dun & bradstreet

CICM Chartered Institute of Credit Management

General Data Protection Regulation

What does it mean for you?

THIS DOCUMENT WAS COMMISSIONED BY THE CICM.

THE AIM IS TO PROVIDE BACKGROUND INFORMATION FOR CICM MEMBERS ON THE FORTHCOMING GENERAL DATA PROTECTION REGULATION (GDPR).

WHAT IS THE GDPR?

The General Data Protection Regulation, or GDPR, will come into effect throughout the EU on 25 May 2018, and will replace the current Data Protection Directive 1995 that has been enacted into legislation in individual member states, such as the Data Protection Act 1998. Brexit will not affect the UK's preparation or participation in the GDPR. The UK will still be subject to EU Law next May, and the UK Government has signalled its intention to observe it following its departure from the EU.

The GDPR is being implemented to update privacy legislation to take account of technological developments and the rise of social media. It is also being implemented to harmonise legislation throughout Europe. As a Regulation (rather than a Directive), it will be directly applicable throughout Europe and, therefore, will be the same in all member states (other than a few minor derogations). With all the upheaval of adjusting to new legislation, this point has been often overlooked: in the long term, it will make doing business both with other member states within Europe and for international companies dealing with Europe more convenient as there will only be one set of laws to navigate and manage.

Whilst previous drafts of the legislation proposed extreme measures, the final draft is generally more widely perceived as commercially balanced, and can be seen as an evolution of the current law rather than a revolution. Nonetheless, businesses will still need to plan and take remedial steps now in order to be ready for May 2018.

KNOW YOUR DATA PROTECTION DEFINITIONS

One point prone to being overlooked is that the cornerstone definitions of the current Directive and Data Protection Act 1998 generally remain unchanged under the GDPR. If you have a good understanding of the concepts of "Personal Data," "Sensitive Personal Data," "Controller," and "Processor," you can transfer those to your understanding of the GDPR.

Two things are of particular note here. First, "Sensitive Personal Data" or, rather, "special categories" of data, now includes biometric and genetic data but excludes criminal convictions data. Processing convictions will now be dealt with under Government authority, possibly the Home Office (but definitely not the Information Commissioner's Office - ICO). No official guidance has yet been given on exactly what processing criminal convictions under official authority will look like in the UK – which is concerning to organisations that have legitimate business needs to process this data.

Second, "Processors" are for the first time given legal obligations under the GDPR, alongside Controllers. As a Processor, most obligations still fall to the Controller, but it is important that businesses are aware of (a) when they are acting as a Controller and a Processor (many businesses have dual roles depending on the nature of work being carried out), and (b) what their obligations are as a Processor – both to their Controller and the data-protection authorities.

The definition of a data subject has not changed with the GDPR. But while reviewing GDPR procedures, it's worth ensuring the extent of what constitutes a data subject is properly captured. Bear in mind the GDPR makes no distinction between private and business activity, and be aware that when you are dealing with unincorporated businesses, such as sole traders or partnerships, all data will be personal data, as will data relating to directors and shareholders at incorporated companies. All contact information of individuals at companies (unincorporated or not) will be caught. It's not just members of the public that the GDPR applies to.

KNOW YOUR GROUND OF PROCESSING

One huge area of misunderstanding with the GDPR concerns its lawful grounds of processing. Generally, these have not changed from the Directive. Whatever ground of processing your business currently relies upon will most likely be the ground of processing you will rely on under the GDPR. "Legitimate business interest" – the most commonly used ground in the UK – remains present in the GDPR, and will even be extended to countries like Hungary and Spain that have so far not incorporated this concept into domestic legislation (an example of the harmonisation mentioned above). Care will need to be taken, though, to ensure you are properly executing the ground you are relying on as the GDPR places new or increased obligations here.

For example:

Processing under legitimate interest – This must be balanced against the rights and freedoms of the data subject and, when using this ground, businesses must record (internally) why they consider that their legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subjects. In addition, businesses should also specify what their own legitimate interests are (publicly).

Processing under consent – The GDPR clarifies that "affirmative consent" is required – i.e. a statement or clear affirmative action – for consent to be valid. This means silence, pre-ticked boxes or inactivity can no longer be construed as consent. A data subject ticking a box or signing a document would be sufficient as long as the relevant information is "clearly distinguishable" from other matters in the documentation (it should not be hidden in a lengthy contract).

Whatever ground of processing a business relies on will now need to be communicated clearly through its "fair processing notice" (i.e the document that communicates the information the GDPR stipulates must be provided to data subjects) sometimes known as a Privacy Notice or Privacy Policy. When drafting this, it might be tempting to take a "belt and braces approach" and try to include as many as possible in your fair processing notice. Whilst it's advisable to include all that genuinely apply, it's not advisable to claim both legitimate interest and consent.

Data Protection Authorities will dimly view businesses that ostensibly process on consent, only to claim another ground if such consent is withdrawn as this makes a mockery of the consent mechanism. Instead, be confident in your ground, understand it thoroughly, and be able to justify it if ever called upon to do so.

KNOW YOUR "HIGH-RISK" ACTIVITIES

Encryption and pseudonymisation often are topics best left to IT technical specialists. But from a general legal perspective, it should be noted that the same risk-based approach to data processing activities applies under the GDPR. Of note in the GDPR in relation to security is the obligation to carry out a privacy impact assessment to determine the level of risk of a particular activity. In practical terms, this generally means a business needs to assess all of its activities to establish which ones are high-risk, an exercise which can be very time-consuming.

KNOW WHEN TO NOTIFY OF A BREACH

For the first time, all companies processing data within the EU will be under a legal obligation to notify the local Data Protection Authority if they suffer a data breach that could result in harm to data subjects. The US is well ahead of Europe in imposing this obligation on businesses, so this is something that companies with a US presence will be better prepared for. Be aware that not all breaches require notification, and that the time frame – 72 hours – could be very difficult to achieve. It's worth reviewing your breach management procedures!

KNOW WHICH RIGHTS YOUR DATA SUBJECTS HAVE

All current data subject rights will remain in place, and most are being expanded. To manage these data subject rights, company resources should be focused on providing correct and detailed fair processing notices, streamlining subject access requests (i.e. ensuring good company procedures to ensure requests are responded to within the new 28-day deadline), ensuring efficient procedures to manage "rectify and erasure requests" as well as restrictions on processing when a subject has raised a rectification query that has not been resolved.

If you process under legitimate business interest, beware of this quirk in rights: currently, the data subject can only demand to delete their data if they provide the controller with "compelling legitimate grounds" to do so. The GDPR flips this burden and states that where a Controller processes data under the legitimate interest basis, the data subject can object at any time, and it will be for the Controller to prove a compelling legitimate grounds for processing the data. Key to the credit industry, though, are the rights surrounding profiling.

KNOW YOUR PROFILING

Profiling is a form of automated decision making that relies on personal data. Credit scoring is significant profiling. Those familiar with the current data protection restrictions around automated decision-making will be comfortable with restrictions on profiling. It is important to note that data subjects do not have the right to avoid being profiled, but they do have the right not to be subjected to a decision based on purely automated profiling.

Safeguards around profiling include:

1) Informing the data subject at the time the data is collected:
   a) That profiling will occur
   b) The logic involved in profiling (this does not mean providing intellectual property protected algorithms, but more a top-line explanation of what the algorithm may rely on)
   c) The envisaged consequences of the profiling (e.g. "a decision on your credit worthiness")
2) Implementing a process to respond to data subjects inquiring whether they have been profiled and the consequences
3) Implementing a process to have the automated decision reviewed and sense-checked by a human if requested by the data subject

4) Implementing a process to cease profiling if requested by the data subject unless there are "compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject." Bearing in mind the crucial nature of credit profiling to the lending market, most applicable businesses should seek to fully leverage this exception
5) Carrying out a privacy impact assessment for all profiling activities – these are generally "high-risk" activities
6) Ensuring safeguards such as proper mathematical or statistical procedures (i.e. robust algorithms), or random sampling of results to support the veracity of the profiling
7) Ensuring technical and organisational measures to correct data inaccuracies and avoid errors (proactive sampling would be preferable to waiting for complaints)
8) Minimising the risks of discriminating against individuals based on their sensitive personal data

KNOW YOUR INTERNATIONAL DATA TRANSFERS

The GDPR will do little to make transfers out of the EU any less complex than they are today. However, companies with subsidiaries inside and outside of the EU should note the inclusion of Binding Corporate Rules (BCRs) in the GDPR. BCRs are a mechanism for intra-company transfers around the world – and for the first time are being given a legislative basis. Bearing in mind the current threats to other mechanisms such as standard contractual clauses and the Privacy Shield, BCRs will be an attractive option to many companies after May 2018.

dun & bradstreet

CICM Chartered Institute of Credit Management

dnb.co.uk