Mills & Reeve's Brexit risk register

As the date for the UK leaving the EU looms ever closer our legal experts have pulled together a must-read risk register for all organisations. Our register pulls out the vital issues that you need to be thinking about now in the run-up to 29 March 2019.

The risk	How to mitigate it
Uncertainty over the legal basis for transferring personal data across international borders resulting in: • Potential disruption to operations if data flows cease; and/or • The risk of claims, enforcement action or fines for you or your overseas suppliers/customers if personal data is transferred across borders in breach of data protection laws. The main potential risks relate to personal data transfers out of the EU27 to the UK in a "no deal" scenario.	• Undertake an audit of your data flows, both data you send and data you receive, to identify any cross border flows. • Establish which cross border data flows are critical to your operations. • Seek professional advice and engage with relevant suppliers and customers as appropriate. • Where possible, implement appropriate measures before exit day to mitigate risks. For example, entities in the EU27 may require you to agree "Standard Contractual Clauses" before they will transfer personal data to you in a "no-deal" scenario.
Where you are not established in the EU but offer goods or services to EU data subjects, or monitor their behaviour, the General Data Protection Regulation (GDPR) "extra-territorial provisions" apply. There is a risk of fines or enforcement action if you do not appoint an EU "representative" where required under GDPR. Similarly, where you are not established in the UK, but offer goods or services to UK data subjects, or monitor their behaviour, the "extra-territorial provisions" of the UK's post-Brexit version of GDPR ("UKGDPR") may apply. And there is a risk of fines or enforcement action if you do not appoint a UK "representative" where required under UKGDPR.	• Undertake a review of your activities to establish whether they fall within the GDPR or UKGDPR "extra-territorial provisions". • If you are unsure whether this triggers an obligation to appoint a "representative" in the EU or UK, seek professional advice. • If appropriate, designate a representative under a written mandate that meets GDPR/UKGDPR requirements. • If your activities fall within the GDPR's/UKGDPR "extra-territorial provisions" and you have appointed a Data Protection Officer or are obliged under GDPR to appoint a DPO, consider whether your DPO should be located within the EU or the UK.

The risk	How to mitigate it
Possible claims or regulatory action if your data protection documentation is not updated after exit.	• Review relevant documentation e.g. GDPR privacy notices and records of processing activity. • Implement appropriate updates to reflect any transfers to EU27 countries (the EU27 will become “third countries” on exit day, subject to the terms of any withdrawal agreement) and the appointment of any representative.
Data sharing contracts that continue after Brexit may contain inappropriate provisions. For example, they may prohibit personal data transfers to entities based outside the European Economic Area or contain definitions that no longer work properly after Brexit. These contracts might become open to termination or uncertain in scope.	• Review contracts to check whether they contain such prohibitions/definitions. • Consider amending contracts/entering discussions with other parties as appropriate.

For more information or an informal chat please do contact us:

Peter Wainman

Tel: +(44)(0)1223 222408

Email: Peter Wainman@mills-reeve.com

www.mills-reeve.com/Brexit