GDPR Checklist for Data Processors

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 - Documentation

	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.	

Step 2 - Accountability and governance

	Question	***Processor***
Accountability	Your business has an appropriate data protection policy.	
Data Protection Officer (DPO)	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.	
Information risks and data protection impact assessments	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 show you have considered and integrated data protection into your processing activities.	

Training and awareness	Your business provides data protection awareness training for all staff.	
The use of sub-processors	Your business has sought prior written authorisation from the data controller before engaging the services of a sub-processor.	
Operational base	If your business operates outside the EU, you have appointed a representative within the EU in writing.	
Breach notification	Your business has effective processes to identify, report, manage and resolve any personal data breaches.	
Right of access	Your business has a process to respond to a data controllers request for information (following an individuals' request 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 routinely and securely dispose of personal data that is no longer required in line with agreed timescales as stated within your contract with the data controller.	
Right to restrict processing	Your business has procedures to respond to a data controllers' request to supress the processing of specific personal data.	
Right of data portability	Your business can respond to a request from the data controller for the supply of the personal data you process in an electronic format.	

Step 3 – Data Security

Security policy	Your business has an information security policy supported by appropriate security measures.	