# GDPR: Putting the processes in place

03 August 2016

**Companies need to be aware of the changes under GDPR and ensure the appropriate systems are there to comply**

Company directors keen to avoid a sleepless night should make sure that data protection is given priority on their board agendas. Changes to the data protection regime coming into force in May 2018 will mean that businesses providing services to EU citizens could face fines of up to €20 million or 4% of their worldwide turnover, whichever is higher.

Following four years of deliberation, the European Commission has published details of its new rules governing data protection. This moves away from a directive which had been interpreted differently by member states, leading to confusion, and opting instead for a directly applicable regulation.

Britain may have voted to leave the EU, but the General Data Protection Regulation (GDPR) is a good example of the sort of regulation that will still apply to UK companies under certain circumstances. The GDPR governs the data protection of any business providing services to or monitoring the behaviour of EU citizens, making it applicable to those businesses regardless of which country they are domiciled.

The GDPR builds on the principles established under the 1995 Data Protection Directive and introduces some new and significant measures to make the law as future-proof as possible. Although some of these may be considered challenging and possibly onerous, securely protecting the extensive personal data that an organisation can collect and store at the click of a button is vital for businesses. It is a critical part of building consumer trust and will help ensure that corporate reputations are protected.

The Eurobarometer survey by the European Commission in June 2015 showed that 67% of Europeans worried that they had no control over their online information, with 63% admitting that they do not trust online businesses.

With organisations such as Nationwide, TalkTalk, T-Mobile and HMRC all having succumbed to significant data breaches, placing the personal information of millions of people at risk, the lack of confidence is understandable. Even if the UK chooses not to adopt the GDPR for its own national data protection legislation following Brexit, robust data protection laws will still be necessary to ensure consumer trust and to protect cross-border arrangements for data transfers.

The GDPR has simultaneously tightened the regulation and raised the bar on enforcement. Fines currently vary and are relatively low (with a maximum of £500,000 in the UK), however the GDPR will increase the maximum fine significantly, depending on the infringement. Maximum fines can range from €10 million or 2% of an undertaking's worldwide turnover, to €20 million or 4% of its worldwide turnover (whichever is higher). EU countries are likely to be rigorous in their monitoring of businesses complying with GDPR, so ensuring adequate procedures are in place will be essential.

## The changes

Companies bound by the GDPR will need to be aware of the following changes and ensure appropriate systems and processes are in place to comply.

### Consent

The GDPR makes it explicit that businesses must have a valid reason for each and every instance of data processing. In addition, there must be proactive consent that is 'freely given, specific informed and unambiguous'. Pre-ticked boxes, inactive consent or silence indicating deemed consent are far less likely to be permissible.

Even when the data processing relates to multiple purposes, there needs to be affirmative consent for each one. Consequently many businesses will need to review their standard terms and conditions, existing customer contracts and privacy policies.

### Consent from children

Consent given by a child will only be deemed valid if authorised by the parent or guardian. This will apply for children under the age of 16, though in some member states it may apply to under 13s.

### Notification

Businesses will be required to notify their relevant supervisory authority within 72 hours of any data breach, unless that breach is unlikely to compromise the rights and freedoms of the data subjects. If the data controller is unable to do this, the delay will need to be justified to the data protection authority.

### Privacy by design and by default

Businesses will need to be able to demonstrate that appropriate data protection safeguards are considered from the embryonic stages of new product or service design and development. They will also need to evidence that data privacy safeguards are in place by default and that only appropriate and necessary data is collected and stored. Data protection impact assessments (PIAs) will need to be performed regularly to ensure that privacy risks have been identified and mitigated.

### Pseudonymisation

This is a new definition being applied under the GDPR and refers to data that has been processed or encrypted such that it can no longer be attributed to a specific individual or 'data subject'. Under the GDPR, businesses will be encouraged to apply pseudonymisation to the data they hold in order to significantly reduce the risks associated with data processing, while maintaining the data's utility.

The expectation is that data controllers will manage this aspect of data protection and that regulators will consider this technique to be a form of data security.

Pseudonymisation will also be encouraged as a process that will help satisfying the requirements to implement privacy by design. Further guidance on the use of pseudonymisation and the security requirements for data processed in this way are expected to be produced once the regulation comes into force.

**Registration**
Businesses will be required to maintain detailed documentation regarding their processing activities and data protection officers will be required in organisations where activities include large scale data processing.

In the past, it was sufficient to register with the relevant data protection authority, however, under the new legislation, businesses will be expected to maintain detailed documentation relating to their processing activities. Controllers and processors whose core activities include large-scale data processing must appoint a data protection officer.

**Liability for data processors**
The GDPR introduces direct compliance obligations for data processors and as such they may be liable to fines.

**The right to erasure ('the right to be forgotten')**
Following much publicity about this issue, the EU has chosen to enhance the existing rights to have personal data deleted in certain circumstances by giving individuals a new right to erasure. Data subjects will be allowed to request that their data be erased if the processing no longer satisfies the requirement of the GDPR, for example if the data is no longer necessary for the purpose for which it was collected, or if consent has been withdrawn and no other justification exists.

Where personal data was made public, data controllers will also be required to notify other controllers processing the relevant data of the need to erase it. This right to erasure is widely held to be one of the more onerous aspects of the new law and it will be interesting to see if member states draft exemptions. The equivalent provision under the 1995 Data Protection Directive allowed more discretion, just requiring the rectification, erasure or blocking of data 'as appropriate'. This will be one to watch if the UK drafts separate legislation following Brexit rather than adopting the GDPR.

**The right to object to profiling**
Individuals will also have the right not to be subject to decisions based on automated processing, including profiling, that might 'significantly affect' them. Given that profiling involves most forms of tracking and online behavioural advertising employed by many internet businesses, this rule could make the marketing activities of such businesses harder.

**Data portability**
This is another potentially difficult area of GDPR compliance and as such is an aspect of the legislation to monitor closely. The GDPR already gives individuals the right to ask for their data to be provided in a commonly used electronic form.

The right to portability goes beyond this and requires the controller to provide the data subject with the requested information in a structured, commonly used and machine readable format. This clause applies to personal data that has been freely given to the controller and has been processed by automated means.

Although the GDPR will not come into effect until 2018, those businesses that are likely to be affected are advised to begin the groundwork now, starting with a risk assessment to establish where their data is located, what their data subjects have agreed to and whether the data is adequately protected.

## 12 steps

According to the Information Commissioner's Office there are 12 key steps to take now:

- Raise awareness among key decision makers of forthcoming changes to the law and the possible impact
- Document the personal data held by the organisation, where it came from and who it is shared with
- Review policies and procedures that govern how personal data is managed by the organisation

Review privacy notices and put a timed action plan in place to implement any necessary changes

Ensure that all data processing is reviewed and that the legal basis for holding it is identified and documented

Ensure the right procedures are in place for detecting, reporting and investigating data breaches

Review the way in which consent is sought, obtained and recorded including systems in place to verify individual's ages and gather the consent of parents and guardians

Amend procedures to enable the organisation to handle erasure requests and data profiling objections

Appoint a data protection officer if required.

Whatever deal emerges as a result of negotiations with Europe, managing data protection should be considered as much a part of good governance as legal compliance. Whether a business needs to comply with the GDPR or not, having adequate procedures to protect personal data should simply be regarded good business practice. Companies should therefore ensure that their data protection measures are not simply delegated to the data protection team but evaluated as part of the overall business culture and the way the company does business.

Organisations should start with a systematic risk assessment of current practice and procedures to establish how their data is obtained, stored and transferred, in order to understand if it is properly protected. Tools such as GoodCorporation's Data Protection Framework can assist with this process, providing a gap analysis that identifies strengths and weaknesses and producing an action plan that shows what needs to be put in place.

You can read more about the GDPR in our article 'The next steps'.

**Leo Martin is Director at GoodCorporation**



ICSA: The Governance Institute
Saffron House, 6-10 Kirby Street, London EC1N 8TS, United Kingdom