ADDLESHAW GODDARD

DATA PROTECTION IN THE MODERN ERA – THE GENERAL DATA PROTECTION REGULATION

- The General Data Protection Regulation (**GDPR**) is due to come into force across the EU on 25 May 2018.
- The GDPR will grant more rights to individuals, impose significant new burdens on organisations and introduce increased fines and penalties.
- The GDPR (along with the Data Protection Bill currently making its way through the House of Commons) will replace the current Data Protection Act 1998 (which implements the Data Protection Directive 95/46/EC (**Directive**)).

What's it about?

The GDPR represents the biggest change to data privacy law in the last 20 years. The GDPR's aim is to bring a consolidated approach to data privacy law to reflect modern uses of personal data. Much of the GDPR reflects the Directive with many of the concepts being familiar including personal data, data controllers and data processors. However, the GDPR introduces a number of new concepts including:

- enhanced transparency obligations which require organisations to inform individuals how their data is collected, the purpose for which it is processed, the lawful grounds relied on, where it is stored, who it is shared with and the extent of any international transfers of such data;
- a higher threshold for consent, requiring many organisations to review the consent that is currently relied on;
- direct statutory obligations on data processors for the first time;
- mandatory processing provisions to be included in data controller – data processor contracts, causing organisations to amend their existing contracts; and
- new rights for data subjects including the right to erasure ("right to be forgotten").

Why does it matter?

Given the changes the GDPR makes to the Directive, every organisation (whether controller or processor) will need to proactively review its current practices, policies and contracts to ensure compliance with the GDPR and document the steps taken in its compliance programme.

Depending on the type of breach, failure for non-compliance with the obligations of the GDPR could result in an administrative fine of up to €20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher). This does not include the internal time and costs spent in relation to a breach nor the potential PR repercussions.

Now what?

Before pen can be put to paper, an organisation will need to ensure that it understands how it currently processes data. It must engage with employees and key stakeholders to understand the data processing of the organisation and ensure that all are aware of the main implications of the GDPR. It is also essential that organisations provide training to employees in order to ensure compliance.

Many organisations will need to keep a record of each type of personal data being processed, undertake privacy impact assessments to understand risks to personal data in particular systems or projects and provide fair processing notices outlining these processing activities to such individuals (e.g. through HR policies, website privacy policies, etc.).

Organisations will also need to update their contracts to include the prescribed provisions. Any data processor subcontracting its obligations will also need to ensure that such terms are flowed down to the sub-processor.

Who to contact

HELENA BROWN
Partner
+44 (0) 131 222 9544
07407 735118
helena.brown@addleshawgoddard.com

BEATRICE DUKE
Managing Associate
0113 209 2019
07730 320881
beatrice.duke@addleshawgoddard.com

10-20291077-1

addleshawgoddard.com

Aberdeen, Doha, Dubai, Edinburgh, Glasgow, Hong Kong, Leeds, London, Manchester, Muscat, Singapore and Tokyo*

*a formal alliance with Hashidate Law Office