GDPR Checklist for Data Controllers

The first steps towards GDPR compliance are understanding your obligations, what your current processes are, identifying any gaps and determine whether your organisation processes personal data as a “data controller” or “data processor”.
The GDPR applies to “controllers” and “processors,” the definitions are broadly the same as under the General Data Protection Act 1998, whereby the controller explains how and why personal data is being processed and the processor acts on the controller’s behalf.
Please note that if you are a processor the GDPR places specific legal obligations, for example, you are required to maintain the records of personal data and processing activities. However if you are a controller, the GDPR places further obligations on you to ensure the contracts comply with the GDPR.

Undertaking a data protection audit is essential to achieving compliance. This checklist is intended to provide a starting point, rather than providing an exhaustive audit.

Step 1 - Lawfulness, fairness and transparency

	Question	***Processor***
Information you hold	Your business has conducted an information audit to map data flows.	
	Your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.	
Lawful bases for processing personal data	Your business has identified your lawful bases for processing and documented them. *(You need to identify lawful bases before you can process personal data and special categories of data.* *Your lawful bases for processing have an effect on individual’s rights. For example, if you rely on someone’s consent to process their data, they will have a stronger right to have their data deleted. It is important that you let individuals know how you intend to process their personal data and what your lawful bases are for doing so, for example in your privacy notice(s).*	
Consent	Your business has reviewed how you ask for and record consent.	
	Your business has systems to record and manage ongoing consent.	
Consent to process children’s personal data for online services	If your business relies on consent to offer online services directly to children, you have systems in place to manage it.	
Registration	Your business is currently registered with the Information Commissioner's Office.	

Step 2 - Individuals' rights

	Question	*Processor*
Right to be informed including privacy notices	Your business has provided privacy notices to individuals.	
Communicate the processing of children's personal data	If your business offers online services directly to children, you communicate privacy information in a way that a child will understand.	
Right of access	Your business has a process to recognise and respond to individuals' requests to access their personal data.	
Right to rectification and data quality	Your business has processes to ensure that the personal data you hold remains accurate and up to date.	
Right to erasure including retention and disposal	Your business has a process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it.	
Right to restrict processing	Your business has procedures to respond to an individual's request to restrict the processing of their personal data.	
Right of data portability	Your business has processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.	
Right to object	Your business has procedures to handle an individual's objection to the processing of their personal data.	
Rights related to automated decision making including profiling	Your business has identified whether any of your processing operations constitute automated decision making and have procedures in place to deal with the requirements.	

Step 3 – Accountability and governance

Accountability	Your business has an appropriate data protection policy.	
	Your business monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.	
	Your business provides data protection awareness	

	training for all staff.	
Data processor contracts	Your business has a written contract with any data processors you use.	
Information risks	Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.	
Data Protection by Design	Your business has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.	
Data Protection Impact Assessments (DPIA)	Your business understands when you must conduct a DPIA and has processes in place to action this.	
	Your business has a DPIA framework which links to your existing risk management and project management processes.	
Data Protection Officers	Your business has nominated a data protection lead or Data Protection Officer (DPO).	
Management Responsibility	Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.	

Step 4 – Data security, international transfers and breaches

Security policy	Your business has an information security policy supported by appropriate security measures.	
International transfers	Your business ensures an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area.	
Breach notification	Your business has effective processes to identify, report, manage and resolve any personal data breaches.	