GDPR COMPLIANCE
Corporate Support

Aaron & Partners LLP
Solicitors
5-7 Grosvenor Court
Foregate Street
Chester CH1 1HG

Tel: 01244 405555
Fax: 01244 405566

Corporate & commercial - GDPR – recommendations/actions

Recommendation/Action	Responsibility	Resources required	Timescale
A. **Compliance**			
1. **Review Personal Data** Create a spreadsheet and list the personal data ("PD") the Company holds. Identify : • where it came from • the reasons why the client stores it • the legal basis for the Processing; • create a yes/no checklist as to whether the Company really needs to store it. What is the justification for retaining specific data?	Company		
2. **Clear out Personal Data** Delete PD that is no longer required for legal, regulatory or historical reasons. The less PD is held the easier compliance will be. • record what data was removed and why.	Company		
3**. Identify who is responsible for each element of GDPR.** Is the Company obliged to appoint a Data Protection Officer ("DPO")? If not, will the Company nominate a responsible person with knowledge of GDPR? Will the client be making a voluntary appointment of DPO? • ensure that Company staff know what they should be doing to prevent a data breach. • Training may be required.	Company		
4. **Review and update IT security data policies and procedures.** Policies and procedures must be accessible and clear.	Company		
5. **Review existing insurance cover in event of a data breach.**	Company		

• Has the Company's insurance been updated to reflect the new penalties?			
B. **Client Policies, procedures and documentation**			

6. **Review the Company's existing documentation and amend to ensure that data subjects are clearly notified of their rights under GDPR:**
• Website – review legal notices to ensure:
  ○ GDPR compliant
  ○ consistent
• Contracts with clients.
		Copies of the following in Word format:
		1. The Company's website privacy policy/legal notices
		2. Template documentation used with the Company's customers including any:
		i. standard letters of engagement/appointment
		ii. Terms & conditions of supply
		iii. bespoke contracts in respect of specific services	

7. **Review existing consents.** • Are these necessary? • Do the Company collect sensitive personal data? • Is consent freely given, specific, informed and unambiguous? • Has consent been given by way of a statement or clear affirmative action?		As above.	
8. **Create/keep records of Consent (where this is relied upon as the basis for Processing PD).**	Company		
9. **Review and update the Company's Privacy Notices.**		Copies of the Company's existing privacy notices.	
10. **Review Data Subject Access policy and procedures to ensure GDPR compliance:** • Create template Data Subject Access documentation.		Copy of existing policy - or draft a new policy (if required)	
11. **Prepare Data correction request policy and template responses.**		Draft new policy and templates.	
12. **Prepare Data breach reporting policy and procedures**:		Draft new policy and	

• Create a register/document any breach, its effects and remedial action taken; • Review template internal breach notification documentation; • Create template breach reporting documentation.		templates.	
C. **The Company's Contractual Arrangements with third party processors ("TTPs").**			
13. **Identity third party processors ("TPP") who process Personal Data on the Company's behalf.** • Undertake due diligence into systems, policies and procedures of TPPs. • What Personal Data do they process; • Do the Company have consent to transfer PD to the TPP.	Company		
14. **Review existing contractual arrangements with TPP.** • Are these compliant with GDPR; • Do the Company need to vary the contract to include the GDPR prescribed clauses; • Check record keeping procedures of TPPs.		Copies of all existing contracts with third party processors.	
D. **The Company – transfer of data within the Group (if relevant)**			
15. **Review and advice on existing arrangements for transfer of PD within the Group whether within the EEA or outside:** • Are these compliant with GDPR; • Do consents need to be renewed? • Do contractual arrangements need to be reviewed? • Binding corporate rules?		Copies of any existing data processing/transfer agreements for review.	