LAN SUPPORT

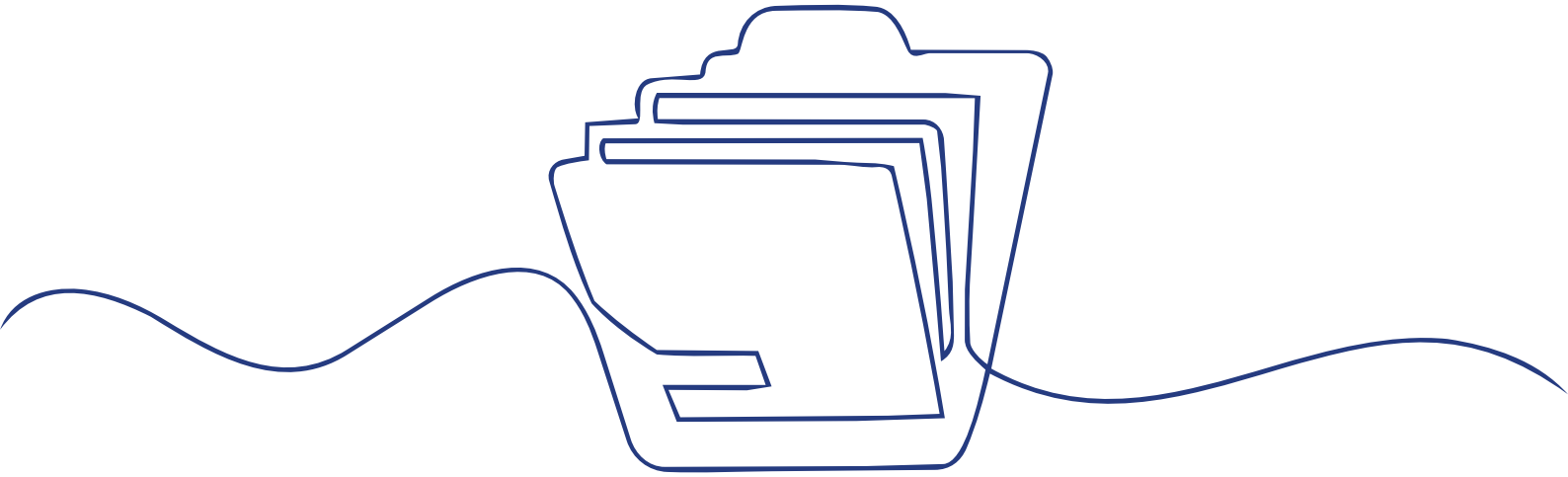
IT Service Excellence 30 Years 1996 -2026

GDPR Compliance Checklist for SMBs

A practical guide to UK data protection requirements for small and medium-sized businesses

GDPR Compliance Checklist for SMBs Introduction

GDPR can feel complex, but for most SMBs it's built on a simple idea: personal data should always be handled responsibly, kept secure, and managed transparently.



In other words, treat people's information with care, make sure it's properly protected, and be clear about how and why you're using it. Get those fundamentals right, and you're already well on the way to meeting your obligations.

This checklist breaks it down into 10 clear, actionable steps so you can quickly assess your compliance posture and identify gaps.

Step 1: Understand What Personal Data you Actually Hold

Before you can comply with GDPR, you need full visibility of your data.

Start by building a simple data inventory:

• What personal data do you collect?
(names, emails, addresses, payroll data, etc.)
• Where is it stored?
(Microsoft 365, CRM systems, spreadsheets, backups, paper files)
• Who has access to it internally?
• Who do you share it with externally?
• Why do you collect it in the first place?

Tip: Many SMBs discover they are storing far more data than they realised, often in unmanaged spreadsheets or old shared drives.

Step 2: Establish a Lawful Basis for Processing

GDPR requires you to have a valid reason for handling personal data.

Each activity involving personal data must fall under one of the lawful bases:

• **Contractual necessity:** required to deliver services or employment contracts
• **Legal obligation:** required for tax, payroll, or regulatory purposes
• **Legitimate interests:** e.g. business communications or service improvement
• **Consent:** only where individuals actively agree
(must be clear and recorded)

Important: Consent is often overused. In many SMB scenarios, legitimate interest or contract is more appropriate.

Step 3: Ensure your Privacy Notice is Accurate and Transparent

Your privacy notice is your public statement of how you handle data.

It should clearly explain:

- What personal data you collect
- Why you collect it
- How long you keep it
- Who you share it with (including third parties and cloud providers)
- How individuals can exercise their rights
- How they can contact you about their data

Keep it written in plain English—avoid legal jargon wherever possible.

Step 4: Implement strong access controls

One of the most common GDPR issues is overexposure of data within the business.

To reduce risk:

- Apply the principle of least privilege
(only give access to what's needed)
- Regularly review user permissions
- Immediately revoke access when staff leave or change roles
- Use Multi-Factor Authentication (MFA) across key systems
- Separate administrative access from day-to-day user accounts

A surprising number of breaches occur simply because old accounts are never removed.

Step 5: Protect Personal Data with Appropriate Security Measures

GDPR doesn't prescribe exact tools, but it does require "appropriate technical and organisational measures".

For SMBs, this typically includes:

- Endpoint protection (anti-virus / EDR solutions)
- Full disk encryption on laptops and mobile devices
- Secure configuration of Microsoft 365 or Google Workspace
- Regular patching and updates
- Secure backups with tested restoration processes
- Email security (anti-phishing and anti-spam controls)

Security should be layered, not reliant on a single tool.

Step 6: Put a Data Breach Response Plan in Place

If something goes wrong, GDPR requires swift action.

Your plan should include:

- What qualifies as a personal data breach
- Who is responsible for incident response
- How incidents are reported internally
- How you assess risk to individuals
- When to notify the ICO (within 72 hours if required)
- When to inform affected individuals

Practising a "mock breach" once a year can significantly improve response time and confidence.

Step 7: Manage Third-Party and Supplier Risk

You remain responsible for data even when it is processed by third parties.

Check that:

- You have Data Processing Agreements (DPAs) in place
- Suppliers have appropriate security certifications or controls
- You understand where data is physically stored (UK/EU/US, etc.)
- Access is limited to what is necessary
- Suppliers are reviewed periodically, not just at onboarding

Cloud services like Microsoft 365, backup providers, and CRM platforms all fall into this category.

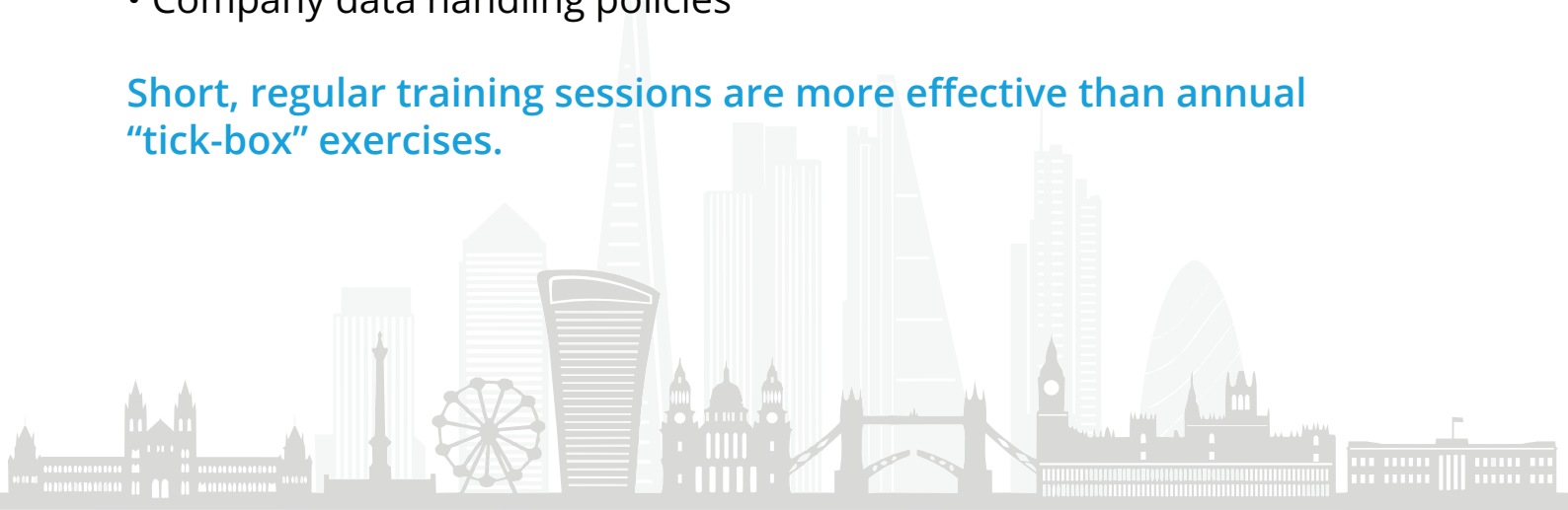
Step 8: Train Staff to Reduce the Risk of Human Error

Most GDPR incidents are caused by human behaviour rather than technical failure.

Training should cover:

- How to identify phishing emails
- Safe handling of customer data
- Password and authentication best practices
- Reporting suspicious activity or mistakes
- Company data handling policies

Short, regular training sessions are more effective than annual "tick-box" exercises.



Step 9: Apply Clear Data Retention Rules

GDPR requires you not to store personal data longer than necessary.

To stay compliant:

- Define retention periods for each data type
- Automate deletion where possible
- Review stored data regularly (especially legacy systems)
- Ensure backups are also governed by retention rules
- Document your retention policy clearly

If you don't need it, you shouldn't keep it. Simple as that.

Step 10: Maintain Accountability and Documentation

GDPR is as much about evidence as it is about practice.

You should be able to demonstrate compliance through:

- A Record of Processing Activities (ROPA)
- Documented policies and procedures
- Staff training records
- Risk assessments where appropriate
- Evidence of security controls in place

If you were audited, you should be able to show, not just explain, your processes.

Common SMB GDPR mistakes

Many small and medium-sized businesses fall into predictable traps:

- Over-relying on consent when another lawful basis applies
- Keeping customer data “just in case”
- Not reviewing old user accounts or permissions
- Weak password practices and no MFA
- No formal breach response plan
- Outdated or generic privacy policies

GDPR compliance doesn’t have to be complex or resource-heavy. For most SMBs, it’s about getting the fundamentals right and maintaining consistency.

If you can clearly explain your data, control access, secure systems properly, and respond effectively to incidents, you are already most of the way there.

How LAN Support Can Help

For many SMBs, GDPR compliance is closely tied to everyday IT decisions, from Microsoft 365 configuration and endpoint security through to backup strategy and staff awareness.

At LAN Support, we help organisations build practical, right-sized security and compliance foundations that reduce risk without adding unnecessary complexity.

For businesses that need additional support, we also provide dedicated GDPR and compliance services, including our GDPR Helpdesk, FOI Helpdesk, and outsourced Data Protection Officer (DPO) and compliance support. These services are designed to give you access to expert guidance when you need it, helping you stay compliant, respond confidently to data-related requests, and reduce the burden on internal teams.