24th May 2016

New EU Data Protection legislation comes into force today. What does this mean for your business?

After years of discussion and proposals, the General Data Protection Regulation ("**GDPR**") finally comes into force today (24 May 2016).

Businesses that process (i.e. collect, record, store, hold, and/or use) data about individuals ("**personal data**") now have two years (until 25 May 2018) to comply with the GDPR, as this is when EU Member States must adopt the GDPR into national law.

Given the extent of the changes, however, businesses will need to start preparing for compliance with the new legislation sooner rather than later.

Background

EU data protection legislation has been in force since 1995, when the EU Data Protection Directive came into force ("**DPD**").

As a directive, each EU member state was required only to implement the minimum standards contained within the DPD into national legislation. There are, therefore, inconsistencies between each Member State's data protection laws. For example, the UK's legislation which adopted the DPD – the Data Protection Act 1998 ("**DPA**") - has many differences to its German equivalent.

The GDPR, as a Regulation, must be adopted by each Member State as written, which will provide greater certainty to businesses who deal with personal data across Europe.

A full account of the changes that will be introduced under the new legislation is beyond the scope of this article, but some of the key changes that are likely to affect businesses that process personal data are set out below. One of the most significant changes is the level of fines that businesses may be exposed to if they fail to comply with the new legislation.

Fines

Under the DPA, the maximum fine which may be imposed on a business for non-compliance is £500k.

The GDPR introduces a new maximum fine of up to €20 million or 4% of a business' total worldwide annual turnover, whichever is higher.

This represents a significant increase in the level of fines that local data protection authorities can impose on businesses, and its aim is clearly to incentivise all businesses (large and small) to take care and to act responsibly when dealing with individuals' personal data.

Although the current maximum fine under the DPA is not negligible, for larger companies, the bigger deterrent against non-compliance has tended to be the potential reputational damage that can be caused by widespread publication of a serious breach of the DPA. The potential for reputational damage will continue to be a major deterrent, but it is now coupled with the potential for hefty fines as well.

Data Controllers and Processors

Under the DPA, the responsibility for ensuring that personal data is processed in compliance with the DPA falls on the party that collects the personal data and that chooses how to use it ("**controller**").

Where the controller appoints a third party to process personal data on its behalf, and in accordance with its instructions ("**processor**"), the controller is responsible for any breach of the DPA by the processor. Under existing legislation, therefore, it is not unusual for prudent controllers to impose various contractual obligations on processors, as the obligations under the DPA do not generally extend to the processor.

The GDPR now places direct responsibility on processors (for example in relation to security arrangements and transfers of personal data). As a result businesses, such as those that provide third party outsourcing services to controllers, should now consider how to address their new responsibilities.

Territorial Scope

Under current EU data protection legislation, a business must either be based, or have equipment which it uses to process personal data, in a Member State for that Member State's data protection laws to apply.

Businesses have tried to avoid being subject to the current EU data protection legislation by not establishing any premises or equipment within the EU, albeit with less success recently.

The GDPR extends the territorial scope of the EU data protection legislation vastly, applying to all businesses that:

- offer goods or services to EU residents (whether a payment is required or not); or
- monitor EU residents' behaviour within the EU.

The effect of this is that even where a business, located outside the EU, does not offer goods or services to customers in the EU, they could still be caught by the GDPR where they analyse EU residents' internet usage (which will include where they use tracking cookies).

Data Subjects' Rights

A "data subject" is the person whose personal data is being processed.

Right to be forgotten: The current position under the DPA is that a controller must ensure that the personal data it processes is accurate and up-to-date, and retained only for so long as is necessary. The data subject may apply to court to obtain an order against the business to correct or destroy any personal data which is not processed in accordance with the DPA.

Recent case law has extended the above right so that individuals can apply directly to organisations to ask them to remove or delete personal data held about them: unless the organisation has a legitimate reason for retaining personal data, it must comply with the request.

The right to be forgotten has now been codified in the GDPR. In addition, the following concepts have been introduced to increase data subjects' rights under the new legislation:

- **Privacy by Design:** The GDPR introduces a new obligation on businesses to implement safeguards in their products/services, at the earliest stage in their development, to safeguard personal data. Any default settings must be privacy-friendly (for example in apps and social media websites).

- **Data Portability:** The GDPR introduces a new right for data subjects to ask service provider businesses to transfer information they hold electronically either to them or to a third party. Any such transfer must be in an 'electronic format which is commonly used'. A business may, therefore, need to incur costs in changing the format to one which is commonly used.

Not only should businesses start considering how they will respond to and action requests to be forgotten and/or to port personal data, but also what safeguards to implement in any new products and services they develop.

Notification of Security Breach

Controllers and processors each have obligations under the GDPR to report security breaches.

The processor's responsibility is to report a data breach to the controller, without undue delay, after becoming aware of the breach.

The controller is under an obligation to notify the supervisory authority without undue delay and – where feasible - not more than 72 hours after becoming aware of the breach. However, there is no obligation to report it where the breach is *"unlikely to result in a risk for the rights and freedoms of individuals".* No guidance has been provided on this wording, but it is understood that this reporting obligation will apply where there is a risk of damage to the data subject.

The onus is on the controller to decide what is and is not likely to create a risk, and whether to report it to the supervisory authority.

The controller is, furthermore, required to communicate the breach to the individual whose personal data is subject of the breach, where there is a *"high risk for the rights and freedoms of individuals"*. Again, no guidance has been provided on this wording, however it is understood that this will extend to situations where there is a threat of identity theft. Once again, the onus will be on the controller to decide the severity of the risk.

Controllers should, therefore, consider whether their data protection policies address the process which their employees and contractors must follow where there is a security breach. It would be prudent also for controllers to keep a log of security breaches, and where they have chosen not to inform the supervisory authority and/or data subject of a security breach, to record in that log the reasons in each case for that decision.

Data Protection Officers ("DPO")

Many businesses already have in place internal data protection policies which include details of how employees and contractors are to process personal data, who to report breaches to, and what to do when considering outsourcing business processes to third parties.

Organisations which are controllers or processors and who either:

- regularly and systemically monitor data subjects; or
- process sensitive personal data,

on a large scale will now be required under the GDPR to appoint a DPO. What 'large scale' processing will entail has not yet been decided.

The DPO's responsibilities will include advising controllers and processors of their obligations under the GDPR, monitoring their compliance, and co-operating with supervisory authorities. The DPO must be selected on the basis of their *'professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks [prescribed to them under the GDPR].'* Group companies may appoint a single DPO.

Businesses should therefore consider whether they are likely to need to appoint a DPO under the GDPR. Given the level of expertise required of the DPO and the fact that the recruitment process can take a while, businesses should consider this well in advance of 25 May 2018.

Impact Assessments

The GDPR now requires controllers to conduct a detailed impact assessment on the risks associated with processing certain personal data, and how those risks will be addressed, each time they consider adopting a new type of processing (including through new technology) where there is a *"high risk for the rights and freedoms of individuals"*.

Where a DPO has been appointed, the business should seek the DPO's advice when conducting any impact assessment.

International Data Transfers

Under the DPA, the controller may only transfer personal data outside the EU:

- with the data subject's consent (which is often obtained through a clause in the controller's privacy policy);
- (where the controller does not have the individual's consent) to countries which the European Commission has identified as 'safe' ("**safe harbours**"). These countries are, as we have recently seen with the removal of the USA as a safe harbour, subject to change; and
- where the controller has ensured that it has appropriate safeguards in place to protect the privacy of the personal data; where the controller appoints a third party to process personal information, this is achieved by the controller imposing the same obligations on the processor as the DPA imposes on it; for this purpose

the EU has provided a set of standard clauses which can be included in contracts between controllers and processors to show compliance with the DPA ("**standard clauses**").

The GDPR introduces changes to the above as follows:

- where the controller is relying on the data subject's consent, it must now be explicit consent (which could be provided by a pop-up with a tick-box); burying a clause in a privacy policy, which states that a person consents to the transfer of their personal data outside the EU, is likely to no longer be sufficient;

- there will still be a list of safe harbours, however this list will be subject to periodic review (which will be at least every four years); the safest option for a controller may be to include the standard clauses (see below);

- parties will still be able to rely on standard clauses to show compliance with the DPA.

Under the GDPR, these obligations apply directly to processors as well as controllers. Processors, therefore, need to ensure that any contracts they have with sub-processors, and which extend beyond 25 May 2018, address international transfers of personal data.

Conclusion

The GDPR extends the scope of current EU data protection legislation, most notably in that it applies now to processors and to companies based outside the EU which monitor the behaviour of EU residents.

Given the nature and the extent of the obligations imposed on businesses by the GDPR, and in particular the considerable higher level of the fines, businesses should start preparing themselves as far in advance of 25 May 2018 as possible.

Authors

Eesheta Shah
Consultant
Media and Technology
eesheta.shah@marriottharrison.co.uk

Richard Woods
Associate
Media and Technology
richard.woods@marriottharrison.co.uk

Marriott Harrison LLP
11 Staple Inn
London
WC1V 7QH

DISCLAIMER

The information and any commentary contained in this article is for general information purposes only and does not constitute legal or any other type of professional advice. Marriott Harrison LLP does not accept and, to the extent permitted by law, excludes liability to any person for any loss which may arise from relying upon or otherwise using the information contained in this article.

If you have a particular query or issue you are strongly advised to obtain specific, personal advice about your case or matter and not to rely on the information or comments in this article.