GDPR Readiness & Compliance Checklist

A practical checklist for assessing GDPR readiness across lawful basis, data subject rights, and breach management

GDPR · Data Protection · Privacy · DPIA · Data Subject Rights · Breach Management

GDPR compliance depends on demonstrable process, not a policy on file. This checklist sets out a practical sequence for assessing data protection readiness across the areas a regulator or data subject is most likely to test.

A Lawful Basis & Consent

- [ ] Identify and document a lawful basis for every processing activity
- [ ] Maintain consent records where consent is the lawful basis, including how and when it was given
- [ ] Provide a straightforward way for data subjects to withdraw consent
- [ ] Review lawful basis whenever a new processing purpose is introduced
- [ ] Confirm privacy notices describe processing purposes in plain language

B Records of Processing Activities

- [ ] Maintain a record of processing activities covering purpose, categories of data, and recipients
- [ ] Document data retention periods per processing activity
- [ ] Identify cross-border data transfers and the safeguards applied to each
- [ ] Keep processing records current as systems and vendors change
- [ ] Make records available on request to demonstrate accountability

C Data Subject Rights

- [ ] Provide a documented process for handling access, rectification, and erasure requests
- [ ] Verify the identity of the requester before actioning a data subject request
- [ ] Track request status and response timelines from receipt to closure
- [ ] Handle objections to processing and requests to restrict processing
- [ ] Support data portability requests in a structured, exportable format

D Data Protection Impact Assessments (DPIA)

- [ ] Screen new projects and systems to determine whether a DPIA is required
- [ ] Complete DPIAs for processing likely to result in high risk to data subjects
- [ ] Document identified risks and the mitigations applied before go-live
- [ ] Consult the Data Protection Officer, where appointed, on DPIA outcomes
- [ ] Review and update DPIAs when processing scope or risk changes

E Breach Management

- [ ] Maintain a documented incident response process for personal data breaches
- [ ] Assess and record the likely risk to data subjects for every breach identified
- [ ] Notify the supervisory authority without undue delay where notification thresholds are met
- [ ] Notify affected data subjects directly where the breach poses a high risk to their rights
- [ ] Maintain a breach register recording facts, effects, and remedial action taken

F Third-Party & Processor Contracts

- [ ] Maintain a register of processors and sub-processors handling personal data
- [ ] Confirm data processing agreements are in place with all processors
- [ ] Define processor obligations for security, breach notification, and sub-processing
- [ ] Review processor security practices before onboarding and periodically thereafter
- [ ] Confirm international transfer safeguards are documented for offshore processors

G Governance & Accountability

- [ ] Appoint a Data Protection Officer or accountable owner where required
- [ ] Embed data protection by design and default into new systems and projects
- [ ] Maintain data protection policies aligned to current practice
- [ ] Review data protection roles, responsibilities, and reporting lines periodically
- [ ] Report data protection status and open risks to management

H Training & Awareness

- [ ] Deliver data protection training to staff who handle personal data
- [ ] Refresh training when processes, systems, or regulatory guidance change
- [ ] Track completion of training and maintain evidence for audit purposes
- [ ] Raise awareness of how to recognise and report a suspected data breach