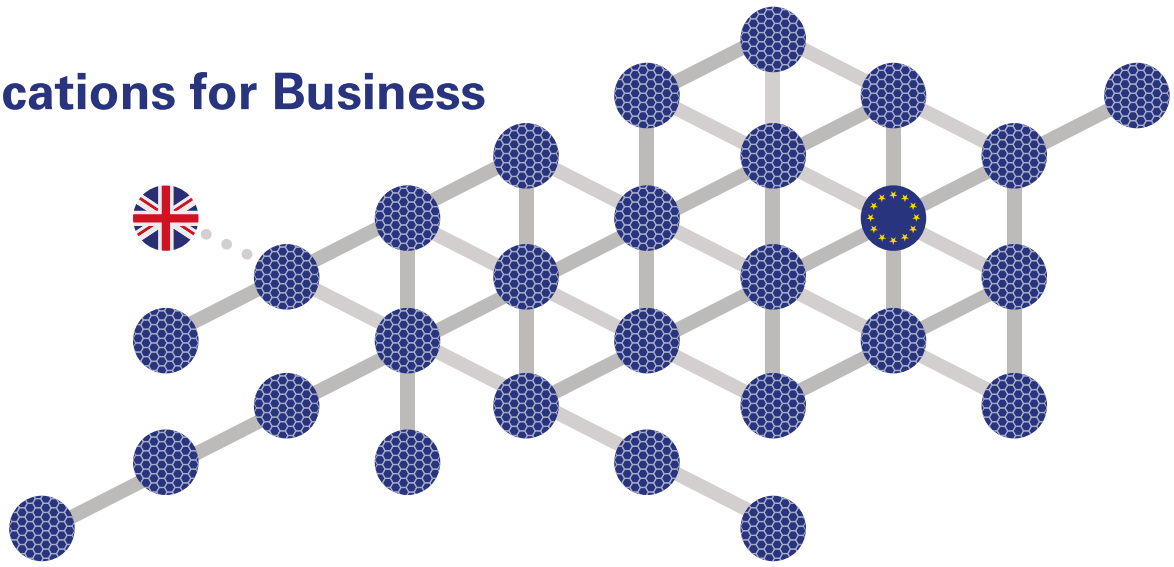
SHEPHERD+ WEDDERBURN

GDPR
The Implications for Business



The General Data Protection Regulation (GDPR) will come into force on 25 May 2018. GDPR introduces wide-ranging changes to UK data protection legislation and, if they have not already started, it is essential that businesses begin to take steps towards compliance. The Government has confirmed that the UK will implement GDPR and it is widely expected that the UK will continue to comply with GDPR even after Brexit.

What are the main changes?

GDPR follows a similar approach to existing data protection legislation, however, there are some material changes:

Tougher Fines

GDPR significantly increases the level of fines that can be imposed. A fine of up to €20m or 4% of total worldwide turnover, whichever is higher, may be imposed for more serious offences, such as a breach of the basic data protection principles or a breach of international transfer restrictions. A fine of up to €10m or 2% of total worldwide turnover, whichever is higher, will apply to less serious offences such as a failure to maintain a data processing register.

Scope

All businesses, even those located outside the EU, must comply with GDPR where they offer goods or services to individuals within the EU or monitor the activity of people within the EU (eg. internet profiling).

Accountability Requirement

GDPR introduces an obligation on data controllers and processors to show how they are complying with the data protection principles. This includes the creation and maintenance of data processing registers. If not already in place, comprehensive governance measures should be put in place to minimise the risk of a breach and safeguard the protection of personal data. Appropriate measures include privacy impact assessments for high-risk processing and steps to ensure that data protection is incorporated by design and by default rather than being an afterthought. An element of accountability has always formed part of data protection law but GDPR places greater focus on this and businesses should ensure that existing policies and record-keeping are sufficient to satisfy the new requirements.

A prime example of this increased focus is that data controllers must notify the Information Commissioner's Office within 72 hours of becoming aware of a data breach that poses a risk to data subjects.

Data Processors

At present, data processors are not under any direct obligations (other than via the data controller) and the data controller is responsible for any breach committed by its processor. GDPR imposes specific obligations on data processors, including an obligation to implement appropriate security standards, ensure adequate record-keeping and inform the data controller of any breach.

SHEPHERD+ WEDDERBURN

Data processors will now be exposed to regulatory fines or private claims from individuals in the event of a breach. GDPR also mandates a number of provisions that must be included in all contracts involving the processing of personal data. This increased regulatory burden and exposure to risk may result in a change to existing commercial arrangements and businesses should have a dialogue with relevant suppliers.

Data Protection Officers (DPO)

In some circumstances a DPO will need to be designated by the data controller or processor. This will primarily apply where the processing involves regular and systematic monitoring of data on a large scale or to the public sector. The DPO must have sufficient knowledge to perform the role and a single DPO may be designated for a group of undertakings.

Consent

Where processing is based on consent, the data controller will be required to demonstrate that such consent was given by the individual and the opportunity to withdraw consent must be made as easy as the giving of consent. There is no grandfathering of consent under GDPR and so businesses must ensure that pre-existing consents are GDPR compliant. As a result, certain businesses may seek to move away from using consent and seek to rely on an alternative legal basis, such as performance of a contract or a legitimate interest of the data controller.

Data Subjects' Rights

The rights of data subjects have been extended such as the right to be forgotten, where an individual may request the deletion of their data when certain grounds apply. There is also a right to restrict processing in some circumstances together with a new right to have personal data provided to data subjects in a manner which allows it to be transferred easily (referred to as data portability). Parties will need to ensure they have processes in place to cater for the exercise of these rights.

What should businesses be doing now?

If they are not already doing so, all businesses, large and small, should be assessing their interaction with personal data and how GDPR will impact them and the sector in which they operate. Given the level of change that may be required, the deadline of May 2018 could arrive far sooner than anticipated.

SHEPHERD AND WEDDERBURN'S BREXIT ADVISERS

JOINING THE DOTS OF THE EU REFERENDUM

What next?

Shepherd and Wedderburn has been for many years offering balanced and impartial advice on how the different scenarios might play out in the event of constitutional change.

Now that the vote has been cast to leave the EU, members of our dedicated Brexit group continue to interrogate the regulatory and commercial issues and to advise clients on next steps and outcomes.

For further information in the first instance, please contact:

Joanna Boag-Thomson
Partner
T +44 (0)141 566 8570
M +44(0)775 387 1607
E joanna.bt@shepwedd.com

Bookmark our Brexit Advisers page for a comprehensive collection of Brexit updates and guidance

shepwedd.com/brexit

© 2017 Shepherd and Wedderburn LLP. Shepherd and Wedderburn LLP is a limited liability partnership (with registered number SO300895) regulated by the Law Society of Scotland and authorised and regulated by the Solicitors Regulation Authority (with number 447895).