THE FUTURE OF DATA PROTECTION

An extract from Perspective:
The understanding your customer issue
Essential insights into the issues facing your industry today
Trevor Parker, Chief Compliance Officer at Equifax, discusses the changes that will result from the new General Data Protection Regulation and what they may mean for both businesses and consumers.

As most readers will already be aware, the General Data Protection Regulation (GDPR) will represent a new legal framework for data in the EU. Whilst there are similarities with the existing UK Data Protection Act 1998 (DPA), some of the requirements are different.

The result of the 23rd June 2016 referendum on membership of the EU is unlikely to hold up progress. Recently¹ the Information Commissioner’s Office (ICO) said:

“It is extremely likely that GDPR will be live before the UK leaves the European Union. Remember that the GDPR is actually already in force, it is just that Member States are not obligated to apply it until 25th May 2018.”

“We (the ICO & the UK Government) believe that future data protection legislation, post Brexit, should be developed on an evolutionary basis, to provide a degree of stability and clear regulatory messages for data controllers and the public.”

Therefore, notwithstanding Brexit, it’s worth paying close attention to the GDPR now. This is because the new regulations will be relevant for those UK organisations operating internationally. International consistency around data protection laws and rights is crucial both to businesses and organisations operating across borders, as well as to consumers and citizens within the EU.

The UK ICO has a good record of working closely with regulators in other countries, and we expect that will continue. The ICO’s view is that reform of UK data protection law remains necessary and UK businesses would do well to understand GDPR. We expect that the substantive elements are likely to apply in the UK from 2018 onwards.

Like the Data Protection Act (DPA), the GDPR applies to personal data. Under GDPR, the precise definition of personal data has changed, so that personal data now includes data such as online identifiers (an IP address, for example). In this respect, GDPR brings the law up to date and recognises that organisations use technology to collect a broad range of data about individuals.

The rules are changing at a fascinating time for data. There is undoubtedly a trend towards greater understanding by individuals that data about them exists and that it can be used, possibly in ways with which they disagree. Actions like those brought by Max Schrems² against Facebook could well become more common. Media stakeholders were quick to report on it and it tapped into a rich seam of consumer interest. GDPR recognises that the world we operate in now is somewhat more familiar with technology (and the data trails that each of us leave behind) than the one that existed when the DPA came into being.

Current data protection arrangements require businesses to understand whether they are controllers or processors, and these terms remain in the new world. Essentially, a controller says how and why data is processed, and the processor acts on the controller’s behalf. In the future, what is expected of each party will become more onerous. For example, controllers must ensure their contracts with processors comply with the GDPR.

The GDPR contains principles that broadly align with those we are familiar with from the DPA. Personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

READ MORE...
The future of data protection

Turning to credit referencing and in particular to credit data sharing, the current premise for the lawful sharing and use of credit data is recognised as being under the ‘legitimate interests’ condition for processing personal data. GDPR brings a new right for an individual to request that the data controller cease automated decision-making and profiling (e.g. credit risk scoring) when processing under this condition. Credit granters will need to consider the practical implications of this and may wish to seek a more certain way to safeguard their operations.

The need for transparency is a central theme which runs throughout the GDPR. This raises another important matter linked to credit data-sharing: the need for clear and explicit privacy notices to accurately reflect how data will be shared with, and used by, credit referencing agencies (CRAs). Equifax believe this is best achieved through the agreed use of a standard privacy notice wording across the credit data-sharing industry that relates to credit referencing. We are currently engaged in discussions with key industry stakeholders and we would encourage all credit data sharers to work with their trade associations on this matter.

This article just skims the surface of the proposed changes. The result of the EU referendum and the scope for local regulators to interpret certain aspects of the new regulations means organisations need to read the ICO’s guidance and get the ball moving.

If they have not already done so, data controllers and processors should take the opportunity to read the ICO’s guidance about GDPR, understand the impact on their organisation and get their GDPR project underway.

1. 29th September 2016.
2. An Austrian lawyer and data activist.

EQUIFAX

Idea in brief

THE SITUATION
General Data Protection Regulation (GDPR) will represent a new legal framework for data in the EU and is due in May 2018.

THE CHALLENGE
The result of the EU referendum and the scope for local regulators to interpret certain aspects of the new regulations means organisations need to read the ICO’s guidance and get the ball moving.

THE TAKE AWAY
The implementation of GDPR is unlikely to be straightforward...and organisations need to get their GDPR project underway for it to be ready in time.

If they have not already done so, data controllers and processors should take the opportunity to read the ICO’s guidance about GDPR, understand the impact on their organisation and get their GDPR project underway.

1. 29th September 2016.
2. An Austrian lawyer and data activist.

CLICK HERE FOR MORE ARTICLES