dponesto

A FREE CHECKLIST FROM DPONESTO

GDPR Compliance Checklist

A practical, working checklist for UK GDPR compliance — not a legal treatise.

This checklist covers the areas the ICO and most auditors focus on first. Work through each section and be honest about gaps — this is a diagnostic tool, not a tick-box exercise.

Lawful Basis & Transparency

- ☐ We have identified and documented a lawful basis for every processing activity
- ☐ Our privacy notice is up to date, easy to find, and written in plain English
- ☐ We only collect data that is necessary for the stated purpose (data minimisation)
- ☐ Marketing consent is captured clearly and separately from other consents

Records of Processing (ROPA)

- ☐ We maintain a Record of Processing Activities covering all major systems
- ☐ The ROPA is reviewed and updated at least annually
- ☐ Special category data (health, etc.) is identified and given extra protection

Individual Rights & DSARs

- ☐ We have a documented process for handling Data Subject Access Requests
- ☐ We can respond within the statutory one-month timeframe
- ☐ Staff know how to recognise and escalate a rights request (it doesn't have to say 'DSAR')
- ☐ We have a process for handling erasure, rectification, and objection requests

Retention & Deletion

- ☐ We have a retention schedule covering our main data categories
- ☐ Data is actually deleted or anonymised when retention periods expire
- ☐ Backups and archived systems are included in retention planning

Breach Preparedness

- ☐ We have a documented data breach response process
- ☐ Staff know how to report a suspected breach internally
- ☐ We understand the 72-hour ICO notification requirement and when it applies

dponesto

Third Parties & Contracts

- ☐ All data processors have a signed Data Processing Agreement (DPA)
- ☐ We carry out due diligence before appointing new processors
- ☐ International data transfers use an approved transfer mechanism

Governance & Accountability

- ☐ A named individual (DPO or equivalent) is accountable for data protection
- ☐ Staff receive data protection training on induction and periodically thereafter
- ☐ We consider data protection at the design stage of new projects (privacy by design)

> *If you've ticked fewer than half of these, that's a normal starting point for most SMEs — but it does mean your regulatory exposure is currently higher than it needs to be. Dponesto can help you close these gaps proportionately, starting with the highest-risk items first.*

Why not book a free 30-minute consultation with dponesto? We would love to talk with you about making sure your data is as robust as you need it to be. Make a booking here