THINKHOUSE
Gowling WLG's in-house lawyer community

RE-THINK

Data Protection

After four years of debate in Europe, the new General Data Protection Regulation ("GDPR") has been agreed (almost). With a wider reach than the existing Data Protection Directive, it will apply directly to controllers as well as processors. In December 2015 agreement was reached in Europe on the GDPR and we saw an unofficial draft of the 'final' text. The final text is expected this Spring/Summer, the GDPR coming into action two years from publication (2018).

The GDPR will also apply to organisations outside of Europe which are targeting goods and services at or tracking/ profiling individuals in Europe.

The GDPR will have direct effect (so no national implementation) - unlike the current Directive which is implemented into Member State laws by national legislation – and as a result led to a mis-matched patchwork of data protection laws across Europe. Although a more uniform approach will likely come about as a result of the direct application of the GDPR, there is however still plenty of room allowed by the GDPR for national regulators to set national/sector standards and variances.

With penalties for breaches set at (the higher of) 4% of global annual turnover for the previous financial year or 20 million euros, all organisations need to start preparing for the GDPR now.

Preparing for the GDPR

- Brief the board so they are aware of the risks to the business and what needs to happen over the next two years to get GDPR compliant.
- Appoint/train a Data Protection officer. Some organisations must appoint one under the GDPR but even if not mandatory for your organisation think about appointing one anyway. There will be a lot to do and it will take a particular skill set and experience. Data protection experts will be in demand so get yours lined up sooner rather than later.
- Conduct a data protection assessment to find out exactly what personal data is processed around the business, why and whether it is done compliantly under current law.
- Review and update existing data protection policies, training, privacy notices etc so that they are fully up to date for compliance with current laws. Then over the next couple of years get them to the next level for GDPR compliance.
- Assess what processing of personal data will need to be consent based in the future and assess whether the business already has the necessary consents or whether these need to be obtained, what information to be provided to data subjects so it's an informed consent and how you will evidence consent.
- Implement new compliance tools the business might not have had previously such as Data Protection Impact Assessments, Security Breach Handling Policy, Data Retention and Destruction Policy, Data Subject Access Request Handling Policy. Previously these might have been considered nice to haves but in the future will become a must have to help stay on the compliant side of the GDPR.
- Map personal data sharing around the group and to and from third parties and put in place mechanisms for compliant international personal data transfers.
- Update data processor and security provisions in contracts to cover extended processor obligations that controllers must contractually impose. If you are a processor, assess additional risk impact on the business of additional contractual and security obligations and direct responsibility and potential fines under the GDPR.

THINKHOUSE
Gowling WLG's in-house lawyer community

RE-THINK

Please see below a link to the position of the Council at first reading with a view to the adoption of the Regulation

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT

KIRSTEN WHITFIELD

Director

T +44 121 393 0755
Kirsten.whitfield@gowlingwlg.com

PETER HALL

Partner

T +44 (0) 370 730 2834
Peter.hall@gowlingwlg.com