UK PRIVACY POLICY CHECKLIST: WHAT YOUR BUSINESS NEEDS TO KNOW

The most common privacy compliance gaps aren't hard to fix. They are just easy to overlook until a Subject Access Request or ICO complaint makes them impossible to ignore. This checklist covers what your business is required to have in place under UK GDPR and the Data Use and Access Act 2025.

LAWFUL BASIS AND DATA CATEGORIES

Your privacy policy must state the lawful basis for every type of personal data you collect: consent, contract, legitimate interest, legal obligation, vital interests, and/or public task. It must also identify what categories of data you collect (for example, identity data), why, and where it comes from if not directly from the individual.

"We comply with UK GDPR" is not sufficient, you need a lawful basis. Neither is stating "to improve our services" - as you need to be able to rely on a lawful basis, likely being "legitimate interest".

DATA SUBJECT RIGHTS

Individuals have 8 rights under UK GDPR. Your policy must name each one, explain it in plain English, and tell people how to exercise it, including a working contact email or form.

It must also state:

- the one calendar month response timeframe
- the right to complain to the ICO, with their contact details

NEW COMPLAINTS HANDLING

You must describe how privacy complaints are received, acknowledged, investigated and escalated by your organisation. This is the first thing the ICO will likely check.

A contact email with no described process does not meet the requirement. The way you handle complaints could be listed within your privacy policy, and in your privacy policy you need to make clear that a data subject has a right to make a complaint.

AUTOMATED DECISION-MAKING

If your business uses automated processes to make or influence decisions about individuals, including AI tools, scoring models or algorithmic pricing, your privacy policy must say so and explain the logic and consequences. Most businesses underestimate how broadly this applies.

Under the DUAA 2025 there are more avenues to use legitimate interests as a lawful basis for automated decision making, but you still need to ensure you have appropriate safeguards in place.

LEGALVISION®

UK PRIVACY POLICY CHECKLIST: WHAT YOUR BUSINESS NEEDS TO KNOW

RETENTION AND SECURITY

Your privacy policy must state how long you keep each category of personal data and why. Being vague and stating "as long as necessary" does not satisfy this.

It should also confirm the measures in place to protect data and how breaches are handled.

ACCOUNTABILITY

Your policy must name your organisation as the data controller with your company name and contact details.
If you have a Data Protection Officer their details should be included

DATA SHARING AND INTERNATIONAL TRANSFERS

Your policy must identify who you share personal data with and on what basis. If data is transferred outside the UK or EEA, the transfer mechanism you may use must be stated:

For example, countries that have an adequacy decision (i.e., similar protections to the UK GDPR) or use of the standard contractual clauses and the UK addendum.

Cookies and tracking must be covered in the policy policy or a linked cookie notice.

DUAA 2025: WHAT HAS CHANGED

The *Data Use and Access Act 2025* came into force in February 2025. If your privacy policy predates that, it may be non-compliant.

The three gaps most commonly missing:

1. the right to complain
2. automated decision-making disclosure
3. using a wrong lawful basis

PRIVACY POLICIES

- No complaints process or one with no described procedure
- No automated decision-making disclosure
- Generic retention periods with no rationale

A Subject Access Request or ICO complaint could surface quickly.

CONTACT US
visit our website | legalvision.co.uk
email us | info@legalvision.co.uk
call us | 0808 258 4780

LEGALVISION®