

GDPR Compliance Basics

A practical starting checklist for sole traders and SMEs handling personal data, whether that's customer records, supplier details, or staff information.

1. Know what data you hold

☐	List the personal data you collect (customers, suppliers, staff, prospects)
☐	Identify where it's stored (CRM, spreadsheets, email, paper files)
☐	Identify who has access to it, and why

2. Have a lawful basis

☐	Identify the lawful basis for each type of data you process (e.g. consent, contract, legitimate interest)
☐	Record that basis somewhere, rather than relying on memory

3. Privacy notice

☐	A privacy notice is published on your website and is easy to find
☐	It explains what you collect, why, how long you keep it, and who it's shared with

4. Data subject rights

☐	You have a process for responding to access requests, correction requests, and deletion requests
☐	You know your response deadline (one calendar month, as a general rule)

5. Security measures

☐	Devices and accounts holding personal data are password-protected
☐	Data is backed up, and backups are also protected
☐	Old paper records are disposed of securely (e.g. shredded)

6. Data breach procedure

☐	You have a simple written procedure for what to do if data is lost, stolen, or wrongly shared
☐	You know that notifiable breaches must be reported within 72 hours

7. Third parties and processors

☐	Contracts are in place with any supplier that processes data on your behalf (payroll, cloud storage, marketing tools)
☐	You've checked whether those suppliers store data outside the UK/EEA, and what that means for you

8. Retention and housekeeping

☐	You have a retention policy setting out how long different types of data are kept
☐	Old or unnecessary personal data is deleted on a regular schedule

9. Staff awareness



Anyone handling personal data understands the basics, even if that's just you and one other person

A note on scope

This checklist covers the core building blocks most sole traders and SMEs need; it is not a substitute for legal advice, particularly if you handle special category data (health, financial, or similarly sensitive information) or operate at larger scale.

Smallbizbod helps small businesses put practical data protection policies and processes in place, without the jargon. Book a free, no-obligation chat at www.smallbizbod.com.