Cybersecurity, Data Privacy & Information Management Alert

Weil

December 6, 2018

The GDPR is here – what now?

By Barry Fishley and Briony Pollard

In the run-up to the introduction of the General Data Protection Regulation ("**GDPR**") many organisations rushed to prepare for the regulatory changes. According to Deloitte's 2017 GDPR survey, 89% of organisations surveyed had a formal readiness programme. However, only 15% expected to be fully compliant by 25 May 2018. Organisations faced a range of challenges including data mapping difficulties, how to promote a positive culture of data protection compliance and how to balance the interests of the organisation with the interests of users or consumers.

We consider what has happened since the GDPR's implementation and identify some challenges organisations face under the new data protection regime.

What has happened since the introduction of the GDPR?

Rise in complaints

Since the introduction of the GDPR there has been a sharp increase in the number of complaints to data protection regulators across Europe. The French data protection regulator, the Commission Nationale de l'Informatique et des Libertés ("**CNIL**"), reported a 64% increase in the number of complaints in the four months after the GDPR came into effect, compared with the same period last year. The UK Information Commissioner's Office ("**ICO**") and the Irish Data Protection Commission have also reported increases in complaints of 160% and 76% respectively over the past year. The data protection authorities of other European Member States have received similarly inflated numbers of complaints in recent months, which reflects the widespread public interest in the new data protection rules.

First challenges

Within 48 minutes of the GDPR coming into force, None Of Your Business, Max Schrems' non-profit organisation, launched the first challenge under the GDPR. In four separate filings, Schrems challenged some of the largest technology, social media and networking service providers for obliging users to give "forced consent" as a condition to use their services. On 28 May, La Quadrature du Net, a French digital rights group, filed several complaints against a number of US-based technology companies. Other campaign groups, Privacy International and the Center for Digital Democracy, are also planning action.

Organisations have also reported an increase in questions and requests from data subjects. Technology companies, media groups, retailers and banks are obvious targets due to the vast amount of information they hold

about customers. Reportedly, many have failed to respond to such requests within a month of receipt, as required under the GDPR. However, the Data Protection Officer of a global social media and networking company stated that the post-GDPR spike in requests has already started to decline. It may be that the public scrutiny of data protection issues triggered by the new legislation will abate and provide organisations with some respite from the administration involved in compliance with the data subject access obligations.

First breaches

On 13 June 2018, Dixons Carphone admitted that it had suffered a data breach, which occurred prior to the implementation of the GDPR. This raises the question of whether such incidents would be dealt with under the previous, or the new, data protection regime. In April, a European Commission official stated that data breaches that had occurred before 25 May, but that had been kept silent until after that date, would be liable for sanctions under the GDPR. The ICO appears to be aligned with this approach, and has stated, in response to the Dixons Carphone incident that it "will look at when the incident happened and when it was discovered as part of [its] work and this will inform whether it is dealt with under the 1998 of 2018 Data Protection Acts". The European Commission official added that a retrospective adoption of the GDPR would be necessary "if this behaviour [of keeping a data breach secret]…continue[s]". Data breaches are often discovered long after they have occurred. Ponemon Institute's 2017 Cost of Data Breach Study found that it takes UK organisations an average of 191 days to identify a breach and 66 days to contain it. The result is that more pre-GDPR breaches may yet come to light.

The first major UK data breach since the implementation of the GDPR was announced on 27 June 2018. Ticketmaster admitted that data relating to 40,000 UK customers had been compromised between February and June 2018. The incident is subject to an ICO investigation. Any enforcement action against Ticketmaster will likely set the tone for the ICO's future approach. In an effort to allay fears of the new pecuniary penalties that can be imposed under the GDPR, which can reach Euro 20 million or 4% of worldwide turnover (whichever is higher), the ICO emphasised earlier this year that it intends to use its powers "proportionately and judiciously". The investigatory process is lengthy, so we may have to wait some time for the results of the Ticketmaster and Dixons Carphone investigations, and to see the extent to which the ICO chooses to exercise its new powers.

Areas of difficulty

The GDPR provides for stronger data subject rights than under the previous regime, including in respect to the right to erasure (or the so-called "right to be forgotten"). This will likely lead to difficulties with back-up data. Holding back-up data is considered processing, and therefore falls under the scope of the GDPR. The GDPR stipulates that personal data may be kept only for as long as necessary for the purposes for which the personal data are processed. In practice, many organisations do not or cannot delete back-up data, for operational or technological reasons. For example, some back-up systems do not allow for control of the content or format of the data, which makes it very difficult to identify, locate and erase particular data. A possible solution is for organisations to anonymise or pseudonymise back-up data; if individuals cannot be identified from the data, the GDPR will not apply. However, the principles of data protection will apply to data that has been pseudonymised where use of additional information could result in the identification of a natural person. The French regulator, the CNIL, has stated that organisations do not have to delete back-ups when complying with the right to erasure, so long as it is clearly explained to the data subject that back-up data will be kept for a specified length of time (as outlined in the organisation's data retention policy). The ICO has stated that in addition to providing clear information on data retention to data subjects, organisations will have to take steps to ensure erasure of personal data from backup systems. The action required however, will depend on the technical mechanisms available and other circumstances particular to the organisation. The ICO stated that in most cases, organisations may retain personal data in a backup provided the backup data is simply held and is not accessed.

Another grey area in relation to the right to erasure is suppression lists. If an organisation maintains a suppression list, which includes data relating to an

individual who has made a request 'to be forgotten', then the organisation may be not compliant with the data subject's rights under the GDPR. However, if the organisation deletes the individual's personal data from a suppression list, and acquires a marketing list which includes the same individual's personal data, the organisation will have no way of knowing that that individual previously made a successful erasure request. If the organisation then contacts the individual, it will be technically non-compliant with the GDPR. Either course of action may potentially frustrate an organisation's ability to be compliant with data protection laws. This will remain a balancing exercise for organisations until greater clarity is provided.

What to expect

Case law developments

In a landmark ruling, *Various Claimants v WM Morrisons Supermarket Plc* (2017), a group action brought by employees, Morrisons was held vicariously liable for a data breach carried out by a rogue employee, out of working hours and at home on a personal computer. The judgment has significant implications for data controllers and processors, as Morrisons was vicariously liable for the acts of its employee despite having discharged its own obligations under the Data Protection Act 1998 and common law. The Morrisons ruling, together with the ruling in *Google v Vidal-Hall* (2015) in which it was held that claimants in data protection cases need not have suffered a material loss to claim compensation, are likely to alter the data protection litigation landscape. The lower threshold required to bring a data protection case, combined with the greater potential to recover damages from employers and the reinforcement of data subject rights under the GDPR, means we are likely to see a rise in data protection cases being brought.

The Court of Appeal recently upheld the Morrisons ruling, but importantly, did not determine whether organisations could be vicariously liable for fines arising as a result of acts of their employees under the Data Protection Act 1998, and by extension, the GDPR and Data Protection Act 2018. Morrisons have stated that it plans to appeal to the Supreme Court, but like the Court of Appeal judgment, a Supreme Court judgment is unlikely to clarify whether organisations can be vicarious liability for fines arising as a result of their employees under the GDPR.

Regulatory guidance

In the run-up to the GDPR, the ICO emphasised that it had no intention of making early examples by levying large fines against breaching organisations, and stated that it would continue its moderate approach to enforcement. The Commissioner specified that the ICO would focus on organisations that deliberately, persistently or negligently misuse personal data. Since the implementation of the GDPR, the ICO has provided little further commentary on enforcement under the new regime, and the eight monetary penalties issued since 25 May have been for breaches under the old legislation. Time, and the outcomes of the Ticketmaster and Dixon Carphone investigations, will reveal how the new regime will affect organisations in practice.

The ICO has published a Guide to Data Protection, which covers the GDPR and Data Protection Act 2018. The European Data Protection Board (formerly the Article 29 Working Party) has recently published guidelines on consent, certification procedures and transfers of data outside the European Union, and is due to publish further guidance on the GDPR.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any member of the Cybersecurity, Data Privacy & Information Management Group.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
Briony Pollard	View Bio	briony.pollard@weil.com	+44 20 7903 1372