Fundamental Rights Impact Assessment (FRIA)	*The assessments aim to identify specific risks to individuals' rights and necessary measures to be taken in the event of a risk. The deployers should assess the impact before the high-risk AI system is deployed.*
Creative Commons (CC) Copyright	*Specify how data can and cannot be reused.*
AI4SG (Artificial Intelligence for Social Good)	*AI4SG refers to an approach in which artificial intelligence systems are designed to prevent or reduce problems that could negatively affect human life or the natural environment. It also encompasses the development, design, and deployment of AI in ways that promote socially beneficial, ethically preferable, and environmentally sustainable outcomes.*
ACM (Association for Computing Machinery)	*A global association for computing professionals established in 1947. The ACM promotes computing as both a scientific discipline and a professional field through its journals, conferences, and standard-setting activities, and is widely recognised for its Code of Ethics and Professional Conduct, which supports responsible and ethical practice in technology.*
Prompt injection	*A method in which someone adds additional hidden counterfactual instructions to an AI system's prompt in order to induce responses in a way that was not intended by the original prompt.*
Fraud detection	*A domain that analyses data to identify and prevent dishonest or illegal activities (e.g. fake transactions, identity theft).*
Multi Factor Authentication (MFA)	*A tradition security mechanism for validation where users must validate their identity with two or more verification steps (e.g. log in with a password and then provide a code valid for 10 seconds sent to their phone).*

More AI terms' definitions, explanations and examples, please check AI Literacy Playbook for PMs.

Annex II

Classification of High-Risk AI

Figure 1. Classification of High-Risk AI: Check if it is a High-Risk AI, or Not?

Governance for High-Risk AI Systems: Compliance Mechanism under AI Act

Compliance Requirements under AI Act	Potential Actions from SMEs
Risk Management System *It is important for the risk management system to be established as a continuous mechanism throughout the whole life cycle of the AI system.*	Be responsible for conducting regular systematic reviews and updating on • Reasonably foreseeable (potential) risks posed to patients' health, safety and fundamental rights, • Evaluation of other risks that have been identified from the post-market surveillance.
Data & Data Governance *As the AI system is developing, companies should ensure that all the training, validation and testing datasets are subjected to quality criteria whenever such data is used.*	Should ensure that AI systems are trained on data sets that are sufficiently broad and cover all relevant scenarios, so that they will not pose a risk to fundamental rights or the health and safety of their customers.
Technical Documentation	Must ensure relevant technical documentation from before the AI system is placed on the market and keep it up-to-date throughout the life cycle of AI.
Record-Keeping *Ensure, at least, the level of traceability of the functioning of a high-risk AI system, as well as the intended purpose of the system AI, and logging capabilities.*	Providers have an obligation to: • Identifying situations that may result in a high-risk AI system; • Facilitating the post-market monitoring; • Monitoring the operation of high-risk AI systems as a part of the requirements of high-risk AI systems.
Transparency & Information to Deployers *Should provide information about the high-risk AI system in a proactive manner.*	Information should go beyond the mere explanation of the capabilities and functionalities of the AI system, such as: • Expected to function as intended, and the expected level of accuracy in achieving the specified purpose. • Instructions for use of AI should be concise, complete, correct and clear information that is relevant, accessible and comprehensible to the deployer.
Human Oversight	May ensure the trustworthiness of their AI system by establishing appropriate involvement of humans in the high-risk AI procedure. The type and degree of human oversight may vary: 1. Reviewing and validation by humans afterwards 2. Effective AI output with the possibility of human intervention afterwards 3. Monitoring AI systems and the possibility of interference in real-time.
Accuracy, Robustness and Cybersecurity *Ensure, at least, the mere requirements are in place for the robust and accurate AI system throughout the entire lifecycle*	• The outputs should be reproducible. • An AI system should adequately deal with errors or inconsistencies. • AI systems should be resilient against both overt attacks and more subtle attempts to manipulate data.

Annex III

A. E-Commerce Company

Company Context:
A 100-person Luxembourg-based e-commerce company, GreenWorld Supplements, markets vitamins, herbal teas, protein powders, organic dietary supplements, and skincare products to a customer base of approximately 120,000 active users. The company's growth strategy leans heavily on personalisation and automated arrangement.

Its AI-driven systems contain:

- **RecoWell:** a recommendation engine that personalises supplement offers across the website, mobile app, and marketing emails.
- **SmartDiscounts:** a dynamic pricing and bundling system optimising recommendations based on seasonal need or supply.

Operations are headquartered in Luxembourg and serve consumers across the EU (covered by GDPR and the EU AI Act). Since the system utilises personal and potentially health-related data for individualised suggestions, it is located near the "limited to high-risk" limitation under the EU AI Act.

A1. Business Context

AI Solutions in detail

- **Recommendation Engine:** Suggests supplements based on what users look at, buy, or say about their health goals.
- **Personalised Marketing Emails:** Send weekly product suggestions made for each user.
- **Dynamic Discounting:** Changes discounts and deals in real time to manage stock and boost sales.
- **Chatbot:** Responds to frequently asked questions regarding dosage, delivery options and product sourcing.
- **Inventory Prediction:** Forecasts seasonal demand trends (e.g., Vitamin D & C in winter or sunscreens in summer).
- **Future Goals:** Integrate wearable health data for personalisation, expansion of recommendation models to wellness subscriptions.

Business Goals

- **Conversion:** Increase the rate of visitors turning into buyers.
- **Basket Size:** Suggest products that work well together, such as Vitamin D with Vitamin C in winter or sunscreen with after-sun skincare.
- **Retention:** Keep customers coming back by giving simple, useful wellness tips and a good overall experience.
- **Sustainability:** Promote environmentally responsible choices by highlighting organic, recyclable, or fair-trade certified products within AI-generated suggestions.

Stakeholders

- **Internal stakeholders:** IT and data teams build and protect the system. Marketing uses it for product suggestions and emails. Compliance and legal teams ensure rules are followed. Management makes the main decisions. Customer service talks to users and solves problems.
- **External stakeholders:** Customers use the system and need to trust it. Suppliers care about how their products are shown. Regulators check if the company follows the law. Tech partners help keep the system running.
- **AI risks impacting stakeholders:** Problems like data leaks, unfair suggestions, unclear decisions, or breaking the rules can affect everyone above.

A2. Governance Risks

Data Sensitivity: The system uses personal data that might show health details. To protect privacy, users should give clear consent before data is collected. Data should be kept anonymous, and only what's needed should be stored. Storage and use must follow privacy rules, or there could be legal and trust problems.

Decision Automation: The system makes suggestions and prices automatically based on user actions. If this includes health info, it can be risky under GDPR rules and may hurt user trust.

Human Oversight: The system makes product and price decisions on its own. Over time, it might make mistakes or biased choices. People should regularly check the results and step in if needed to keep things fair and legal.

Bias and Harm: Sometimes the system may suggest more costly items or show different results to different people. Checking it often helps keep things fair and reliable.

Security & Resilience: The system stores private data, so it needs strong protection. Good access control, encryption, and backups help avoid data leaks and keep it working well.

Regulatory & Contractual: Following rules like GDPR and the EU AI Act is very important. But these rules can change and make planning hard. Staying transparent, ethical, and compliant is key.

Transparency & Explainability: Customers may not know why certain products are shown. The system should give a short, clear reason, for example, "you viewed this before," "similar to what you liked," or "popular now." It should also let users choose to see regular (non-personalised) options.

B. FinTech Company

B1. Business Context

This case focuses on a small fintech company based in the European Union. The firm has about twenty five employees and develops software that helps banks and small businesses handle financial decisions more securely.

At the heart of its operations are two products:

- **FraudGuard** is used to spot irregular payment activities and flag potential fraud before transactions are completed.
- **CreditRisk Support** is a decision support tool that helps credit officers review loan applications more consistently.

Since both platforms process sensitive financial information, they are required to comply with European frameworks such as the AI Act and the GDPR, which together promote transparency, accountability, and strong safeguards for data protection.

AI solutions:

- **Current:** The AI team has built models that automatically flag possible fraud and assist with credit scoring. Human officers make the final call before a loan is accepted or declined.
- **Potential:** The next stage focuses on adding multilingual explanations, adaptive risk scoring, and more detailed traceability, in line with the ISO/IEC 42001 standard for AI management.

Stakeholders

- **Internal stakeholders:**
  - The AI and IT team manages data security, model performance, and regulatory compliance.
  - The Risk and Compliance team reviews fairness, bias, and data handling in line with EU regulations.
  - The management team approves updates and oversees incident response if systems behave unexpectedly.
- **External stakeholders:**
  - The systems are used by partner banks and small or medium sized business clients. They also process information that belongs to individual users, whose financial data forms part of daily operations.
- **AI risks affecting stakeholders:**
  - Any issue in the system could impact clients, partner banks, or even the internal AI and management teams. Regulators may also be affected if compliance gaps appear or reports are incomplete.

B2. Governance Risks

Data Sensitivity: Fraud and credit data contain personal and financial details that require careful handling. If those records are stored or shared improperly, it could lead to privacy concerns and breaches of GDPR obligations.

Decision Automation: When scoring or fraud detection runs entirely on its own, the system can make mistakes or overlook important context. For this reason every flagged case is double checked by a human analyst before any action is taken.

Human Oversight: Analysts regularly check AI outputs, and no loan is declined automatically. Flagged transactions are constantly reviewed by a qualified officer.

Bias and Fairness: Even when a model performs well overall, it can quietly start favouring certain regions or customer types. These shifts are not always apparent at first. The team now reviews approval data by group each month to catch slight imbalances early before they turn into real fairness problems.

Security and Resilience: There is always a chance that a system could be breached or some data could slip through. If that happened, private financial details might be exposed. To reduce that risk, the company tests its defences regularly and keeps recovery plans ready so that operations can continue with minimal disruption.

Regulatory and Contractual: Incorrect or biased outputs could expose the company to financial loss or legal scrutiny. Maintaining documentation and audit logs helps demonstrate compliance with the AI Act and ISO/IEC 42001.

Transparency and Explainability: Trust will erode if users cannot understand why a decision was made. Clear summaries and appeal options accompany each credit decision.

C. HR Tech Company

C1. Business Context

This case is about a company that makes AI-powered tools for hiring and managing employee performance in the field of human resources technology.
The company has about forty employees and mostly works with medium-sized clients in the UK and EU, but it also has some partnerships in the US.

The two main systems of the company are:

- **RecruitRanker** is an AI-powered platform that looks at job applicants and finds people who might be a good fit for open positions.
- **PulseSignals** is a tool that helps managers find early signs of how well their employees are doing and how engaged they are.

The EU AI Act says that both systems are high-risk because they deal with sensitive personal and employment information (worker management, employment, and access to self-employment). They also follow the UK/EU GDPR, especially Article 22, which deals with automated decision-making. The Equality Act 2010, and for U.S. clients hiring in New York City, Local Law 144, which requires bias audits and candidate notices.

Business Goals:

- Make shortlists faster without giving up quality or fairness.
- Make sure that every candidate has an equal chance and reduce bias.
- Use clear, simple language to explain things and make it easy for people to ask for reviews or appeals.
- Show both clients and authorities that you are responsible and follow the rules.
- Use structured human oversight to responsibly scale your business.

AI Solutions

- **Current:**
  - The AI team has made models that help them rank applicants and find possible problems with their performance. Automation makes decisions faster, but human managers still review and approve all hiring and evaluation results.
- **Future plans:**
  - The next step is to make multilingual transparency notices, adaptive bias-monitoring dashboards, and full traceability throughout the AI lifecycle, all in line with ISO/IEC 42001 standards for responsible AI management.

Stakeholders

- **Internal stakeholders**
  - **AI & IT Team:** Oversees data management, model performance, and compliance with the AI Act and GDPR.
  - **HR & Compliance Team:** Ensures fairness, lawfulness, and unbiased data processing.
  - **Management Team:** Handles incident response, approves system updates, and enforces accountability.
- **External stakeholders**
  - **Client Organisations:** Use the platform to hire people and analyse their workforces.
  - **Candidates and Employees:** People whose personal information is used to hire or evaluate them.
  - **Regulators:** May look over documents to make sure they follow AI, data protection, and equality laws.
- **Risks to stakeholders:**
  - Mistakes, security breaches, or bias could hurt candidates' chances of getting a job, hurt client relationships, or make people less likely to trust the company. If rules about openness, fairness, or paperwork aren't followed, regulators may step in.

C2. Governance Risks

Data Sensitivity: Performance data, résumés, and interview notes contain personal information that must be processed in accordance with the strict data minimisation, purpose limitation, and security requirements of the GDPR and EU AI Act.

Bias and Fairness: Algorithmic ranking can unintentionally advantage or disadvantage certain demographic groups. To identify and address such issues, the company conducts regular fairness reviews and parity checks to maintain equal treatment for all candidates.

Automated Decision-Making: AI systems assist with shortlisting and performance flagging, but human managers make all final hiring and evaluation decisions. This prevents fully automated outcomes and ensures compliance with Article 22 of the GDPR and Article 14 of the AI Act.

Transparency and Explainability: Candidates receive clear, accessible disclosures about the use of AI in recruitment and evaluation. They can also request explanations for AI-assisted outcomes to maintain trust and fulfil legal transparency obligations.

Human Oversight: Trained analysts and hiring managers regularly review AI outputs. Escalation protocols specify when automation must be paused or overridden, ensuring that accountability and human judgment remain central.

Security and Resilience: As a smaller vendor handling sensitive HR data, the company applies strong encryption, access controls, and incident response procedures to prevent data breaches or unauthorised access

Compliance with Laws and Contracts: The company maintains Data Protection Impact Assessments (DPIAs) under the GDPR and Fundamental Rights Impact Assessments (FRIAs) under the AI Act. It documents bias audits, proof of human review, and model monitoring to demonstrate ongoing legal compliance and responsible governance.

D. Legal Company

D1. Business Context

A legal firm that has specialised in various fields of law, including labour law, consumer protection law and contract law. This firm is located and functions in the European Economic Area, with 100 employees, and makes a revenue of about 17 million euro per year.

AI solutions

- **Current:** The IT department in the law firm has developed a legal chatbot with the goal of efficiently managing repetitive and simple enquiries, including answers to factual questions, providing legal information to search and identifying case references.
- **Potential:**The IT department is also planning to enhance the features of the developed AI system. For the future potentials the chatbot will be able to handle the client onboardings, multilingual support, and tailored answering based on the given facts.

Stakeholders

- **Internal stakeholders:** Responsible for the functioning of the chatbot are
  - The IT department, who is responsible for the security management of digital components, and compliance of the chatbot, and
  - Management team, who is responsible for the legal compliance of the chatbot and the Representatives, who handle the complaints from the users.
- **External stakeholders: A**ffected by the chatbot can be clients, who are non-legal persons and the targeted users of the chatbot.
- **AI risks impacting stakeholders:** Clients, IT department, Management team, potential competitors.

D2. Governance Risks

Data Sensitivity: users who want to delete or withdraw their chat could face privacy invasion issues.

Decision Automation: AI systems that provide answers/explanations that are incorrect, or made up without human intervention/approval can cause governance risks.

Human Oversight: The legal team regularly reviews the chatbot's responses, and in complex/high-risk situations, or when answers are the result of hallucinations, users are advised to consult directly with a lawyer.

Bias and Harm: The chatbot may mistakenly generate responses that reflect discriminatory biases, potentially resulting in breaching users' rights and leading to data protection violations. (e.g. in labour law, it frequently results in biased outcomes that favour either the employee or the employer. Or responses based on gender)

Security & Resilience: To some extent, customers may share sensitive data in chats, and unauthorised access could cause damage to the firm.

Regulatory & Contractual: If the chatbot provides incorrect replies, the legal firm may face legal actions, and in case of any technical or legal failures in the management of an AI system will essentially cause reputational damage for the company, who is aiming to grow.

Transparency & Explainability: The users may not trust the answers of the chatbot, or may not be convinced enough.

References

Corporate Governance and Implementation Resources

- Australian Institute of Company Directors. (n.d.). AI governance checklist for SME and NFP directors. *https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-resources/ai-governance-checklist-sme-nfp-directors-web.pdf*

European Union AI and Data Protection Law

- European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on artificial intelligence (Artificial Intelligence Act) 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) 2016/798. Official Journal of the European Union, L 168, 1–191. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. *https://eur-lex.europa.eu/eli/reg/2016/679/oj*

International AI Governance and Ethics Frameworks

- Bettoni, A., et al. (2021). An AI adoption model for SMEs: A conceptual framework. *IFAC-PapersOnLine, 54*(1), 702–708.
- Cheong, C. (2024). Transparency and accountability in AI systems. *Frontiers in Human Dynamics.* https://www.frontiersin.org/journals/human-dynamics/articles/10.3389/fhumd.2024.1421273/full
- Organisation for Economic Co-operation and Development. (2019). *OECD AI principles*. https://oecd.ai/en/ai-principles
- Rožman, M., Oreški, D., Crnogaj, K., & Tominc, P. (2023). *Agility and artificial intelligence adoption: Small vs. large enterprises. Naše Gospodarstvo/Our Economy, 69*(4), 26–37. https://doi.org/10.2478/ngoe-2023-0021
- Shorenstein Center on Media, Politics and Public Policy. (2024). *The CLeAR documentation framework for AI transparency: Recommendations for practitioners, context, and policymakers* (K. Chmielinski, Author). Harvard Kennedy School. https://shorensteincenter.org/clear-documentation-framework-ai-transparency-recommendations-practitioners-context-policymakers/

International Standards and Risk Frameworks

- ISO. (2023). *ISO/IEC 42001: Artificial intelligence — Management system standard.* International Organization for Standardization. https://www.iso.org/standard/42001
- ISO. (2023). *ISO/IEC 23894: Artificial intelligence — Guidance on risk management*. International Organization for Standardization. https://www.iso.org/standard/77304.html
- National Institute of Standards and Technology (NIST). (2023). *AI risk management framework (AI RMF 1.0)* [NIST.AI.100-1]. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
- National Institute of Standards and Technology (NIST). (2023). *NIST AI RMF playbook*. https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook
- National Institute of Standards and Technology (NIST). (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile*. https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence
- National Institute of Standards and Technology. (2023). *AI risk management framework*. U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework

United Kingdom AI and Data Governance

- Government of the United Kingdom. (2025, June 27). Data (Use and Access) Act 2025: data protection and privacy changes. https://www.gov.uk/guidance/data-use-and-access-act-2025-data-protection-and-privacy-changes
- Information Commissioner's Office (ICO). (n.d.). Data (Use and Access) Act 2025. https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/
- Information Commissioner's Office (ICO). (n.d.). A guide to the data protection principles (UK GDPR). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/
- Information Commissioner's Office (ICO). (n.d.). A guide to data security (Article 32). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/
- Information Commissioner's Office (ICO). (n.d.). Contracts and liabilities between controllers and processors (UK GDPR). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/
- Information Commissioner's Office (ICO). (n.d.). Processors checklist. https://ico.org.uk/for-organisations/advice-for-small-organisations/getting-started-with-gdpr/data-protection-self-assessment-medium-businesses/processors-checklist/
- Information Commissioner's Office (ICO). (n.d.). Personal data breaches: A guide (72-hour rule). https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/
- Information Commissioner's Office (ICO). (n.d.). *When do we need to do a DPIA?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/
- Information Commissioner's Office (ICO). (2025, under review). *Rights related to automated decision-making, including profiling (Article 22).* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/
- Information Commissioner's Office (ICO) & Alan Turing Institute. (n.d.). *Explaining decisions made with artificial intelligence.* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/

United States Privacy Regulations

- California Privacy Protection Agency (CPPA). (n.d.). *California privacy regulations.* https://cppa.ca.gov/regulations/
- Colorado Office of the Attorney General. (n.d.). *Colorado Privacy Act.* https://coag.gov/resources/colorado-privacy-act/
- Virginia Office of the Attorney General. (2023, February 2). *Virginia Consumer Data Protection Act (CDPA): Summary. https://www.oag.state.va.us/consumer-protection/files/tips-and-info/Virginia-Consumer-Data-Protection-Act-Summary-2-2-23.pdf*

Environmental Framework

- *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 (pp. 3645–3650). Florence, Italy: Association for Computational Linguistics. https://aclanthology.org/P19-1355/*
- *Schwartz, R., Dodge, J., Smith, N. A., & Etzioni, O. (2020). Green AI. Communications of the ACM, 63(12), 54–63. https://doi.org/10.1145/3381831*
- *Patterson, D., Gonzalez, J., Le, Q., Liang, C., Munguia, L. M., Rothchild, D., ... & Dean, J. (2021). Carbon emissions and large neural network training. arXiv preprint arXiv:2104.10350*
- *Li, N., Ma, T., & Deng, X. (2024). Analysis of the coupling degree between regional logistics efficiency and economic development coordination. PLoS One, 19(1), e0293175.*

E-Commerce Company Use-Case

- Mohd Rasdi, R., & Umar Baki, N. (2025). Navigating the AI landscape in SMEs: Overcoming internal challenges and external obstacles for effective integration. *Plos one*, *20*(5), e0323249.
- European Commission, "Ethics Guidelines for Trustworthy AI" (AI HLEG, 2019) https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
- OECD AI Principles (2019) https://oecd.ai/en/ai-principles
- Floridi, Luciano, and Josh Cowls. "A unified framework of five principles for AI in society." *Machine learning and the city: Applications in architecture and urban design* (2022): 535-545.

FinTech Company Use-Case

- AI Act - Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union.
- GDPR - Regulation (EU) 2016/679. *General Data Protection Regulation.* Official Journal of the European Union.
- ISO/IEC 42001 - ISO/IEC 42001:2023. *Artificial Intelligence Management System Standard.* International Organization for Standardization.

HR Tech Company Use-Case

- EU AI Act — official text (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
- EU AI Act — Annex III (employment high-risk): https://artificialintelligenceact.eu/annex/3/
- EU AI Act — Article 14 (Human oversight): https://artificialintelligenceact.eu/article/14/
- UK GDPR — automated decision-making & profiling (ICO): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/
- Explaining decisions made with AI (ICO & The Alan Turing Institute): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/
- Equality Act 2010 (GOV.UK overview): https://www.gov.uk/guidance/equality-act-2010-guidance
- NYC Local Law 144 (AEDT): https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page
- Kaminski, M. (2023). Regulating The Risks Of Ai. Boston University Law Review, 103(5), 1347-1411.

Legal Company Use-Case

- 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) [2024] OJ L 2024/1689.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). OJ L 2016/119.
- European Commission, 'AI Act' Shaping Europe's Digital Future <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed on 28 September 2025.
- Casimir Rajnerowicz, 'The Professional's Guide to Legal AI Chatbots: Advancing Practice with Conversational AI' (22 May 2025, V7) <https://www.v7labs.com/blog/legal-ai-chatbots> accessed on 28 September 2025.
- Council Bars and Law Societies of Europe, 'Guide on the use of Artificial Intelligence-based tools by lawyers and law firms in the EU' European Lawyers Federation <https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/Events/20220331_AI4L/EN_IT_Law_2022_Guide-AI4L_web.pdf> accessed on 28 September 2025.

Contact us!

Thank you for reading this research and opinion report. If you have any questions or would like to discuss our findings further, please don't hesitate to contact us.

+44 7400715479

info@huxai.tech

huxai.tech