Checklist

Mandatory provisions for data processing contracts

✓	Requirements under the DPA	Requirements under the GDPR
	The processor is to act only on instructions from the controller.	Needs to be a binding contract (or legal act) with the processor which sets out the: • subject matter (eg. the services performed), nature and purpose of the processing (eg. to enable the processor to carry out the services); • duration of the processing; • type of personal data; • categories of data subjects; and • obligations and rights of controller.
	The processor is required to take technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	The processor may only process the personal data in accordance with the controller's documented instructions. There is an exception for processing required by EU or Member State laws.
		The process must ensure that employees or other people authorised to process the personal data are subject to appropriate obligations of confidentiality.
		The processor must keep the personal data secure (implementing appropriate technical and organisational measures).
		The processor must obtain the controller's consent before using a sub-processor and enter into equivalent data processing obligations with that sub-processor.
		The processor must assist the controller, by technical and organisational measures, with responding to requests from data subjects exercising their rights.
		The processor must assist the controller with complying with the controller's obligations to implement appropriate technical and organisational measures, notify personal data breaches and carrying out data protection impact assessments.
		The processor must delete or return all personal data at the end of the provision of processing services unless EU or Member State Law requires the processor to keep a copy.
		The processor must make available to the controller information to demonstrate compliance with the obligations and allow audits by the controller or its mandated auditor.
		The processor must inform the controller if, in its opinion, the controller's instruction breaches EU or Member State data protection law.

GDPR - getting data protection right

The EU General Data Protection Regulation (GDPR) and Data Protection Act 2018 are now in force. This has been described as “the biggest change to data protection law for a generation”. It’s not just us saying that – those are the words of the Information Commissioner, Elizabeth Denham.

There has been quite a lot of focus on the consequences of getting data protection compliance wrong, with headlines about fines of up to €20million, or 4% of global annual turnover if that is higher.

At Mills & Reeve we focus on the practical steps your organisation can take to get data protection compliance right

Get in touch

Richard Sykes
Partner
T +44(0)121 456 8436
richard.sykes@mills-reeve.com

Paul Knight
Partner
T +44(0)161 234 8702
paul.knight@mills-reeve.com

Peter Wainman
Partner
T +44(0)1223 222408
peter.wainman@mills-reeve.com

MILLS & REEVE
Achieve more. Together.

www.mills-reeve.com/GDPR