GDPR & data protection compliance checklist

A practical guide for scaling businesses to identify key data protection risks and readiness

Whether you're preparing for investment, M&A, or simply scaling your business, data protection compliance is essential. This checklist outlines common issues we help clients address – from governance and contracts to documentation and regulatory risk.

1. Data governance & responsibility

- Appointed a data protection officer (DPO) or designated a responsible lead?
- Mapped what personal data you collect, how it's stored, used, and shared?
- Completed a data protection impact assessment (DPIA) for high-risk processing?

2. Privacy documentation & policies

- Up-to-date privacy policy and cookie policy accessible to users and employees?
- Internal data handling policies (IT security, retention, breach management) documented and implemented?
- Employee contracts updated to reflect data processing/monitoring?

3. Legal bases & individual rights

- Clear legal basis for all personal data processing (e.g. consent, contract)?
- Internal processes to respond to data subject access requests (DSARs) within statutory timelines?
- Ability to honour individual rights (e.g. erasure, rectification, portability)?

4. Third party processors & international transfers

- Third party agreements include UK GDPR-compliant data processing clauses?
- International transfers assessed and covered by safeguards (e.g. standard contractual clauses)?
- Supplier onboarding includes privacy and security due diligence?

5. Security, breaches & incident management

- Appropriate security measures (e.g. encryption, access control, testing) in place?
- Documented breach response plan, including ICO – Information Commissioner's Office, and individual notifications?
- Staff training provided on incident identification and response?

6. Ongoing monitoring & regulatory readiness

- Policies reviewed annually or after major business changes?
- Maintained a Record of processing activities (ROPA)?
- Ready for ICO audits or investor due diligence?

Final thoughts

GDPR compliance isn't just a tick-box exercise – it's about building trust with your customers, employees, and partners. As your business grows, so do the risks (and opportunities) tied to how you manage data. Getting the foundations right now saves cost, reputation, and hassle later – especially when investors, customers or regulators start asking the hard questions.

Let's talk

Ashfords advises high-growth companies, investors and acquirers on data protection strategy, compliance and risk mitigation. Our cross-disciplinary team ensures data compliance supports – not slows – your commercial objectives.

Ashfords – Venture & Growth Capital Team

Pragmatic legal advice for ambitious founders

Sam Brown
s.brown@ashfords.co.uk
T +44 (0)20 7544 2402

Chris Dyson
c.dyson@ashfords.co.uk
T +44 (0)117 321 8054

Rory Suggett
r.suggett@ashfords.co.uk
T +44 (0)117 321 8067

Sign up to our newsletter **Venture** to receive more insights for growing businesses

Find further useful resources on the **Ashfords' Business Scaleup Hub**

Follow us on **LinkedIn**

ashfords