Meritas Data Protection & Privacy
The GDPR - new data governance obligations on businesses
February 2017

Let's start with the good news. The current obligation to register with the national data protection authority will be abolished. Along with the fines and criminal offences of failing to do so.

In its place, the General Data Protection Regulation (GDPR) introduces raft of "data governance" obligations which puts the emphasis on organisations carrying out self-assessment exercises and documenting their data processing. The idea is to move away from box-ticking registration, to a culture where the use of personal data protection is scrutinised, justified and embedded into corporate and institutional data processing.

In some cases, such as when core activities require "regular and systematic monitoring of data subjects on a large scale" businesses will be required to appoint Data Protection Officers. Data Protection Officers must have a direct reporting line to the highest level of management and have a protected employment status- they cannot be dismissed for performing their functions.

Businesses are encouraged to adopt "data protection by design", meaning that they should think about the data protection consequences of all their activities. They should regularly audit the data they hold and document the reasons for doing so. They should train staff in data protection and adopt good practice techniques such as "pseudonymisation" to make it harder to identify individuals (for example, by using employee numbers instead of names in statistical analysis).

Where an activity might impact on privacy more seriously, such as monitoring people, or processing sensitive personal data, organisations will be required to carry out formal "Privacy Impact Assessments" to document the risks and the safeguards to be put in place. In certain cases, they will also have to notify the ICO of the Privacy Impact Assessment and seek permission before undertaking the proposed activity.

Organisations also have transparency obligations, meaning that it will be obligatory to say more about what they are doing. These requirements go beyond the typical privacy policy we see today. In addition to setting out the purposes for processing and the identity of the data controller, they include explaining the legal basis for the processing, the period(s) for which the data will be retained and people's legal rights - including that they have a right to complain to the ICO.

Businesses will therefore need to update their privacy policies and look at whether additional statements and disclosures need to be given, including at the point of data collection. This is especially true if a business is relying on the individual's consent. Under the GDPR, consent must be "unambiguous" and separate consents are required for each processing activity. Individuals must be presented with a sufficiently granular and genuine choice.

The new GDPR also focuses to "data processors" (those who process data on behalf of others). This means that many businesses which are not subject to the current regime, will now be liable. Worse, data processors will now have an obligation to inform the data controller if the processing they are

asked to undertake is unlawful. Meaning in effect that suppliers will have to police their customers' activities.

Data processors will also have an obligation to notify data controllers if there is any unauthorised loss or damage to personal data. And the data controllers themselves will have an obligation to notify the ICO within 72 hours of such an event. Unless an exemption applies, they will also have to inform the individuals whose data has been compromised. At the moment, only communication service providers (think "Talk Talk") have to do this, but soon it will apply to all data controllers.

Individuals have greatly enhanced rights under the GDPR and ensuring that they can exercise those rights will place an additional burden on business. The existing "subject access" right (broadly the right to see the information processed about you) will be extended. In addition, individuals will have new rights, such as the right to erasure (aka the "right to be forgotten"), a new right to require organisations to "restrict" processing while complaints are investigated and a right to "data portability". Portability is similar to subject access, but data has to be provided in a machine readable format and an organisation can be required to send the data directly to a new data controller. In other words, customers can ask a business to port their data to a new provider. This may help some businesses in lowering barriers to entry to certain markets, but it also means that businesses must develop systems to cope with portability requests.

The GDPR will make some things easier for businesses, especially those who trade across Europe, as the law will be harmonised to a greater extent. However, for a great many it will make life that bit harder, especially in transitioning to the new regime. Further, the potential fines for getting it wrong are to increase massively to the greater of 20 million Euros or 4% of the worldwide turnover of a business. Given this, businesses may want to examine their insurance cover and should in all cases ensure the data protection is moved higher up the boardroom agenda.

Over the next few months the Meritas Data Protection & Privacy Group will issue a series of articles. We will analyse all the chapters of the GDPR, describe the new obligations it introduces and the main challenges for businesses, organizations and institutions. We also aim to provide practical recommendations to ease the transition to the new regime introduced by this European general regulation.

Robert Lands
Partner, Head of Commercial & IP
Howard Kennedy, UK
robert.lands@howardkennedy.com

Carlos Pérez Sanz
Partner, Head of IT & Compliance
ECIJA, Spain
cperez@ecija.com