GDPR Checklist

Ask Yourself....	Your Answer /Action Plan	CONSIDERED / COMPLETED?
Does GDPR apply to me territorially? It does if you process personal data about **EU residents** (even if you are based outside of the EU). If you have EU residents on your email list, as customers, as employees, as contractors, or service providers, then it applies. If you are able to identify individuals from the EU through cookies or IP addresses then it applies to you.		
Do I process data that GDPR applies to? If you process data that is capable of identifying an individual (including cookies and IP addresses) wholly or partly through automated means or manually as part of a filing system, then GDPR applies. This includes storage and publication of photo and video.		
What data do I process and for what purpose? Prepare a data inventory of the types of data you process. This inventory must be a dynamic inventory that is consistently updated for record keeping purposes.		
Do I process sensitive data? Sensitive data is data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation		

What are my lawful grounds for each of the processing activities that I have identified? • the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes; • processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; • processing is necessary for compliance with a **legal** obligation to which the controller is subject; • processing is necessary in order to protect the **vital interests** of the data subject or of another natural person; • processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller; • processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. If one of your grounds is Legitimate Interests, you will need to complete an assessment of legitimate interest.		
Have you identified all transfers to third parties and what country the third party is in? There are strict rules on transfers to third parties outside of the European Economic Area (EEA). Check whether the country has an adequacy finding or if it is in the United States it is certified under the Privacy Shield. You will also need this information to add to your Privacy Notice.		
Do I have a GDPR compliant Privacy Notice? Chances are that even if you have a privacy policy, it is not GDPR compliant as GDPR prescribes numerous things that need to be included in the privacy notice.		

Have I added my GDPR compliant Privacy Notice to my website? If you don't already have a link on your website to your privacy policy, add one in so that it appears on every page of your website. If you do already have one, make sure that you replace the old privacy policy with the new privacy notice.		
Have I sent my GDPR compliant Privacy Notice to my subscribers? GDPR requires you to send your Privacy Notice to your EEA resident subscribers to confirm, amongst other things, how you collect and process their personal data, for what purposes you use their data, the legal grounds of processing such data, how you keep their data secure and their rights in relation to such data.		
Have I added my Opt In wording to my sign up box? If you have a sign up box on your website that collects email addresses etc in return for your newsletter or other free opt in, ensure that you have GDPR compliant opt in wording at the point of collection (ie underneath the sign up box) together with a link to your Privacy Notice. GDPR requires you to be able to prove opt-in, so make sure your systems record this information.		
Have I obtained GDPR compliant consent for electronic marketing communications? See the ICO checklist for compliant consent. If you do not have compliant consent, email your list for fresh consent – https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/		
Have I obtained GDPR compliant consent for processing sensitive data Processing sensitive data requires explicit consent – this could be by the data subject signing the form where data has been collected or a double verification process.		
Have I put in place a procedure for recording consents including explicit consent for sensitive data? GDPR requires this. Does your email marketing system track consents to opt ins? Do you keep a filing system of hard copy consent forms?		

Have I put in place a system for managing opt outs/ withdrawing of consent? GDPR requires you to keep records of opt outs. Does your email marketing system manage this for you?		
Have I put in place GDPR compliant Processor Agreements with the third parties to whom I transfer personal data? Under GDPR it is mandatory to have a written agreement with your third party processor (eg payroll, software providers etc). GDPR prescribes what must be included in that agreement.		
Have I put in place a system for data subject requests? As a general rule, you must respond within 30 days to data subject requests.		
Do I need to appoint a Data Protection Officer? Certain businesses will need to appoint a Data Protection Officer. GDPR prescribes who this might be and what their duties are.	IABC chapters/regions are highly unlikely to need this. EMENA Region and EU based chapters may be an excpetion.	
Do I need to carry out a Data Protection Impact Assessment? A DPIA is required when the processing is likely to result in a high risk to the rights and freedoms of natural persons.	IABC chapters/regions are highly unlikely to need to this.	
Have I put in place a system for data breach notification? A data breach occurs where there is a loss alteration, unauthorised disclosure of or access to personal data AND there is a risk to the rights and freedoms of individuals. If there is a data breach, you must notify the ICO within 72 hours of the breach.		

Is your insurance adequate? Contact your insurance broker to discuss any increased liability due to GDPR (eg increased fines or additional liability as a data processor) and ensure that your insurance coverage is sufficient.		
Do I have a Data Retention Policy in place? If not, you must create and enforce a data retention policy.		
Have I reviewed the security of my data? Where and how do we store data? Can it be easily hacked or stolen?		
If I have employees, have I worked out lawful grounds for processing and obtained signed copies of the employee Privacy Notice? Historically you may have relied on consent in an Employment Agreement to process employee data. Post GDPR you will need to work out separate lawful grounds of processing for each processing activity (eg payroll processing for contractual purposes, social security processing for requirements of law etc). Grounds other than consent should be relied on where possible as consent can be withdrawn at any time. Where consent is necessary, this should be in a separate document to the Employment Agreement. The Employee Privacy Notice template is in the GDPR pack. See the Employee Checklist in the GDPR Pack.		
If I have employees, have I arranged for data protection training for them? Employees will need to be aware of how to properly process data, record consents, how long to store data, when to report data breaches, how to respond to data subject requests. THIS APPLIES IF YOU USE AN ASSOCIATION MANAGEMENT COMPANY.		