



AI Governance, Made Simple

The business owner's 90-day plan for using AI safely, legally and with confidence.

Clear steps, ready-to-use templates and honest answers to "does this apply to me?". Built on the same body of knowledge that AI governance professionals study for the IAPP's AIGP certification, rewritten for people who run a business.

Danilo Stojkovic

PeritumAI | October 2026 | Free guide

General education, not legal advice. Law as of October 2026. Unofficial: not affiliated with, endorsed by or produced by the IAPP. AIGP is a trademark of the International Association of Privacy Professionals. You may share this guide freely in its complete, unchanged form.

Start here

The short answer. If your business uses AI, you need a small set of habits: know which AI tools you use, put one person in charge, set a few clear rules about data and checking, take extra care where AI touches customers or decisions about people, and look again every few months. For most small businesses that's a few pages and a few hours a month, not a compliance department.

Who this guide is for

You run or manage a business, roughly 1 to 250 people. You use AI tools, or your staff do, or you're about to. You're not a lawyer or a technologist, and you don't have time to become one.

You want to know three things: does any of this apply to me, what's the smallest sensible thing I should do, and in what order.

This guide answers those three questions. It also works if you're a manager in a bigger company who has been handed "AI governance" and needs a starting point.

How to use it

1. **Read Part 1 (about 20 minutes).** It explains what AI governance is and helps you work out how much of it you need. Take the 2-minute sizing check on page 6.
2. **Follow Part 2, the 90-day plan.** Fifteen steps in four phases. Each step says why it matters, what to do and how you know it's done. Each one is tagged with the level it's for, so you can skip what doesn't apply.
3. **Copy the templates in Part 3.** An AI tool list, a one-page AI policy, vendor questions, checklists and an incident plan. Fill them in and you have most of your paperwork.

Where this guide comes from

AI governance professionals study a shared body of knowledge, published by the IAPP (the International Association of Privacy Professionals) for its AIGP certification. It has four parts: what AI is and how organizations govern it, the laws, how AI is built, and how AI is bought and used.

Most business owners don't build AI. They buy it and use it. So this guide takes that body of knowledge and keeps the parts that matter to you, with the focus on the last part: using AI you got from someone else.

Please read. This is general education, not legal advice. Laws are described as they stood in October 2026, and AI law is changing fast, especially in the US. Where a decision has real legal or financial consequences, check with a qualified lawyer in your country. This guide is unofficial and isn't connected to the IAPP.

Contents

Part 1. Understand it

1. What AI governance actually is	five jobs
2. Where you're already using AI	more places than you think
3. How much do you need?	the 2-minute sizing check
4. Builder or user?	why your role decides your duties
5. Which rules might reach you	EU, US, UK and elsewhere

Part 2. Do it: the 90-day plan

Phase 1, days 1 to 14: see what you have	steps 1 to 3
Phase 2, days 15 to 30: set the rules	steps 4 to 7
Phase 3, days 31 to 60: make the risky uses safe	steps 8 to 11
Phase 4, days 61 to 90: keep it working	steps 12 to 15

Part 3. Use it: templates and checklists

T1 to T10	tool list, policy, vendor questions, checklists, incident plan
-----------	--

Part 4. Keep going

Ten common mistakes, when to call a professional, glossary, sources

Understand it

What AI governance is, how much of it you need, and which rules might apply to you.

1. What AI governance actually is

AI governance is how you make sure the AI your business uses helps more than it hurts, and that someone is responsible when it doesn't.

It sounds big. In practice it's five jobs:

- 1 Know what AI you use.** Keep a simple list of every AI tool and what it's used for. You can't manage what you don't know about.
- 2 Put someone in charge.** One named person owns the list, the rules and the decisions. In a small business that's often the owner or the operations lead.
- 3 Set clear rules.** Which tools are allowed, what data may never go in, and the rule that a person checks AI output before it's used.
- 4 Check before you trust.** Before AI talks to customers or helps decide about people, test it, ask the vendor hard questions and plan for mistakes.
- 5 Keep watching.** AI tools change, and so does how people use them. Review regularly, and have a plan for when something goes wrong.

Why AI needs its own rules

Normal software does what it's told, the same way every time. AI is different in ways that matter for a business:

- **It guesses.** AI produces the most likely answer, not a guaranteed right one. Chatbots can state wrong facts with total confidence. This is called "hallucination".
- **It learns from data, including the bad parts.** If past data was unfair, the AI can repeat that unfairness at scale.
- **It's hard to explain.** It's often hard to say exactly why an AI gave a particular answer.
- **It changes.** Vendors update their models, sometimes without telling you. A tool that worked last month can behave differently today.
- **It touches your data.** Whatever your staff type into an AI tool goes to the tool's provider. Depending on the settings, it may be stored or used to train future models.

What you get out of it

Fewer embarrassing or costly mistakes. Customer and client data that stays where it should. A ready answer when a client, partner or insurer asks "how do you use AI?". And staff who use AI more, not less, because they know what's allowed.

Good governance also makes AI safer to use for real work. Teams with clear rules usually move faster than teams that are unsure what they're allowed to do.

2. Where you're already using AI

You probably use more AI than you think. Many businesses say "we don't use AI" and then find a dozen tools. AI now hides inside ordinary software.

Check these places:

Where	Typical AI inside
Chat assistants	Public chatbots and AI assistants staff use for drafting, research, summaries and translations, often on personal accounts
Office and email software	Built-in writing assistants, meeting summaries, email suggestions
Meetings and calls	Recording, transcription and note-taking bots that join calls
Customer service	Website chatbots, automatic replies, ticket sorting
Sales and marketing	CRM lead scoring, ad targeting, AI-written copy, AI images and video
Hiring and HR	CV screening, candidate ranking, video interview analysis, performance tools
Finance	Invoice reading, fraud alerts, credit checks, forecasting
Software and IT	Coding assistants, security tools, AI features your developers add to your own product

Example. A 20-person online store said it used "one chatbot". A 15-minute staff survey found nine tools: two chat assistants on personal accounts, a meeting note-taker, AI product descriptions, an AI image tool, the help desk's auto-replies, the ad platform's targeting, a fraud filter from the payment provider and a free CV screener the manager had tried once.

Staff using AI tools the business hasn't approved is called **shadow AI**. It isn't a sign of bad staff. It's a sign that people find AI useful and nobody has told them the rules yet. Step 2 of the plan deals with it.

3. How much do you need? The 2-minute sizing check

Governance should match the risk. A five-person design studio and a bank both use AI, and their governance should look nothing alike. Too little is risky. Too much stops useful work and pushes people back to shadow AI.

Answer these eight questions. **Your level is the highest one you hit.**

#	Question	If yes
1	Do you or your staff use AI for internal work only, like drafting, summaries, research or code?	Level 1
2	Does personal data (about customers, staff or anyone else) or confidential client data go into AI tools?	Level 2
3	Does AI talk to customers or the public directly, like a website chatbot or automatic email replies?	Level 2
4	Do you publish AI-generated images, video, audio or articles?	Level 2
5	Does AI help decide things about people: who gets hired, promoted or fired, who gets credit, insurance, housing, a place in education, healthcare or public services?	Level 3
6	Do you sell a product or service with AI inside, or put your own brand on an AI tool?	Level 3
7	Are you in a regulated sector, such as finance, insurance, healthcare, legal, education or public services?	Level 3
8	Do you have customers, users or staff in the European Union, or do people there use your AI's output?	Add the EU items in section 5

Level 1: Basic

AI for internal work, no sensitive data.

- One owner
- A tool list
- A one-page policy
- A short staff briefing

About 1 to 2 days of work, then an hour a quarter.

Level 2: Careful

Personal data, customer-facing AI or published AI content.

- Everything in Level 1
- Vendor checks and settings
- Honest disclosure to customers
- Testing before launch
- An incident plan

About 4 to 8 days of work over 90 days.

Level 3: Serious

Decisions about people, selling AI, or a regulated sector.

- Everything in Level 2
- Impact assessments
- Human review of decisions
- Bias checks
- Professional legal advice

Plan for ongoing work and outside help.

Time estimates are rough guides for a business of about 10 to 50 people, not promises.

Honest note. Most small businesses land on Level 1 or 2. If that's you, you don't need committees, audits or expensive software. You need the steps in this guide tagged for your level, done properly.

4. Builder or user? Why your role decides your duties

Most businesses are users of AI, not builders. That matters, because laws put the heaviest duties on the companies that build AI and sell it.

The EU AI Act uses two words you'll see a lot:

- **Provider:** the company that develops an AI system, or has it developed, and offers it under its own name. Think of the company behind a chatbot or a CV-screening product.
- **Deployer:** an organization that uses an AI system under its own authority, for work. That's probably you.

US laws often use "developer" and "deployer" in a similar way.

You can become a provider by accident

Under the EU AI Act, a business that uses or resells AI is treated as the provider of a high-risk system if it does one of three things (Article 25):

1. puts its own name or brand on a high-risk AI system someone else made
2. makes a significant change to a high-risk system that the original maker didn't plan for
3. uses an AI system, even a general chatbot, for a high-risk purpose it wasn't meant for, such as screening job applicants

Example. A recruitment agency builds a CV-ranking tool on top of a general AI model and sells it to employers under its own brand. For that tool, the agency is the provider, with provider duties, even though it never trained a model. The employers who use it are deployers.

These rules cover high-risk systems and apply once the high-risk rules start: 2 December 2027 for uses like hiring and credit, 2 August 2028 for regulated products. Even so, before you add AI to something you sell, or rebrand an AI tool, pause and get advice. It's an easy way to take on big duties without noticing.

5. Which rules might reach you

Two things to remember. First, the laws you already follow still apply when AI is involved: privacy, discrimination, consumer protection, contracts, copyright and product safety. "The AI did it" is not a defense. Second, the new AI-specific laws mostly target a few things: banned uses, high-risk uses like hiring and credit, and being honest that AI is involved.

Real case. In 2024, a Canadian tribunal ruled against Air Canada after its website chatbot gave a customer wrong information about a bereavement fare discount. The airline argued the chatbot was responsible for its own words. The tribunal disagreed: the company is responsible for all the information on its website, chatbot included (Moffatt v. Air Canada, 2024 BCCRT 149).

Laws that apply almost everywhere

Area	What it means for your AI use
Privacy and data protection	If personal data goes into AI, privacy law applies: tell people, have a lawful reason, use only what you need, keep it secure, and use a proper contract with the AI vendor. In the EU and UK this is the GDPR (General Data Protection Regulation). Many other countries have similar laws.
Discrimination	Hiring, lending, housing and insurance decisions must not be unfair to protected groups, whether a person or a tool made them. You can be responsible for a vendor's biased tool.
Consumer protection	Don't make claims about AI you can't back up, like "our AI guarantees results". In the US, the Federal Trade Commission (FTC) has acted against companies for deceptive AI claims, for example in its "Operation AI Comply" announced in September 2024.
Confidentiality and contracts	Putting client documents into a public AI tool may breach your contracts or professional duties, even if no law mentions AI.
Copyright	Who owns AI output, and whether the AI was trained on others' work, is still being fought over in courts. Check the tool's terms, and be careful with AI images and text you publish commercially.

The European Union: the EU AI Act

The EU AI Act is the most detailed AI law so far. **It can apply to you even if your business isn't in the EU**, for example if you offer AI to people in the EU or the AI's output is used there (Article 2). It sorts AI by risk:

Category	What it covers	When (law as of Oct 2026)
----------	----------------	---------------------------

Banned	A short list of practices, including social scoring, reading the emotions of workers or students (except for medical or safety reasons), harmful manipulation, exploiting vulnerable people and building face databases by scraping images (Article 5)	Since 2 February 2025. Two more bans, on AI that creates non-consensual sexual images of real people or child abuse material, apply from 2 December 2026.
High-risk	AI used in sensitive areas such as hiring and managing workers, credit scoring, life and health insurance pricing, education and essential services (Annex III), and AI inside regulated products such as medical devices (Annex I)	2 December 2027 (Annex III) and 2 August 2028 (Annex I). These were moved by a 2026 amendment; older guides say 2026 and 2027.
Transparency	AI that talks to people must be built so they know it's AI: a duty on the maker (provider), and on you if you built or brand the chatbot. Whoever publishes a deepfake must label it. AI-generated text published to inform the public on matters of public interest must be disclosed, unless a person reviewed it and takes editorial responsibility (Article 50).	From 2 August 2026
Everything else	Most business AI: writing assistants, spam filters, most recommendations	No extra duties beyond AI literacy

AI literacy (Article 4). Since 2 February 2025, any organization that uses AI in the EU must take measures to support AI literacy among its staff and others using AI on its behalf. In plain words: people need enough understanding of the AI they use, for the way they use it. There's no exam, certificate or fixed number of hours. A 2026 amendment softened the original wording, which required organizations to "ensure" a sufficient level. Step 7 covers this.

If you use a high-risk system, from 2 December 2027 (Annex III uses) or 2 August 2028 (Annex I products), the deployer duties include: use it as the instructions say, give oversight to trained people with the authority to step in, make sure the input data you control is relevant and representative enough, monitor it, stop using it and tell the provider and the regulator if it presents a risk, report serious incidents, keep its logs for at least six months, tell workers before using it at work, and tell people when it helps make decisions about them (Article 26). Deployers that use high-risk AI for credit scoring or for life and health insurance pricing, and public bodies, must also do a fundamental rights impact assessment before first use (Article 27).

Maximum fines are EUR 35 million or 7% of worldwide turnover for banned practices, EUR 15 million or 3% for most other duties, and EUR 7.5 million or 1% for giving regulators false or misleading information. For small and medium-sized businesses, the maximum is whichever of the two amounts is lower (Article 99). Actual fines depend on how serious the breach was, the company's size and how it cooperated.

The United States

There's no broad federal AI law. Existing laws apply, enforced by agencies such as the FTC (consumer protection) and the Equal Employment Opportunity Commission (discrimination at work). On top of that, states and cities add their own rules. Some examples, status as of October 2026:

- **New York City (Local Law 144):** automated tools that substantially help hiring or promotion decisions need a yearly independent bias audit, a published summary and notices to candidates.
- **Illinois:** its Human Rights Act bans discriminatory use of AI in employment decisions and requires notice to workers, from January 2026. Illinois also regulates AI analysis of video interviews.
- **California:** for businesses covered by its privacy law (broadly, those with yearly revenue above about USD 25 million, adjusted for inflation, or that trade in large amounts of personal data), rules on automated decision-making technology for significant decisions, such as jobs, housing, lending and healthcare, with compliance due by 1 January 2027.
- **Colorado:** its 2024 AI Act was repealed and replaced in May 2026 by a narrower law focused on notices and consumer rights, effective 1 January 2027.
- **Texas and Utah:** Texas's Responsible AI Governance Act (in force January 2026) mainly limits government uses and bans certain intentionally harmful uses. Utah requires disclosing generative AI to consumers in some situations.

US state AI law changes month to month, and federal action against state AI laws adds uncertainty. Check the current status before you rely on any date here.

The UK and elsewhere

- **United Kingdom:** no general AI law as of October 2026. Existing regulators apply existing law to AI, especially the UK GDPR, enforced by the Information Commissioner's Office (ICO). Its rules on automated decisions changed on 5 February 2026 (Data (Use and Access) Act 2025): decisions made only by a machine with significant effects are now generally allowed with safeguards, such as telling people, letting them challenge the decision and offering a human review. Stricter rules remain for sensitive data such as health data.
- **South Korea:** a framework AI law (the AI Basic Act) with rules for high-impact AI and labeling of generated content.
- **Everywhere else:** most countries have a privacy law, consumer law and anti-discrimination law that already cover your AI use. Many are adding AI-specific rules. A quick check with a local adviser is worth it if AI touches customers or decisions about people.

What this means for most businesses. If you use AI for everyday work, your main legal duties are the ones you already have: protect personal and client data, don't mislead customers, don't discriminate. Add AI literacy if you operate in the EU, and labeling if you publish deepfakes or AI-written news-style content. Telling customers they're talking to AI is good practice everywhere. The heavy rules start when AI helps decide about people's lives.

PART 2

Do it: the 90-day plan

Fifteen steps in four phases. Do them in order. Skip a step only if its level tag doesn't apply to you.

Each step is tagged: **All** for every business, **Level 2+** if you scored Level 2 or 3, **Level 3** only for Level 3. Time estimates are rough, for a business of about 10 to 50 people.

PHASE 1 | DAYS 1 TO 14

See what you have

Goal: one person in charge, and a complete list of the AI you use, each item sorted by risk.

1 Put one person in charge

30 minutes **All**

Why: when everyone owns AI, nobody does. One owner makes decisions quickly and keeps the list current.

1. Name an AI owner. In a small business this is usually the owner, a director or the operations lead. They don't need to be technical. They need authority to say yes or no.
2. Write down what they decide: which tools are approved, which new uses need a closer look, and when to get outside advice.
3. Name a backup, and tell the whole team who to ask about AI.
4. Level 3: add a small review group. For example, the owner plus whoever handles legal or compliance, IT or security, and the business area using the AI (often HR). Meet monthly at first.

Done when: the team knows who the AI owner is and how to reach them.

2 List every AI tool you use

2 to 4 hours **All**

Why: this list is the base for everything else. Most businesses find tools nobody knew about.

1. Send staff a short, friendly survey: "Which AI tools do you use for work, for what, and do you put any client, customer or staff information into them?" Say clearly that nobody gets in trouble for past use. You want honesty, not hiding.
2. Check the places in the table in section 2: software subscriptions, your office suite's AI features, browser extensions, meeting bots, your website and help desk, HR and finance systems.
3. Ask your main software vendors which of their features use AI.
4. Put everything in the AI tool list (template T1). One row per use, not just per tool: the same chatbot used for marketing copy and for summarizing CVs is two different risks.

Done when: you have a list with every AI use, its owner, what data goes in and who is affected.

3 Sort each use: green, amber or red

1 to 2 hours **All**

Why: you can't give everything the same attention. Sorting tells you where to spend your effort.

1. Go through your list with the traffic-light questions (template T2).
2. **Green:** internal help, no personal or confidential data, a person checks the result. Allow it under your policy.
3. **Amber:** personal or confidential data, customer-facing, published content, or output used without much checking. Allow it with conditions: approved tool, business account, the checks in Phase 3.
4. **Red:** decisions about people's jobs, money, housing, health or education; anything on the EU banned list; anything that could seriously hurt someone if wrong. Pause or review it properly before it continues.
5. Stop anything clearly unsafe now. For example, confidential client files pasted into free chatbot accounts with training switched on.

Done when: every row in your list has a color, and every red item has a review date or has been stopped.

PHASE 2 | DAYS 15 TO 30

Set the rules

Goal: approved tools, a one-page policy, clear data rules, and a team that knows all three.

4 Choose your approved tools and set them up safely

Half a day **All**

Why: banning AI doesn't work. People just use it in secret. Giving them good, approved tools is what reduces shadow AI.

1. Pick a small set of approved tools that cover what people actually need (from your survey).
2. Use business or team accounts, not personal free accounts. They usually come with better data terms and admin controls.
3. Check the settings and the terms, and write the answers in your tool list:
 - Is your data used to train the provider's models? Switch it off where you can.
 - How long are your inputs kept? Where is the data stored?
 - Who in your company can see what others typed? Can you remove users when they leave?
4. Turn on sign-in protection (two-step login) for every AI account.
5. Set up a simple way to request a new tool: an email to the AI owner with what it is, what it's for and what data goes in.

Done when: your approved list is published to staff, and every approved tool has its data settings checked and recorded.

5 Write a one-page AI policy

2 hours **All**

Why: staff can't follow rules nobody wrote down. One clear page beats a 30-page document nobody reads.

1. Start from template T3 and adjust it to your business.
2. Cover: approved tools, data that never goes in, the rule that a person checks and owns every output, when to tell clients or customers AI was used, banned uses, and how to report a problem.
3. Keep it short and in plain words. If it doesn't fit on one or two pages, it's too long.
4. Have the owner sign it, date it, and set a review date in six months.

Done when: the policy is signed, shared with every staff member and saved where people can find it.

6 Draw a clear line on data

1 hour **All**

Why: data leaks are the most common real AI risk for small businesses. What goes into an AI tool leaves your control.

1. Use the data red list (template T4) and add anything specific to your business.
2. Decide three groups: never in any AI tool (for example passwords and card numbers), only in approved business tools (for example client documents), and fine anywhere (public information).
3. Teach one simple habit: remove names and identifying details before pasting, when the task doesn't need them.
4. Level 2+: if personal data goes into an AI tool, check with your privacy rules. You may need a processing contract with the vendor and an update to your privacy notice. If the use is high-risk for people, the GDPR may require a data protection impact assessment (DPIA), a structured check of the privacy risks (GDPR Article 35).

Done when: the red list is in your policy, and staff can say in one sentence what never goes into AI.

7 Brief your team

45 minutes, plus 10 minutes per new joiner **All**

Why: rules only work if people understand them and the reasons behind them. In the EU, supporting AI literacy is a legal duty for any organization that uses AI (EU AI Act Article 4).

1. Run a short session using the outline in template T9: what AI is good and bad at, your policy, your data rules, how to check output, how to report problems.
2. Show real examples from your own work: a good use, a wrong answer the AI gave confidently, a data mistake to avoid.
3. Give extra training to people who use AI for higher-risk tasks, such as anyone handling customer chatbots or HR tools.
4. Record who attended and when. A simple list is enough. It's your evidence that you took AI literacy seriously.
5. Add the briefing to onboarding for new staff.

Done when: everyone who uses AI has been briefed, and you have a record of it.

PHASE 3 | DAYS 31 TO 60

Make the risky uses safe

Goal: every amber and red use has been checked, and the right safeguards are in place before it runs.

8 Check your AI vendors

1 to 2 hours per important vendor **Level 2+**

Why: when you buy AI, its risks become partly yours. The vendor's AI may itself be built on another company's model and run on someone else's cloud.

1. For each amber or red tool, send the vendor questions (template T5), or find the answers in their documentation.
2. Watch for these warning signs: no clear answer on whether they train on your data, no information on how the tool was tested, no way to tell you about incidents or changes.
3. Put the important answers into the contract where you can: no training on your data without permission, notice before major changes, prompt incident notice, help with your own legal duties, and deletion of your data when you leave.
4. Diary a re-check. Vendors update their AI often. Review important vendors at least once a year and when they announce big changes.

Done when: every amber and red tool has answered vendor questions on file, and any gaps are either fixed in the contract or accepted in writing by the AI owner.

9 Make customer-facing AI honest and safe

Half a day per tool **Level 2+**

Why: a chatbot speaks for your business. If it gives wrong information, you can be held responsible, as the Air Canada case showed.

1. **Tell people it's AI.** Say so clearly at the start of the conversation. In the EU, from 2 August 2026, the chatbot's maker must build this in (Article 50). If you built the chatbot yourself or offer it under your own name, that duty may be yours. Either way, customers expect it. Label realistic AI-made or altered images, audio or video of real people, places or events (deepfakes): in the EU that's a duty for whoever publishes them.
2. **Limit what it can do.** Keep it to topics it can answer well. Don't let it make promises about prices, refunds, legal or medical matters unless the answers come from your approved content.
3. **Give people a way out.** An easy route to a human, and a clear way to complain.
4. **Test before launch.** Ask it 30 to 50 real customer questions, including awkward ones and attempts to trick it into ignoring its instructions. Check every answer. Fix what fails and test again.
5. **Watch it after launch.** Read a sample of real conversations every week at first, then monthly.

Use the launch checklist (template T6).

Done when: the checklist is complete and signed off by the AI owner before the tool goes live.

10 Keep a human in charge of decisions about people 1 to 3 days per use, plus advice **Level 3**

Why: this is where AI law is strictest and where harm is most serious. A biased hiring or credit tool can hurt many people quickly and expose you to discrimination claims.

1. **Assess before you use it.** Write down what the tool decides or recommends, who is affected, what could go wrong and what safeguards you'll use. If personal data is involved, a GDPR data protection impact assessment may be required. Template T7 gives you the questions.
2. **Make human review real.** The reviewer needs training, time and the authority to overrule the AI. A person who clicks "approve" on every recommendation is not oversight.
3. **Check for unfair results.** Compare outcomes across groups, such as men and women or older and younger applicants, using the vendor's test results and your own data. In New York City, hiring and promotion tools need an independent bias audit.
4. **Tell people.** Let applicants, staff or customers know AI is used, and how to ask for a human review. In the EU, people generally have the right not to be subject to decisions made only by a machine that seriously affect them (GDPR Article 22). In the UK, such decisions are generally allowed since February 2026, but only with safeguards like these.
5. **Get professional advice** before you start. The rules here depend heavily on your country, state and sector.

Done when: each people-decision use has a written assessment, a trained reviewer, a bias check, a notice to affected people and legal sign-off.

11 Keep your AI claims honest

1 hour **Level 2+**

Why: overstating what AI does, sometimes called "AI washing", can be a deceptive business practice. Regulators have taken action against it.

1. Review your website, sales material and proposals for claims about AI.
2. Remove or prove claims like "guaranteed", "unbiased", "100% accurate" or "replaces a lawyer".
3. Say plainly what the AI does and what a person still does.

Done when: every public AI claim is accurate and you could back it up if asked.

PHASE 4 | DAYS 61 TO 90

Keep it working

Goal: a plan for when things go wrong, a regular review habit, and simple records.

12 Plan for when AI goes wrong

2 hours **Level 2+** **simplified for All**

Why: something will go wrong eventually. A plan written in calm conditions works much better than one invented in a panic.

1. Use the incident plan (template T8). Decide what counts as an AI incident: wrong advice given to a customer, personal data leaked into a tool, unfair outcomes, offensive output, a tool being tricked or misused.
2. Make reporting easy and blame-free, so staff tell you early.
3. Know your off switch. For each amber or red tool, write down who can turn it off, how, and what you do instead while it's off.
4. Know your deadlines. A personal data breach under the GDPR must generally be reported to the regulator within 72 hours of becoming aware of it, unless it's unlikely to put people at risk (Article 33). Check your contracts and insurance policy for notice duties too.

Done when: the plan is written, the team knows how to report, and every amber or red tool has a named person who can switch it off.

13 Set a review rhythm

1 hour a quarter **All**

Why: AI tools change, vendors update models, and people find new uses. A tool that was fine in January might not be fine in June.

1. Put a quarterly AI review in the calendar. Use the checklist in template T10.
2. Update the tool list, check new tools, look at any incidents and complaints, and spot check a few real outputs.
3. Watch for "function creep": a tool slowly being used for things nobody approved, like a meeting note-taker starting to be used to judge staff performance.
4. Level 2+: for customer-facing and decision tools, track a few simple numbers, such as complaints, human overrides, error rates or answers that needed correcting.

Done when: the first quarterly review is in the calendar with an owner.

14 Keep simple records

1 hour to set up **All**

Why: if a client, insurer, regulator or court ever asks how you manage AI, records are your answer. Without them, good work looks like no work.

Keep one folder with:

- the AI tool list (T1) and the date of each change
- the signed AI policy and its versions
- training records: who, when, what
- vendor answers and contracts
- assessments and test results for amber and red uses
- incidents, what happened and what you changed
- review notes from each quarter
- Level 3, high-risk systems in the EU: logs kept for at least six months, once those rules apply (Article 26)

Done when: the folder exists and the AI owner knows what goes in it.

15 Run your 90-day review and plan the year

2 hours **All**

Why: this turns a project into a habit.

1. Check every step in this plan: done, not needed, or still open.
2. Ask staff what's working and what's getting in the way. Fix rules that slow good work for no reason.
3. Plan the next 12 months: quarterly reviews, the policy review at six months, yearly training refresh, yearly vendor re-checks, and any law dates that affect you (see section 5).
4. Level 3: consider a recognized framework to structure your program, such as the free NIST AI Risk Management Framework from the US National Institute of Standards and Technology, or the ISO/IEC 42001 standard, which organizations can be certified against.

Done when: you have a dated 12-month AI calendar.

The whole plan on one page

When	Steps	You end up with
Days 1 to 14	1 Owner. 2 Tool list. 3 Green, amber, red.	Someone in charge and a sorted list
Days 15 to 30	4 Approved tools. 5 One-page policy. 6 Data red list. 7 Team briefing.	Clear rules everyone knows
Days 31 to 60	8 Vendor checks. 9 Customer-facing AI. 10 People decisions. 11 Honest claims.	Safeguards on the risky uses
Days 61 to 90	12 Incident plan. 13 Review rhythm. 14 Records. 15 90-day review.	A habit that keeps going

Use it: templates and checklists

Copy these into your own documents or spreadsheet and adjust them to your business.

T1. AI tool list

One row per use. A spreadsheet is fine.

Column	What to write	Example
Tool and vendor	Product name and company	Help desk chatbot, from your help desk software vendor
Use	What it's used for, in one line	Answers customer questions about orders and delivery
Business owner	Person responsible for this use	Customer service lead
Who uses it	Teams or roles	Customer service (setup); customers (chat)
Data that goes in	Types of data	Customer names, order numbers, messages
Who is affected	People the output touches	Customers
Account type and settings	Business or personal; training on or off	Business plan; training off; 30-day retention
Color	Green, amber or red (T2)	Amber
Safeguards	What you do to manage the risk	AI disclosure, human handoff, monthly sample review
Status and dates	Approved, trial, paused; last review	Approved; reviewed 2026-10

T2. Green, amber, red: the triage questions

Question	If yes
Does it help decide about someone's job, pay, credit, insurance, housing, education, healthcare or access to public services?	Red
Could a wrong output seriously hurt someone's safety, health, money or rights?	Red
Does it read emotions of staff, sort people by biometric data (face, voice, body) or monitor staff behavior?	Red (and possibly banned in the EU)
Does personal data or confidential client data go into it?	Amber
Does it talk to customers or the public, or publish content in your name?	Amber

Is its output used without a person checking it first?	Amber
Can it take actions by itself, like sending emails, making payments or changing records (an "AI agent")?	Amber , red if the actions are significant
None of the above	Green

T3. One-page AI policy (template)

[Business name] AI policy

Version _____ | Approved by _____ | Date _____ |
Next review _____

1. Why we have this policy

We use AI to work faster and better. This policy keeps our customers, our staff and our business safe while we do it. It applies to everyone who works for us, including contractors.

2. Who is in charge

Our AI owner is _____. Ask them before using a new AI tool or using an approved tool for something new.

3. Approved tools

Use only the tools on our approved list: _____. Always use your work account, never a personal account, for work tasks. To request a new tool, email the AI owner with what it is, what you want to use it for and what data would go in.

4. Data rules

Never put these into any AI tool: passwords and access codes, payment card and bank details, government ID numbers, health information, and anything a client has asked us to keep confidential. Client documents and personal data may go only into approved tools marked for that use. Remove names and identifying details when the task doesn't need them.

5. Check everything

AI can be wrong while sounding sure. A person must check every AI output before it is used, sent or published. The person who uses the output is responsible for it, not the AI.

6. Be open about AI

Tell customers when they are talking to an AI. Label realistic AI-generated images, audio and video. Tell clients when AI did a significant part of work for them, where they would expect to know or our contract requires it.

7. Not allowed without the AI owner's written approval

Using AI to make or recommend decisions about people (hiring, performance, pay, credit, pricing for individuals). Using AI to monitor staff. Connecting AI to our systems so it can act on its own. Putting AI into anything we sell. Any use our AI owner has listed as banned.

8. Report problems

If an AI tool gives harmful, unfair or wrong output that reached someone, or if data went where it shouldn't, tell _____ straight away. We want to know early. You won't be blamed for reporting a problem honestly.

T4. Data red list

Never in any AI tool	Only in approved business tools	Fine anywhere
<ul style="list-style-type: none">• Passwords, keys, access codes• Payment card and bank account details• Government ID numbers• Health, medical and genetic data• Anything under a confidentiality order or marked "do not share"	<ul style="list-style-type: none">• Client documents and contracts• Customer names and contact details• Staff records and CVs (and only for approved uses)• Internal financials• Unreleased product or pricing plans	<ul style="list-style-type: none">• Public information• Your published marketing• General questions with no names or details• Made-up example data

Adjust to your business. Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data used to identify someone, and data about health, sex life or sexual orientation gets extra protection under the GDPR (Article 9) and many other privacy laws.

T5. Twelve questions to ask an AI vendor

1. What exactly does the AI do, and what is it meant to be used for? What should it not be used for?
2. Do you use our data to train or improve your models? Can we switch that off, in writing?
3. How long do you keep our inputs and outputs? Where is the data stored? Can we delete it?
4. Which other companies' AI models, clouds or data does your product rely on? How will you tell us about changes?
5. How did you test it for accuracy? What are its known limits and failure cases?
6. How did you test it for unfair results across groups of people? Can we see the results?
7. How is it secured? Do you have independent security certifications or reports?
8. Will you tell us before major changes to the model, and how much notice will you give?
9. How and how fast will you tell us about incidents, errors or data breaches?
10. What documentation do you provide to help us meet our own legal duties, for example under the GDPR or the EU AI Act? Under the EU AI Act, what role and risk category do you consider your product to be? (The category can change with how you use it, so check it against your own use.)
11. Who owns the outputs? Do you protect us if a third party claims the output infringes their rights?
12. What happens to our data and our setup if we leave or you shut down?

T6. Customer-facing AI launch checklist

- ☐ Customers are told clearly, at the start, that they're dealing with AI
- ☐ Topics are limited to what it can answer well; it declines the rest politely
- ☐ Prices, refunds, legal, medical and safety answers come only from approved content, or go to a person
- ☐ A person is easy to reach, and there's a clear way to complain
- ☐ Tested with 30 to 50 real questions, including awkward ones and attempts to trick it; all failures fixed and retested
- ☐ It doesn't ask for more personal data than it needs; your privacy notice mentions it

- ☐ Vendor questions (T5) answered and on file
- ☐ Someone named reviews a sample of conversations on a set schedule
- ☐ You know who can switch it off, and what happens when it's off
- ☐ Realistic AI-made images, audio or video of real people, places or events are labeled
- ☐ AI owner has signed off. Date: _____

T7. Decisions about people: assessment questions

For any AI that helps decide about hiring, staff, credit, insurance, housing, education, healthcare or access to services. Write the answers down.

1. What does the tool decide or recommend, and what happens to a person as a result?
2. Who is affected, and are any of them vulnerable, such as children, older people or people in financial difficulty?
3. What data does it use? Could any of it stand in for a protected trait, like a postcode standing in for ethnicity?
4. What happens if it's wrong? How would you even notice?
5. Have outcomes been compared across groups? What did the vendor's tests and your own checks show?
6. Who reviews the AI's recommendations? Do they have the training, time and authority to overrule it? How often do they?
7. How are people told AI is involved? How can they ask for a human review, correct their data or appeal?
8. Which laws apply where you operate? Has a lawyer confirmed this?
9. Is a GDPR data protection impact assessment needed? In the EU, does the system count as high-risk under the AI Act?
10. Decision: go, go with conditions, or stop. Signed by the AI owner, with date and next review.

T8. AI incident plan (one page)

Stage	What to do
1. Report	Anyone who sees a problem tells _____ straight away by _____. Don't wait to be sure.
2. Contain	Stop the harm first. Pause or switch off the tool, take down the wrong content, remove access, use the fallback (manual process).
3. Assess	What happened, who is affected, how bad is it, is it still happening? Was personal data involved? Note the time you became aware.
4. Notify	Check who must be told: affected customers, clients under your contracts, your insurer, the vendor. For a personal data breach under the GDPR, the regulator generally within 72 hours, unless it's unlikely to put people at risk. Get advice if unsure.
5. Fix	Find the root cause: the tool, the data, the instructions, the people or the process. Fix it, test it, then restart.

6. Learn

Record what happened and what changed. Update the tool list, the policy or the training.
Share the lesson with the team, without blame.

T9. Staff briefing outline (45 minutes)

1. **What AI is good and bad at (10 min).** It's great at drafts, summaries and ideas. It guesses, can invent facts confidently and can repeat bias. Show one real wrong answer.
2. **Our rules (10 min).** Approved tools, work accounts, the one-page policy.
3. **Our data line (10 min).** The red list. Remove names when you can. What happens to what you type.
4. **Checking output (10 min).** Check facts, numbers, names, quotes and legal or medical claims. You own what you send.
5. **When something goes wrong (5 min).** How to report, and why early reporting is safe and welcome.

Record attendees and the date. Repeat yearly and when tools or rules change.

T10. Quarterly AI review checklist

- ☐ Tool list updated: new tools, new uses, retired tools
- ☐ New tools checked and colored (T2)
- ☐ Any function creep spotted and dealt with
- ☐ Incidents and complaints reviewed; fixes done
- ☐ A few real outputs spot checked per amber or red tool
- ☐ Vendor changes and announcements checked
- ☐ New staff briefed; training records current
- ☐ Law changes in your markets checked (EU AI Act dates, US state laws)
- ☐ Policy still fits; changes noted for the next version
- ☐ Notes saved in the records folder. Next review date: _____

Keep going

Common mistakes, when to get help, the words you'll meet, and where the facts come from.

Ten common mistakes

The mistake	The better way
"We don't use AI."	You almost certainly do, inside ordinary software. Run the survey in step 2.
"We're too small for this."	Size changes how much you do, not whether. A small business needs a page of rules, not a program. And small businesses are often hit hardest by one bad mistake.
"The vendor is responsible."	The vendor is responsible for its product. You're responsible for how you use it, and for what it says to your customers.
Banning AI completely	Bans push use underground. Approved tools plus clear rules work better.
A 30-page policy nobody reads	One or two pages, in plain words, briefed to everyone.
Rubber-stamp human review	A reviewer who always agrees with the AI isn't oversight. Give them time, training and the power to say no.
Set it and forget it	AI tools and their uses change. Review every quarter.
Adding AI to your product without thinking about roles	Branding or selling AI can make you a provider, with much heavier duties. Get advice first.
Overselling your AI	Claims you can't back up are a legal risk. Say plainly what it does.
Panic about headline fines	Most business AI use is low risk. Do the steps for your level calmly and properly.

When to call a professional

This guide gets most businesses a long way. Get qualified legal or specialist help when:

- AI helps decide about people's jobs, credit, insurance, housing, education or healthcare
- you build AI into a product you sell, or put your brand on an AI tool
- you're in a regulated sector, such as finance, healthcare, insurance or legal services
- you process sensitive data, like health or biometric data, with AI
- an incident has affected customers or leaked personal data
- a client, investor or regulator asks for formal evidence of your AI governance

Glossary

AI system

Software that takes inputs and works out how to produce outputs, such as predictions, content, recommendations or decisions, rather than following only fixed rules a person wrote.

AI agent

An AI that can take actions by itself, like sending emails, booking things or changing records, not just answer.

AI literacy

The skills, knowledge and understanding to use AI in an informed way, and to be aware of its opportunities, risks and possible harm (EU AI Act Article 3(56)).

AI owner

The person in your business responsible for AI decisions. A role this guide recommends, not a legal title.

Bias (in AI)

When AI produces results that are systematically unfair to some groups of people.

Deepfake

AI-generated or AI-altered image, audio or video that looks like real people, objects, places or events and could falsely seem real (EU AI Act Article 3(60)).

Deployer

An organization that uses an AI system for work under its own authority. Most businesses.

DPIA (data protection impact assessment)

A structured check of privacy risks, required by the GDPR before processing that is likely to be high-risk for people.

Function creep

When a tool gradually gets used for purposes nobody approved.

GDPR

The General Data Protection Regulation, the EU's privacy law. The UK has its own version, the UK GDPR.

Generative AI

AI that creates text, images, audio, video or code.

Hallucination

When AI states something false as if it were true.

High-risk AI

Under the EU AI Act, AI used in sensitive areas such as hiring, credit or education, or inside regulated products. It carries the heaviest duties.

Human oversight

A person who understands the AI, watches it and can overrule or stop it.

Personal data

Any information about an identifiable person.

Provider

The company that develops an AI system, or has it developed, and offers it under its own name.

Shadow AI

AI tools staff use for work without the business approving them.

Sources

Laws and statutes as of October 2026. Article numbers refer to the EU AI Act as amended by Regulation (EU) 2026/1744 (consolidated text of 27 July 2026), unless stated otherwise.

- Regulation (EU) 2024/1689 (EU AI Act), as amended by Regulation (EU) 2026/1744: Arts. 2, 3(56), 4, 5, 25, 26, 50, 99, 113, Annexes I and III. eur-lex.europa.eu
- Regulation (EU) 2016/679 (GDPR): Arts. 9, 22, 28, 33, 35. eur-lex.europa.eu
- UK Data (Use and Access) Act 2025, UK GDPR Arts. 22A to 22D (in force 5 February 2026). legislation.gov.uk
- *Moffatt v. Air Canada*, 2024 BCCRT 149 (Civil Resolution Tribunal of British Columbia, February 2024)
- US Federal Trade Commission, "Operation AI Comply" (September 2024). ftc.gov
- New York City Local Law 144 of 2021, NYC Admin. Code 20-870 to 20-874, and rules at 6 RCNY 5-300
- Illinois HB 3773 (2024), amending the Illinois Human Rights Act; Illinois Artificial Intelligence Video Interview Act (820 ILCS 42)
- California Privacy Protection Agency, regulations on automated decision-making technology (2025)
- Colorado SB 24-205 (2024) and SB 26-189 (2026); Texas HB 149 (2025); Utah SB 149 (2024)
- Republic of Korea, Framework Act on the Development of Artificial Intelligence and Establishment of Trust (AI Basic Act)
- NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0), January 2023. nist.gov
- ISO/IEC 42001:2023, Artificial intelligence management system. iso.org
- IAPP, AIGP Body of Knowledge v2.1 (structure of topics only; no IAPP text reproduced). iapp.org

What next

You've finished the guide. The most useful thing you can do now is step 1: name your AI owner today, and send the staff survey this week.

If you want to go deeper, PeritumAI publishes free, plain-English resources on AI governance and safe AI use at **peritumai.com**.

Remember the five jobs: know what AI you use, put someone in charge, set clear rules, check before you trust, and keep watching. Do them in proportion to your risk, and write down what you did.

AI Governance, Made Simple. Danilo Stojkovic, PeritumAI, October 2026. General education, not legal advice. Unofficial and not affiliated with or endorsed by the IAPP; AIGP is a trademark of the International Association of Privacy Professionals. Free to share in complete, unchanged form.