# GDPR Compliance Checklist

UK GDPR data handling requirements covering lawful basis, data subject rights, breach procedures, and documentation obligations. Verify your compliance posture with this comprehensive checklist.

| 7 | 72hr | £17.5m | Free |
|---|---|---|---|
| GDPR PRINCIPLES | BREACH NOTIFICATION DEADLINE | MAXIMUM ICO FINE | COMPLIANCE CHECKLIST |

**How to Use This Checklist**

Work through each section with your Data Protection Officer or compliance lead. Tick items that are fully in place with documented evidence. UK GDPR compliance is an ongoing obligation, not a one-time project. Review this checklist annually.

## 1 Lawful Basis & Processing

- [ ] A **lawful basis** is identified and documented for every processing activity (consent, contract, legitimate interest, legal obligation, vital interest, public task)
- [ ] Where **consent** is the lawful basis, it is freely given, specific, informed, and unambiguous with clear opt-in
- [ ] **Consent records** are maintained showing when and how consent was obtained
- [ ] Consent can be **withdrawn** as easily as it was given, and processing stops promptly
- [ ] A **Legitimate Interest Assessment (LIA)** is documented where legitimate interest is relied upon
- [ ] Processing of **special category data** (health, religion, ethnicity, biometrics) has an additional lawful basis under Article 9
- [ ] **Children's data** processing has appropriate safeguards (consent from parent if under 13)

**Section Score:** ____ /10

## 2 Data Subject Rights

- [ ] Processes exist to respond to **Subject Access Requests (SARs)** within 30 days
- [ ] The **right to rectification** is supported — data subjects can correct inaccurate data
- [ ] The **right to erasure** (right to be forgotten) is supported where no overriding legal basis exists
- [ ] The **right to data portability** is supported — data can be exported in machine-readable format
- [ ] The **right to object** to processing (including direct marketing) is respected immediately
- [ ] The **right to restrict processing** can be applied while disputes are resolved
- [ ] Automated **decision-making and profiling** is identified, and data subjects can request human review

**Section Score:** _____ /10

## 3 Privacy Notices & Transparency

- [ ] A **privacy notice** is published on the website covering all required information (Articles 13 & 14)
- [ ] Privacy notice includes: identity of controller, DPO contact, purposes, lawful basis, retention, rights, complaint procedure
- [ ] An **employee privacy notice** is provided to all staff covering workplace data processing
- [ ] **Cookie consent** is implemented correctly (PECR) — no non-essential cookies before consent
- [ ] Privacy notices are written in **clear, plain language** accessible to the target audience
- [ ] Privacy notices are **reviewed annually** and updated when processing activities change

**Section Score:** ____ /10

## 4 Data Security & Breach Management

- [ ] **Technical measures** protect personal data: encryption at rest, encryption in transit, access controls, MFA
- [ ] **Organisational measures** are in place: policies, training, role-based access, clean desk policy
- [ ] A **data breach response plan** exists with clear roles, procedures, and communication templates
- [ ] **Breach notification to ICO** within 72 hours of awareness (for breaches posing risk to individuals)
- [ ] **Breach notification to data subjects** without undue delay for high-risk breaches
- [ ] A **breach register** records all personal data breaches (including those not notified to ICO)
- [ ] Regular **security testing** (penetration testing, vulnerability scanning) is conducted

**Section Score:** ____ /10

## 5 Documentation & Accountability

- [ ] A **Record of Processing Activities (ROPA)** is maintained per Article 30
- [ ] **Data Protection Impact Assessments (DPIAs)** are conducted for high-risk processing
- [ ] A **Data Protection Officer** is appointed (if required) or a responsible person is designated
- [ ] **Data processing agreements** are in place with all third-party processors (Article 28)
- [ ] **International data transfers** have appropriate safeguards (adequacy decision, SCCs, or BCRs)
- [ ] **Staff training** on GDPR obligations is provided at induction and refreshed annually
- [ ] GDPR compliance is **audited** internally or externally at least annually

**Section Score:** ____ /10

| # | AREA | SCORE | PRIORITY |
|---|---|---|---|
| 1 | Lawful Basis & Processing | / 10 | H / M / L |
| 2 | Data Subject Rights | / 10 | H / M / L |
| 3 | Privacy & Transparency | / 10 | H / M / L |
| 4 | Data Security & Breach | / 10 | H / M / L |
| 5 | Documentation & Accountability | / 10 | H / M / L |
| **TOTAL SCORE** | | **/ 50** | |

**Score Interpretation**

**80–100:** Excellent — well-managed with only minor improvements needed.
**60–79:** Good foundation but gaps exist. Prioritise areas scoring below 6.
**Below 60:** Significant gaps putting your business at risk. Seek specialist review.

## ! Action Items & Notes

**Top 3 Priority Actions:**

1. 
2. 
3. 

**Notes**

**Need GDPR Compliance Support?**

We help UK organisations achieve and maintain GDPR compliance with practical, business-focused data protection solutions.

info@cloudswitched.com

New London House, 6 London St, London EC3R



Completed by: _____ Date: _____ Next review: _____

© 2026 CloudSwitched Limited. All rights reserved. This resource is provided for informational purposes and does not constitute professional IT advice.