General Data Protection Regulation (GDPR)

FACT SHEETS

Introduction

The EU General Data Protection Regulation (**GDPR**) replaces the EU Data Protection Directive. Businesses that fail to comply with the new GDPR by 25 May 2018 will be at risk of claims from affected data subjects and may be subject to significant fines of up to €20 million or 4% of their total worldwide annual revenue.

Principles

Article 5(1) of the GDPR sets out the principles relating to processing of personal data and states that personal data shall be:

a) "processed lawfully, fairly and in a transparent manner in relation to the data subject". Therefore, in order to process personal data businesses must have legitimate grounds for collecting and using that data and be transparent about how they intend to use it. Importantly, the GDPR imposes a higher standard of consent and requires businesses to be able to demonstrate that the data subject gave clear consent to the use of their data (as opposed to implied consent under current data protection law) and puts the onus on businesses to prove that such consent was obtained.

b) "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". In practice, this means that businesses must be clear from the outset as to why they are collecting personal data and what they intend to do with it.

c) "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This means that businesses should collect no more personal data than they need for the purpose.

d) "accurate and, where necessary, kept up to date". Businesses must take reasonable steps to ensure the accuracy of personal data and ensure that any inaccurate data is deleted or amended as soon as possible.

e) "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". Businesses will need to review the length of time they keep personal data and justify how long they retain it.

f) "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage". Businesses will need to implement appropriate organisational and technical measures to protect personal data against unauthorised access.

Article 5(2) of the GDPR introduces the principle of accountability and requires data controllers to be able to demonstrate that their data processing activities comply with the GDPR. Meeting the accountability requirement means doing more than just establishing policies and procedures. Businesses will need evidence to demonstrate the implementation of those policies and processes as well as of effective internal compliance measures and external controls.

Data Subjects' Rights

Chapter III of the GDPR outlines data subjects' rights as follows:

a) the right to receive certain information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" which must be provided free of charge;

b) the right to obtain confirmation "as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data";

c) the right to obtain "without undue delay the rectification of inaccurate personal data concerning him or her";

d) the right to obtain "the erasure of personal data concerning him or her without undue delay";

e) the right to obtain restriction of processing if the accuracy of the personal data is contested or unlawful;

f) the right to receive the personal data and the right to transmit that data to another controller without hindrance;

g) the right to object to processing of personal data concerning him or her; and,

h) the right not to be subject to a decision based solely on automated processing.

To give effect to these rights the GDPR imposes obligations on businesses to comply with them when communicating with data subjects, responding to data subject requests, handling data portability requests, acting as a joint data controller, using automated processing (including profiling) to make decisions or handling a personal data breach.

To prepare for the GDPR businesses should determine the extent to which it will affect their business, review their current procedures, and implement and update their processes to ensure compliance. KBL are happy to explain the changes under the GDPR and explore the risks to which businesses may be exposed.

For further information please contact:

Phil Stephenson pstephenson@kbl.co.uk
Jonathan Shorrock jshorrock@kbl.co.uk
Anneka Traynor atraynor@kbl.co.uk

Tel: 01204 527777 / 01254 268790