# GDPR Compliance Checklist

For UK Wellbeing Professionals

*Use this checklist to ensure you're handling client data legally and safely. Not legal advice - consult a professional if unsure.*

## 1. ICO Registration

* Determine if you need to register with the ICO (if you process client data, you probably do)
* Register with the ICO at ico.org.uk (£40-60 annual fee)
* Keep your ICO registration up to date and display registration number on your privacy policy

## 2. Privacy Policy

* Create a privacy policy explaining how you collect, use, and store data
* Include: what data you collect, why, how long you keep it, who you share it with, client rights
* Display privacy policy prominently on your website
* Review and update privacy policy annually or when practices change

## 3. Lawful Basis for Processing

* Identify your lawful basis (usually: consent, contract, legitimate interests)
* Get clear consent for processing personal data
* Keep records of consent (when obtained, what was agreed to)

## 4. Data Security

* Use strong passwords on all accounts
* Enable two-factor authentication where possible
* Encrypt sensitive data (especially on portable devices)
* Lock devices when not in use
* Use secure cloud storage (not personal Dropbox - use encrypted professional storage)
* Secure physical records (locked filing cabinet)
* Have a plan for what to do if there's a data breach

## 5. Client Rights

* Have a process for clients to request their data (Subject Access Request)
* Know how to respond if a client asks you to delete their data
* Be able to correct data if a client says it's wrong
* Understand when you can/can't delete data (e.g., legal requirements to keep records)

## 6. Data Retention

* Decide how long to keep client records (check your professional body requirements)
* Document your retention policy
* Securely delete data once retention period ends
* Set calendar reminders for when data should be deleted

## 7. Third Parties

* List all third-party services that process client data (booking systems, email platforms, etc.)
* Check these services are GDPR compliant
* Have data processing agreements with any contractors/VAs who access client data
* Mention third-party data sharing in your privacy policy

## 8. Website Compliance

* Have a cookie policy if your website uses cookies
* Get consent before setting non-essential cookies
* Make sure contact forms have a checkbox for consent to store data
* Use SSL certificate (https://) on your website

## 9. Marketing Communications

* Only send marketing emails to people who've opted in
* Include unsubscribe link in all marketing emails
* Include your business name and address in emails
* Process unsubscribe requests within 30 days

## 10. Regular Reviews

* Review data protection practices annually
* Keep up with GDPR changes and updates
* Document what you do to stay compliant
* Consider GDPR training or consulting if handling sensitive data

**Resources:**

• ICO website: www.ico.org.uk

• ICO helpline: 0303 123 1113

• Free ICO guidance for small businesses: ico.org.uk/for-organisations