STEPHENSON HARWOOD

The EU General Data Protection Regulation

Following four years of development, the EU General Data Protection Regulation (the "**GDPR**") was adopted on 27 April 2016 and is set to come into force across the EU on 25 May 2018. The GDPR aims to consolidate and strengthen data protection rights for individuals within the EU. Many of the GDPR's changes will significantly impact your business (not least by significantly increasing the penalties for breach), and organisations should be taking steps now to prepare for its implementation, regardless of "Brexit".

What are the key changes?

Fines

The most eye-catching change is the introduction of maximum fines of up to the higher of 4% of a data controller's worldwide turnover or €20m. This is a huge increase on the current maximum sanctions (being £500,000 in the UK).

Accountability

There is greater emphasis on being able to evidence compliance including by carrying out Privacy Impact Assessment for high risk projects, keeping detailed records of consents obtained and implementing so-called "privacy by design" internal processes.

Breach Notification

A mandatory breach notification regime is introduced requiring regulators to be notified of most personal data breaches within 72 hours and also requiring that data subjects be informed of high risk breaches.

Legal Grounds and Privacy Notices

Legal grounds (such as consent) are made more onerous for organisations to satisfy and the requirements for the content of privacy notices are changed meaning all organisations will likely need to amend their existing privacy notices and terms.

Rights of Data Subjects

Data subjects are given new and enhanced rights including a more extensive "right to be forgotten", a right of "portability" (allowing for free transmission of data in commonly used formats) and strengthened rights to object to processing.

Data Processors

Entities that process personal data on behalf of a data controller (for example, IT service providers) will have certain data protection obligations imposed on them under legislation directly for the first time.

What is the territorial scope?

The GDPR will apply to all businesses that control or process personal data relating to data subjects within the EU, regardless of where the business is based, where the processing relates to the offering of goods or services to EU-based data subjects or the monitoring of data subjects' behaviour in the EU. This means that the GDPR will apply beyond the EU boundaries. Non-EU resident businesses that process data relating to EU citizens must appoint a representative within the relevant member state.

What about Brexit?

On 25 May 2018 the GDPR will become directly effective in all member states of the EU, which is almost certain to still include the UK at that point. This means that the GDPR will be directly applicable in the UK for at least several months before it ceases to apply automatically. After this point it is very likely that the UK government will seek to retain or replicate the GDPR in national law at least in the medium term based on public statements of regulators and government figures. The UK Information Commissioner, Elizabeth Denham, in particular has been clear in her intention that "Brexit" should *not* mean "Brexit" for data protection.

Furthermore, given the extra-territorial scope of the GDPR, any UK (or indeed global) business doing significant business in the EU post-Brexit will still need to apply its rules regardless of its legislative status in the UK.

What should you be doing now?

Although certain provisions may need to be further clarified in guidelines expected prior to implementation in 2018, organisations should start preparing now, given the scale of the changes that will be required. Steps that can be followed now would include:

- **Audit** what data is collected, where it is stored and the legal basis of processing.
- **Review** existing privacy policies and terms with data subjects as well as terms with third party data processors or other counterparties and put in place a plan to make any changes required to comply with the enhanced requirements of the GDPR.
- **Assess** procedures for handling individual requests including subject access and rights of erasure as well as the process for reporting and notifying data breaches.
- **Plan** any changes to systems and processes that will be required to satisfy the requirements, particularly those relating to the Accountability principle and the ability to implement "privacy by design".

The ICO has released a helpful paper with 12 steps to take now which contains some further tips on how to plan for the GDPR.

If you would like further information relating to any of the above, please feel free to contract a member of our team using the details set out below.

Our team

Jonathan Kirsop
Partner
T: +44 20 7809 2121
E: jonathan.kirsop@shlegal.com

Caieta Hendry
Senior associate
T: +44 20 7809 2382
E: caieta.hendry@shlegal.com

Naomi Leach
Senior associate
T: +44 20 7809 2960
E: naomi.leach@shlegal.com

Chloe Haywood
Associate
T: +44 20 7809 2348
E: chloe.haywood@shlegal.com

Katie Hewson
Associate
T: +44 20 7809 2374
E: Katie.hewson@shlegal.com

Alison Kenney
Associate
T: +44 20 7809 2278
E: alison.kenney@shlegal.com

Michelle Gomes
Associate
T: +44 20 7809 2370
E: michelle.gomes@shlegal.com

"The team really know what they're doing. They just become part of our team."

Chambers and Partners UK

Ranked for Data Protection

Legal 500 UK 2016

Stephenson Harwood is a law firm with over 900 people worldwide, including more than 140 partners. Our people are committed to achieving the goals of our clients - listed and private companies, institutions and individuals.

We assemble teams of bright thinkers to match our clients' needs and give the right advice from the right person at the right time. Dedicating the highest calibre of legal talent to overcome the most complex issues, we deliver pragmatic, expert advice that is set squarely in the real world.

Our headquarters are in London, with nine offices across Asia, Europe and the Middle East. In addition we have forged close ties with other high quality law firms. This diverse mix of expertise and culture results in a combination of deep local insight and the capability to provide a seamless international service.

STEPHENSON HARWOOD