Commercial

BREXIT and the new EU Data Privacy Regime: How will your business be impacted?

The recent decision by the UK to withdraw its EU membership ("BREXIT") has undoubtedly thrown into uncertainty its future legislative boundaries in relation to Europe. While the relationship between the UK and the EU is not likely to be significantly harmed by BREXIT and the follow-on negotiations, there now exist some major unanswerable legal questions including how to apply the new EU data privacy rules. These rules are aimed primarily at simplification and harmonisation of the data protection regime across EU Member States. They are contained in the new General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) which is expected to be formally adopted in early 2016 with an effective date in May 2018.

If as a result of the negotiations following from BREXIT the UK remains a member of the single market known as the European Economic Area (EEA), the UK will be subject to the requirement to observe the four freedoms—freedom of movement of persons, capital, goods and services—which include the GDPR. If the UK determines not to be an EEA member, domestic rules will need to be put into place which still provide an "adequate level of protection" for individuals' data privacy. This will be necessary to meet the standards imposed by the European Commission on data transfers by UK businesses into the EEA.

The UK Information Commissioner's Office in charge of data protection issues will need to oversee and ensure that appropriate reforms are implemented in order for the national regime to be deemed adequate. Currently businesses that collect personal data in the United Kingdom must comply with the Data Protection Act 1998 ("DPA") which was the domestic implementation of the 1995 EU Data Protection Directive (95/46/EC). The DPA sets out principles for handling personal data and protecting the privacy of all living individuals or "data subjects" whose data is collected, processed and stored.

The GDPR will alter the existing regulatory landscape for data privacy by providing more rigid rules and by extending the territorial reach of the EU data protection regime. This will apply to cross-border data transfers and require businesses to carry out impact assessments in addition to drafting new clauses into the contracts between data processors and data controllers. Such parties are the persons responsible for handling individuals' private data. Personal data includes any information relating to a data subject by which they can be identified. This means their name, address, date of birth and preferences as well as others' views about them. The GDPR will expand the territorial application of the EU data privacy rules to non-EU businesses that conduct business in an EU Member State. There are no grandfather provisions in the GDPR so its requirements will apply to all existing agreements and businesses.

The GDPR includes a requirement for updated guidelines, tools and procedures to be developed to allow the new legal framework to be effective for mid-2018. This will involve formation of a European Data Protection Board, or EDPB for harmonisation across Europe and interpretation of the rules. The EDPB will also issue guidelines and best practice so that implementation of the GDPR requirements is uniform across all European Member States.

Increased penalties imposed under the GDPR for violations of the data privacy rules include fines of up to 4% of annual global turnover or €20 million (whichever is greater). Breach notification rules in the GDPR will also apply which will make it mandatory to report violations. Data controllers will have to 'promptly' report data breaches to the relevant Data Protection Authority where there is a "high risk" to the rights and freedoms of data subjects. This means such notifications are to be made within 72 hours. Companies will also have to adopt internal procedures for handling data breaches. Data erasure is also covered by the GDPR which entitles the data subject to have the data controller erase his or her personal data and stop any further transfers or processing of that data. This "right to be forgotten" arises when the data is no longer relevant to the original purposes for processing or the data subject has withdrawn his or her consent.

The new post-BREXIT legal landscape for data privacy compliance requires careful navigation. Should you require advice and assistance on compliance with the new rules please contact your usual 3HR consultant or our Commercial Law team which can advise accordingly.

Carol Kilgore
Commercial Solicitor
E: carol.kilgore@3hrcs.com