GDPR CHECKLIST

This checklist is intended to support members in identifying and implementing the key considerations required for compliance with the General Data Protection Regulation (“GDPR”). This checklist is not, and should not be taken to be, a comprehensive list of all matters which require to be addressed for GDPR compliance, and should be read in conjunction our GDPR Guide and all guidance issued by the ICO and the Article 29 Working Party.

Resource

Have you…

- Designated a person or group to lead the effort for GDPR compliance within the firm?
- Built support for your compliance programme within your firm?
- Enlisted the help of other business functions within your firm, such as HR, legal or IT?

Data mapping

Have you…

- Identified what personal data your firm holds, uses, shares and otherwise processes?
- Conducted a comprehensive data mapping exercise?
- Assessed each processing activity in light of GDPR’s data protection principles?
- Created an action plan to deal with processing activities which do not align with these principles?

Processing justifications

Have you…

- Determined and documented the legal basis for processing data for each processing activity?
- Ensured that each processing activity meets at least one of GDPR’s legal processing grounds?
- Reviewed the process for requesting and obtaining data subject consent (if you rely on consent)?
- Ensured that each processing activity involving special category personal data categories falls within one of the permitted processing exceptions?

Contract reviews

Have you…

- Reviewed and updated any contracts under which you contract to receive personal data processing services?
- Reviewed and updated any contracts under which you provide services which involve personal data processing by your firm on behalf of clients?
☐ Reviewed and updated contracts for the procurement of technology solutions which host, or are used, to process personal data?
☐ Established a process for addressing any gaps identified in these contracts?
☐ Developed new contractual styles based around the requirements of GDPR?

**Governance and records**

Have you...

☐ Implemented GDPR-compliant corporate policies?
☐ Reviewed and updated your firm’s privacy statements, including the process for how and when these privacy statements are communicated to individuals?
☐ Reviewed and updated consent mechanisms and language?
☐ Established clear processes and procedures for engaging sub-contractors?
☐ Identified and reviewed all profiling activities and automated decisions?
☐ Reviewed your firm’s internal business processes for handling personal data to check they are privacy friendly?
☐ Established clear processes and procedures for dealing with cross-border data transfers outside the EEA?
☐ Established procedures for dealing with requests by individuals to exercise their rights as data subjects?

**Data Protection Impact Assessments (DPIA)**

☐ Assessed all products, services, internal processes and third party relationships for general privacy impacts and determined whether they require a full DPIA?
☐ Drafted an internal policy describing when the firm must conduct a DPIA and the process for requesting and completing a DPIA?

**Record keeping**

☐ Established a process to collect and maintain accurate records about each of the firm’s processing activities?
☐ Established an audit procedure to ensure that records are accurate, complete and up-to-date?

**Training**

☐ Raised awareness of GDPR throughout your firm?
☐ Educated your firm’s employees (including senior decision makers) about GDPR’s new requirements and what they mean for the firm?
☐ Established data protection training programmes for specific areas of your firm’s business?

**Data security and breaches**

☐ Reviewed the security measures you employ to protect personal data to ensure they are sufficient and appropriate?
☐ Established a clear process for reporting all potential security breaches?
- Developed processes that allow for 24/7 security incident analysis and investigation?
- Assessed the firm’s current personal data security levels and determined how to close identified gaps?