THE NEW DATA DICTUM

GET IN TOUCH

JOHN SHARPLES
Data Protection Practitioner, Giving Solutions
T | +44 (0)20 7556 1217 E | sharplesj@buzzacott.co.uk

Buzzacott
GIVING SOLUTIONS

BUZZACOTT
BEYOND THE NUMBERS

The world of data protection is set for dramatic change. John Sharples, from our Giving Solutions team, outlines what the new regulations mean for your organisation.

Data Protection laws have traditionally been a headache for companies operating across the EU, where regulations differ across countries. But after years of negotiation between member states, change is afoot. 25 May 2018 marks the introduction of the new General Data Protection Regulation (GDPR), a drastic overhaul of current legislation. The GDPR will unify law across member states and, crucially, comes into effect before the UK departs the EU.

The change will affect any organisation holding personal data – that is any information about a living individual that can be identified from that data alone, or alongside other information that the organisation holds. So in reality, this will affect most organisations. Are they ready to ensure compliance?

Strong incentives for best practice

Non-compliance with GDPR could have serious ramifications. The EU is set on synchronising often differing data standards in member states and determined to ensure best practice is upheld. The top level of fines could be up to a whopping €20m, or up to 4% of total worldwide annual turnover of the preceding financial year, whichever is greater.

Faster turnaround times

There will be more responsibility put onto Data Processors, who must notify the Controller if they become aware of a breach. For Data Controllers, there will be mandatory breach reporting to the ICO (Information Commissioner's Office, or other supervisory authority if applicable). In some cases the Controller must communicate the personal data breach to the data subjects. Individuals requesting access to their data must now be responded to within a month.

Tighter checks

The regulation also requires that for types of processing likely to result in a high risk to the rights and freedoms of natural persons, a Data Protection Impact Assessment be carried out. Examples of where this might be required is for outsourcing data processing, data migration to new IT systems and use of Cloud systems.

Data Protection Officer

Lastly, organisations may need to appoint a Data Protection Officer (DPO). This is obligatory in certain organisations:

- for a public authority or body;
- where the core activities of the Controller or Processor consist of operations that profile on a large scale;
- there is large scale processing of special categories of personal data.

A DPO must not have a conflict of interest with any other tasks or duties so cannot for example be a CEO, COO, CFO, Head of Marketing, HR or IT. While many organisations will appoint a DPO to their staff, an external person can fulfil the role.

"The change will affect any organisation holding personal data – that is any information about a living individual that can be identified from that data alone, or alongside other information that the organisation holds."

Time to act

The most likely reasons for non-compliance will be failure to keep personal data secure (both physically and in IT systems), sharing data when no consent has been given, and processing the data for any purpose other than that for which it was collected. To prepare for the new law, organisations should act now to review policies and procedures, to consider if they will need to appoint a DPO and examine any data collection notices in marketing and fund-raising material.

If you're uncertain about how the GDPR might impact you, please contact us.

This article was taken from Buzzacott's firm-wide magazine, Beyond the Numbers ▶