MARSH

May 2016

ADVISER

NEW DATA PROTECTION LAW IN EUROPE 2016

We now have a new data protection law in Europe. It has taken more than four years from the publication of the first draft of the Regulation in January 2012, but after some painstaking work by European Union (EU) bodies that had to consider an unprecedented 4,000+ comments and submissions by national supervisory authorities and other stakeholders, it has now been made law.

On 4 May 2016, the General Data Protection Regulation (GDPR) was published in the Official Journal of the European Union and will enter into force 20 days after publication. However, there is a two-year implementation period before the Regulation becomes directly applicable in Member States.

This two-year implementation period allows both Member States' supervisory authorities and the entities that will be subject to the GDPR time to prepare their organisations for the changes in practice that the Regulation will require. For those organisations that have not been following the path of this Regulation too closely, the sooner you assess the implications of the Regulation for your business and implement the required changes, the better. As noted in the following text, the penalties for non-compliance can be severe and it is therefore important that compliance can be demonstrated well in advance of the end of the implementation period.

In this *Adviser* we aim to set out some of the key provisions of the Regulation that will feed the exposure profile of captured entities and outline the implications for corporate insurance arrangements.

WHY DO WE NEED A NEW REGULATION?

The obvious response to this question is to point to the significant evolution in technology that has changed the way in which data is collected and used since the EU Data Protection Directive 95/46/EC (Directive) (implemented in the UK by the Data Protection Act 1998) was adopted in 1995. To provide some context, 1995 was the year that Amazon was launched, but still predates Facebook and Google.

The Regulation text acknowledges that the dramatic increase in data collection and sharing enabled by technological developments means that both public and private entities are able to make use of personal data on an unprecedented scale. The impetus for the European Commission's proposals to update and modernise the Directive was twofold. First, to empower individuals by guaranteeing the right to the protection of personal data that was recognised by Article 8 (1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union. Secondly, to help build trust in the online environment, which plays a central role in the wider plans to create a Digital Single Market.

HOW DID WE GET HERE?

January 2012 –
EC Vice-President publishes the first draft Regulation.

July 2012 –
EU Parliament working document published by the LIBE Committee.

March 2014 –
Following negotiations, the European Parliament votes on a compromise text.

June 2015 –
The European Council releases its general approach followed by the first trilogue meeting between the three EU institutions.

July 2015 –
Second trilogue meeting.

17 December 2015 –
The EU Parliament's LIBE Committee approve the politically agreed text.

4 May 2016 –
Publication of the Regulation in the Official Journal of the European Union.

25 May 2018 –
Regulation becomes directly applicable in EU Member States.

KEY POINTS

- Fines for the most serious breaches to increase to the greater of EUR20 million or 4% of total worldwide annual turnover.
- Extra-territorial scope.
- Requirement for data controllers to demonstrate that consent was given and requirement for there to be "clear affirmative action".
- Explicit consent required to collect sensitive data.
- Direct obligations on data processors.
- New restrictions on the profiling of data subjects.
- Requirement for organisations to be able to demonstrate and verify compliance.
- Requirement to appoint a data protection officer for public bodies or where processing operations require regular and systematic monitoring of data subjects or where they are processing on a large scale special categories of data.
- Data privacy impact assessments are required for certain new or changed products and services.
- Organisations are required to notify a data breach to the supervisory authority "without undue delay and, where feasible, not later than 72 hours" unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons".
- Organisations are required to notify a data breach to data subjects "without undue delay" when the data breach is "likely to result in a high risk to the rights and freedoms of natural persons".
- New and enhanced rights for data subjects, including the right to erasure and enhanced subject access rights.

WHO DOES THE REGULATION APPLY TO?

Unlike the existing data protection law, the new Regulation will not only apply to companies that are established and/or process data in the EU, the Regulation will also apply directly "to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

It is important to understand where your "main establishment" is considered to be under the Regulation, as this will govern which Member State's supervisory authority will take the role of lead supervisory authority in the event of any complaint and any associated enforcement action.

The "main establishment" is not necessarily the corporate HQ, as the Regulation defines this to be "where the decisions on the purposes and means of the processing of personal data are taken".

For data processors, the change is even starker, as they are now captured directly by this new Regulation. Rather than having their duties defined solely under a contract with the data controller, the Regulation introduces direct obligations on data processors. As a result, supervisory authorities will now be able to enforce the terms of the Regulation directly against processors. The "main establishment" of the processor will be deemed to be "the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union". If their processing activities extend beyond the instructions of the controller, then they may also be deemed a joint controller under the Regulation.

KEY CHANGES

FINES

The biggest headline will undoubtedly be the dramatic increase in the size of the fine that can be levied against an offending entity or individual. Currently in the UK, it is set at a maximum of GBP500,000 but it will now be repositioned to EUR20 million or 4% of worldwide annual turnover, whichever is the greater. Looking beyond the stated monetary cap, the more concerning amendment for many organisations will be the percentage figure, the fact that it is based on turnover and not profit, and the fact that it is based on worldwide turnover rather than the turnover of the entity in the EU country or countries where the offence occurred. For any global organisation with activities inside the EU that are captured by the Regulation, this will be of particular concern.

TERRITORY

As discussed in the preceding paragraphs, many organisations that were not previously subject to EU data protection law will now find that they are captured by the new Regulation. These organisations will need to ensure that their business practices as regards personal data reflect the requirements of the EU as well as any additional territorial regulation that they had been working to.

CONSENT

The Regulation will impose some stricter obligations on organisations where processing is based on consent, making it far harder to obtain. The new Regulation requires data controllers to demonstrate that consent was given and requires there to be "clear affirmative action". Silence, pre-ticked boxes, or inactivity will not constitute consent. In addition, where controllers rely on consent for the processing of sensitive data, the Regulation requires consent to be "explicit".

PROFILING

Always a highly contentious area of data protection practice, the Regulation will introduce new restrictions aimed at targeted advertising based on data subject profiling. Specifically, the Regulation prohibits organisations from taking decisions "based solely on automated processing, including profiling, which produces legal effects concerning [a data subject] or similarly significantly affects [a data subject]".

PRIVACY FUNCTION

Going forward, there will be no requirement to register data collection and processing activities with supervisory authorities, or lodge any statements (as required by certain Member States' supervisory authorities) as to the nature of processing activities. However, the Regulation does set the requirement for detailed records of data collection and processing activities to be kept internally that will likely go beyond that information currently submitted to supervisory authorities. Controllers will not just have to comply with the law, but be able to demonstrate and verify compliance through implementation of "appropriate technical and organisational measures".

DATA PROTECTION OFFICER

Where the processing is carried out by a public body or where "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope, and/or their purposes, require regular and systematic monitoring of data subjects on a large scale, or the core activities of the controller or the processor consist of processing on a large scale of special categories of data", there will be an additional requirement to appoint a Data Protection Officer, and the Regulation lays down certain requirements as to who that can be and the nature of the role.

PRIVACY BY DESIGN

The Regulation will embed privacy considerations in the design phase of any new product or service that touches personal data or technology that processes it. To ensure this happens, there is now a specific requirement (previously recommended by certain Member States' supervisory authorities) for organisations to undertake data privacy impact assessments in the event that the relevant processing operation is "likely to result in high risk to the rights and freedoms of natural persons".

BREACH REPORTING

The Directive contains no specific requirement to notify either the relevant supervisory authority or affected data subjects of a data breach, though a patchwork of national laws and guidance papers had begun to emerge to plug this gap. Now, under the Regulation, all organisations will be required to notify a personal data breach to the supervisory authority "without undue delay and, where feasible not later than 72 hours after having become aware of it", unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons". Organisations will also be required to notify personal data breaches to data subjects when the breach is "likely to result in a high risk to the rights and freedoms of natural persons". These stiff new reporting requirements bring the EU far more in line with the US environment, where the notification of data breaches has been the norm for many years. An exemption from notifying data subjects exists where data is "unintelligible", for example, as a result of encryption.

ENHANCED RIGHTS

Data subjects will have certain rights enhanced in the new Regulation that will create certain operational challenges for organisations in order to comply. Those rights include enhanced subject access rights and, the more widely discussed, right to erasure (commonly referred to as "the right to be forgotten"), which previously existed under law in relation to deletion of data, but has been expanded, in particular, following the decision by the Court of Justice of the European Union (CJEU) in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)*.

INSURANCE IMPLICATIONS

This new set of data protection obligations introduces certain additional obligations, sanctions, and breach response requirements that have the potential to dramatically alter the financial impact of an instance of non-compliance. These financial consequences are likely to see an upwards shift in the loss estimates attached to any data protection items in the company's risk register, potentially breaching acceptable risk tolerances. This adjustment is likely to lead to a re-examination of the adequacy of insurance arrangements. Organisations will need to understand the effectiveness of the coverage bought, the sufficiency of any applicable indemnity limits, as well as the availability of enhanced insurance protection if existing arrangements fall short of requirements. In particular, organisations may wish to consider their insurance protection related to the following:

- The ability under the Regulation for complainants to seek a judicial remedy of a supervisory authority's decision not to pursue a complaint and/or the right of the data subject(s) to seek compensation for the breach as part of a group action. This may lead to a higher number of litigation cases from data subjects and more aggressive enforcement by supervisory authorities who are reluctant to see their decisions challenged.

- The maximum level of fine is due to increase to the greater of EUR20 million or 4% of worldwide turnover for the entire organisation and not just the offending entity. This will significantly add to the potential financial downside for more serious breaches of the Regulation. Not only should organisations consider the higher level of fine, but due to the amounts involved, there is the potential for a more protracted and costly legal process as organisations are likely to explore all potential avenues of challenge against the supervisory authority's decisions.

- The new requirement to notify data subjects without undue delay when a data breach is "likely to result in a high risk (to) the rights and freedoms of individuals" will result in significant expenditure for organisations to implement and manage the practical steps of this requirement where high volumes of personal data are involved.

- The potential for high public awareness of data breaches with associated press attention driven by the new notification requirements should cause organisations to consider any short-term trading impact due to diminished reputation and customer trust. Organisations may also wish to consider the cost of implementing any reputational mitigation strategy.

These changes are set to bring the exposure profile of European organisations more in line with US firms which have had to deal with breach notification obligations and associated privacy litigation for more than a decade. The US experience provides a useful reference point for analysis of the potential cost of EU data breaches in the future, particularly the cost of delivering the crisis management response. For any organisation concerned with the status of their existing insurance arrangements, the following questions should be addressed:

- Does the insurance programme deliver adequate protection for a breach of privacy law and regulation?

- Does the insurance programme deliver adequate protection for the cost of delivering against GDPR breach notification obligations?

- Does the insurance programme deliver adequate protection for group action litigation by affected data subjects?

- Does the insurance programme deliver adequate protection for the costs connected to an investigation by a supervisory authority?

- Does the insurance programme deliver adequate protection for legally insurable fines imposed by a data protection supervisory authority?

HOW CAN MARSH HELP

Marsh is an industry leader in delivering exposure analysis and insurance solutions. Our Global Cyber Practice is able to use the experience of our colleagues across the world to deliver advice and insurance products that will fit the needs of both single-location and multinational organisations.

Our capabilities span the risk advisory and insurance placement space. Specifically, we can assist with:

- Using risk identification and exposure modelling of data and technology-related risks to create a unique profile for the organisation.

- Completing an insurability assessment to identify the effectiveness of existing coverage arrangements against the risk profile and deliver recommendations for future treatment.

- Defining the optimal insurance solution utilising the additional capabilities of the insurance market to deliver specific cover against privacy and technology-related exposures.

For additional information, please refer to your Marsh representative or explore our "Research and Briefings" on this and other related cyber risk topics on marsh.com.

CONTACT

DAVID ARNOLD
Senior Vice President
FINPRO Practice
+44 (0)20 7357 1759
david.arnold@marsh.com