MANAGING AI EXPOSURE IN YOUR BUSINESS

Once data is entered into a public AI tool, your business may lose control of how it is stored, processed or reused. That exposes your business to privacy breaches, loss of legal professional privilege and regulatory action. This factsheet outlines five key actions your business should undertake to reduce risk.

KNOW THE UK LEGAL FRAMEWORK

The UK has no single AI legislation. Regulators apply existing law to AI use. These key frameworks include:

- UK GDPR and *Data Protection Act 2018* (enforced by ICO);
- automated decision-making rules (*Data (Use and Access) Act 2025*);
- sector-specific regulation (FCA, MHRA, Ofcom);
- *Equality Act 2010*, consumer and health and safety law; and
- *EU AI Act* (if serving EU markets).

GET VISIBILITY AND CONTROL

You cannot manage what you cannot see. Put in place:

- a central AI register listing every tool, its purpose and risk rating;
- a data classification framework setting out what staff can input;
- restrictions on public AI tools for confidential or privileged data;
- a Data Protection Impact Assessment before any high-risk AI use; and
- an approval process before any new AI tool is rolled out.

TRAIN YOUR TEAM AND KEEP HUMANS IN THE LOOP

AI supports professional judgement; it does not replace it. You should:

- train staff on data protection, confidentiality and verify outputs;
- require human review of high-impact AI outputs;
- give individuals information, a right to challenge and a right to human review under *Article 22C UK GDPR*;
- audit AI for bias, particularly in recruitment and HR; and
- document the reasoning behind AI-informed decisions.

REVIEW YOUR AI CONTRACTS

Standard software terms rarely cover AI risk.

Under the UK GDPR, your contracts should address:

- ownership of input and output data;
- whether the vendor can use your data to train its models;
- whether the vendor has a compliant data processing agreement covering sub-processors;
- how the vendor protects personal data transferred overseas, including via the UK SCCs addendum; and
- who is responsible if AI tools produce incorrect, biased or unlawful content.

MONITOR REGULATORY CHANGE

Be ready to respond. Be ready to adapt. You should:

- maintain a data breach response plan and report qualifying breaches to the ICO within 72 hours;
- track ICO guidance on AI and automated decision-making;
- follow sector regulator guidance relevant to your business;
- monitor EU AI Act implementation if you are in scope; and
- review your AI governance framework at least annually.

CONTACT US

visit our website | **legalvision.co.uk**
email us | **info@legalvision.co.uk**
call us | **0808 196 8584**

LEGALVISION®