fox williams

Data Protection

Risk and exposure audit
2025

Introduction

Law firms handle significant volumes of personal and sensitive data, making data protection compliance not only a regulatory requirement but a fundamental part of maintaining trust with clients, staff and third parties. The reputational and financial risks of non-compliance with UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations (PECR) are material, particularly in an environment where data breaches and cyber threats are ever-present.

Our data protection team combines deep sector knowledge with practical experience advising professional services firms. We work with law firms to review internal systems, processes and documentation to ensure that privacy compliance is not only demonstrable but proportionate to the risk profile of the firm.

This audit is designed to help you assess your firm's current position against key legal requirements, including data governance, third-party processor arrangements, international transfers and marketing compliance. It will help identify gaps, ensure appropriate accountability, and support decision-making across your firm's leadership and operational teams.

Compliance

- [ ] Who is responsible internally for data protection compliance?
- [ ] Review internal data protection compliance policy.
- [ ] Review staff training for data protection compliance.
- [ ] Check the status of ICO registration.

Data mapping

- [ ] Review data inventory/data map to show what data you have, what you use it for, where it is held and what third parties are involved in processing.
- [ ] Review record of processing activities (ROPA) as required by article 30.
- [ ] Are you processing any special categories of personal data?
- [ ] Are you processing any criminal conviction data?

Legal basis for processing

- [ ] Review the grounds for processing and – in respect of each category of data - on which ground(s) you rely.
- [ ] Assess suitability and validity of consent where applicable.
- [ ] Review any documented legitimate interest assessments.
- [ ] Identify the legal basis for processing any special categories of personal data.
- [ ] Identify the legal basis for processing any criminal convictions data.

Privacy notices

- [ ] Review privacy notices to make sure they include the transparency information required by the GDPR, including:
  - [ ] website privacy policy,
  - [ ] client data protection statement,
  - [ ] staff privacy notice, and
  - [ ] recruitment candidate notice.
- [ ] Check privacy notices are written in plain intelligible language.

Third party data processors

- [ ] Identify all data processors.
- [ ] Review what due diligence is undertaken on processors to check that they provide sufficient data security guarantees.
- [ ] Review data processor agreements for compliance with Article 28.
- [ ] Review data processor agreements as regards international transfers.
- [ ] Review liability / indemnity provisions in processor agreements.

Data protection impact assessment (DPIA)

- [ ] Consider whether any processing requires a DPIA.
- [ ] Check any DPIAs that have been conducted.
- [ ] Consider compliance with data protection by design and default (DPbDD) e.g. in relation to implementation of new technologies.

Data protection officer (DPO)

- [ ] Consider whether you are required to appoint a DPO or if you do so voluntarily.
- [ ] Review DPO job specification where applicable.

Data subject rights

- [ ] Review internal policy for handling data subject requests.

Marketing

- [ ] Review cookies in use and website cookie policy for compliance with PECRs.
- [ ] Check if clear gifs or similar are used for email marketing tracking.
- [ ] Check email marketing template for compliance with PECRs.
- [ ] Review internal policy for obtaining marketing consents where needed and handling opt-outs.

International data transfers

- [ ] Identify all international data transfers.
- [ ] Review the legal basis of any international transfers – eg IDTA or SCCs.

Data security

- [ ] Review internal data security policies.
- [ ] Review personal data breach / incident response plan.
- [ ] Check for personal data breach register.
- [ ] Review staff training of cyber-risk awareness.
- [ ] Review data breach / cyber insurance.

EU GDPR

- [ ] Assess if EU GDPR applies.
- [ ] Consider if you need to appoint a European Representative.
- [ ] If you operate in more than one EU member state, consider which national data protection authority will be “lead authority”.