Checklist

Privacy notice - GDPR compliant

✓	Information to include in privacy notice	Notes
	Your identity and contact details and details of your representative (if any).	You may have nominated a representative for the purposes of the DPA/GDPR.
	Identity and contact details of your data protection officer.	Applicable if you are legally required to appoint a data protection officer.
	The purpose for the processing.	Avoid generalisations that are open to a variety of interpretations (e.g. "improving user experience", "marketing", "IT security", and "future research").
	The legal basis for the processing.	Under the GDPR, it is more difficult to obtain consent - another legal basis for the processing may be more appropriate.
	Any legitimate interests that you are relying on.	The recitals to the GDPR identify certain legitimate activities (e.g. processing for preventing fraud, information security and intra-group transfers). However, this must be weighed against individuals' rights and freedoms.
	The categories of personal data.*	
	Recipients or categories of recipients of the personal data.	For example, group companies or credit reference agencies.
	Details of transfers outside the EEA and any safeguards taken.	The data transfer mechanism used to legalise the transfer must be specified.
	The period for which data will be retained or the criteria used to determine this period.	
	Details of the data subject's rights.	This includes the right to be forgotten, restrict processing and to object to processing, the right to data portability and the right to object to direct marketing.
	The right to withdraw consent at any time (if consent is used as the basis for processing).	Include details of how the data subject can exercise the right.
	The right to lodge a complaint with a supervisory authority.	In the UK, this is the Information Commissioner's Office.
	The source of the personal data (and whether it was a publicly accessible source).*	
	Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.**	
	Details of any automated decision making (e.g. profiling), the auto-decision logic used, the significance and consequences.	

* not needed where data is obtained directly from data subject ** only needed where data is obtained directly from data subject

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