EU General Data Protection Regulation: things you should know

Eduardo Ustaran, Partner, Hogan Lovells International LLP, ***highlights the significant changes being brought in under the newly agreed Data Protection Regulation***

To say that the newly agreed EU General Data Protection Regulation ('GDPR') will change the existing data protection framework in Europe is an understatement. After an intense legislative process of more than 4 years, the all-powerful trio comprising the European Parliament, the Council of the EU and the European Commission have created an ambitious, complex and strict law that is set to transform the way in which personal information is collected, shared and used globally.

Those who are used to the regime originally established by the 1995 Data Protection Directive (95/46/EC) may recognise some familiar concepts and principles, but despite the similarities, the effect of the GDPR will be far greater than that of the Directive. In other words, the GDPR aims to take data protection compliance to a new level. Therefore, it is essential that we start to appreciate what is significant about the GDPR.

Geographical applicability

One very carefully thought-out aspect of the GDPR is its geographical applicability — both within and outside the EU. For starters, the GDPR will be directly applicable across all Member States of the EU without any further intervention from the national parliaments.

One of the main flaws of the original Directive was that it had to be implemented by national legislation in order to become law. That led to a patchwork of obligations that were not identical across the EU and caused a lack of harmonisation. An effective move to address this problem was to change the format of the law altogether and adopt a single and all-encompassing regulation. Therefore, on paper at least, having a single law will provide much needed consistency, although it will still be interpreted in accordance with national approaches and idiosyncrasies.

In terms of the GDPR's applicability beyond Europe, the legislators decided to do away with the old-fashioned references to EU-based data processing 'equipment'. Instead, the applicability of the GDPR to organisations without an establishment in the EU will be determined by the location of the data subjects. To this effect, the GDPR will apply whenever the use of personal data by an organisation relates to:

- the offering of goods or services to individuals in the EU, irrespective of whether a payment is required; or
- the monitoring of those individuals' behaviour in the EU.

In this respect, the GDPR clarifies that tracking individuals on the internet to analyse or predict their personal preferences — as many websites and apps do — will trigger the application of EU law. This measure makes almost every website that drops tracking cookies, or app that retrieves usage information subject to the GDPR.

Putting people in control

Something important to understand at the outset is the overall aim underpinning the GDPR: Putting people in control of their data. This is a theme that is present throughout the text and is emphasised by the strengthening of 'consent' in relation to the use of data.

When relied upon as a justification for the use of data, consent will need to meet very high standards and overcome certain conditions including:

- consent cannot be bundled with T&Cs without clearly distinguishing between the uses of personal data and the other matters governed by the T&Cs;
- consent can be withdrawn at any time and in an easy way that should be explained to the individuals before it is obtained; and
- if consent is presented as 'take it or leave it', it will not be regarded as freely given.

In the end and after some last minute controversy, the requirement for parental consent for the use of personal information of under-16 year olds will be at the discretion of Member States. This is bound to result in a lack of harmonisation and the need for a country-by-country approach to compliance when teenagers' data are involved.

(Continued on page 4)

(Continued from page 3)

Individuals' control over their data will be even more visible through significantly reinforced rights, including:

- information to be provided to individuals at the point of data collection or within a reasonable period afterwards;
- right of access for the data subject;
- right to rectification;
- right to erasure (also known as 'right to be forgotten');
- right to restriction of processing;
- right to data portability;
- right to object to the processing altogether; and
- right not to be subject to a decision based solely on automated processing.

Transparency, erasure and portability in particular are likely to emerge as crucial tools for individuals to use in the face of an ever growing hunger for our digital data. The legislators have worked hard to make these rights more meaningful than ever before, so a greater uptake than until now should be expected.

The big novelty: accountability obligations

From a practical perspective, one of the most notable novelties of the GDPR is the various requirements to make businesses more accountable for their data practices. Brand new responsibilities include:

- implementation of data protection policies;
- data protection by design and data protection by default;
- record keeping obligations by controllers and processors;
- co-operation with supervisory authorities by controllers and processors;
- data protection impact assessments;
- prior consultation with data protection authorities in high-risk cases;
- mandatory Data Protection Officers for controllers and processors for the public sector and Big Data processing activities.

On the data security front, highlights include:

- extremely detailed requirements for controllers to impose contractually onto vendors acting as processors. From a day-to-day compliance perspective, this will be one of the toughest challenges, particularly when engaging cloud services or any of the off-the-shelf solutions on which business rely to communicate and store data; and
- data breach notification to data protection authorities within 72 hours of spotting an incident. This obligation does not apply if there is no risk for individuals, but if the risk is high, controllers and processors will need to notify the individuals as well.

"Crucially, the GDPR does not limit its accountability obligations to controllers. Many of these new requirements apply equally to processors. This is a major practical difference between the GDPR and the Directive, which highlights the new focus on compliance across all roles of the information life-cycle."

Crucially, the GDPR does not limit its accountability obligations to controllers. Many of these new requirements apply equally to processors. This is a major practical difference between the GDPR and the Directive, which highlights the new focus on compliance across all roles of the information life-cycle.

Still restrictions on international data transfers

As counter-intuitive as it may seem to regulate cross-border data flows in the 21st century, the GDPR carries on with the traditional approach to restrict data transfers to non-EU jurisdictions.

Aside from transfers to jurisdictions that are officially declared by the European Commission as adequate, both controllers and processors may only transfer personal data outside the EU if they put in place appropriate safeguards and on condition that enforceable rights and effective legal remedies for individuals are available.

The GDPR has helpfully expanded the range of measures that may be used to legitimise such transfers, which now include:

- Binding Corporate Rules (BCRs);
- standard contractual clauses ('SCCs') adopted by the European Commission;
- standard contractual clauses adopted by a data protection authority and approved by the European Commission;
- an approved code of conduct;
- an approved certification mechanism; and
- other contractual clauses authorised by a data protection authority in accordance with the so-called 'consistency mechanism'.

Some of these methods, such as standard contractual clauses, have been tested over the years, so their benefits and limitations are well known. Others will need some time to show their value and effectiveness.

For example, ad-hoc contractual clauses may become a more realistic solution than SCCs, but they are likely to require a greater amount of effort in terms of drafting and interaction with regulators.

What is patently clear is the growing support for BCRs by lawmakers and

regulators; but BCRs should be seen as a framework for global privacy compliance rather than a simple mechanism to overcome transfers restrictions.

To comply or not to comply

When faced with such a complex and strict framework, an inevitable question always is: what is the risk of non-compliance? This question seems to acknowledge the fact that 100% compliance is unachievable and that getting things right is going to involve a degree of prioritisation.

Corporate cultures and risk-tolerance will play an important role in deciding the level of investment that will be devoted to meeting the requirements of the GDPR, but something that must be taken into account is the potential consequences of non-compliance. These include the right to compensation for breaches for material or immaterial damage, and administrative fines which are well above what has been at the disposal of regulators until now.

In terms of prioritisation, it may be useful to remind ourselves of the types of breaches that may attract the maximum level of fines under the GDPR — up to 20 million euro or up to 4% of total worldwide annual turnover, whichever is higher. These include infringements of the following provisions:

- the basic principles for processing, including conditions for consent;
- the data subjects' rights;
- the conditions for lawful international data transfers;
- specific obligations under national laws, where permitted by the GDPR; and
- orders by data protection authorities, including suspension of data flows.

The next two years will be critical to prepare for compliance with what promises to be a game-changing piece of legislation. Whatever its imperfections, the GDPR is here to stay and the time for action is now.

Eduardo Ustaran
Hogan Lovells
eduardo.ustaran@hoganlovells.com