The Journey to GDPR: Compliance Did Not End on 25 May

By Aaron Simpson, James Henderson and Olivia Lee, Hunton Andrews Kurth

Aaron P. Simpson, Partner
Email: asimpson@HuntonAK.com
London: +44 (0) 20 7220 5612
New York: +1 212 309 1126

The General Data Protection Regulation (GDPR) has now been in force for two months, and anyone who expected the dust to settle before summer will be sorely disappointed. In the months leading up to the GDPR's implementation, 42-46% of businesses surveyed by the Ponemon Institute and SAS Institute anticipated that they would be fully compliant by the 25th May deadline. This was optimistic - a further survey conducted by TrustArc one month following 25th May found that only 20% of businesses had achieved full compliance, by their own estimations.

Some companies now seem to be coming to terms with more realistic compliance projections. According to TrustArc, 76% of businesses now have their sights set on the end of 2018 as a deadline for full compliance. If there is to be reasonable hope of fulfilling these expectations, we will likely need further guidance from EU and national regulators to illuminate some of the murkier corners of the GDPR that remain pertaining to the extra-territorial scope of the law, data transfers and issues related to dropping cookies in the website context.

Even the most basic question of applicability of the GDPR under Article 3 can prove troublesome, and many organizations, especially those non-European companies operating websites accessible from the EU, are still unsure as to whether their compliance is expected. A literal reading of the GDPR, coupled with an orthodox approach, could potentially result in the vast majority of the world's online businesses falling within scope. But, from a pragmatic perspective, do we expect regulators to require compliance from companies simply because their websites happen to be accessible to individuals in the EU? Some businesses clearly feel as though there is at least a risk of this, and have taken the extreme approach of blocking access entirely from devices located in the EU. A more pragmatic interpretation would require that there be some kind of intention on the part of the organization in question to target those in the EU – both through the offering of goods or services and with regards to "monitoring" – before a website could be considered to fall within scope.

A related concern pertains to the same extraterritorial application of the law. Now that businesses that are not established in the EU can be subject directly to the GDPR as a result of their processing of personal data in the EU, how are data transfers to be considered? In these circumstances, has an actual "transfer" occurred if there is no controller entity established in the EU that can be considered to have made such a transfer? If such data collection is considered a

transfer of personal data, non-EU businesses that are subject to the GDPR face practical hurdles to compliance, and questions regarding the relevance of data transfer mechanisms in the context of a business whose data processing is directly subject to the GDPR.

In relation to cookies, the myriad of divergent responses to the heightened consent requirements that now apply under the e-Privacy Directive will not have escaped notice. Some organizations have seemingly turned a blind eye, producing no cookie consent mechanism on their website, while others have opted to stick with the pre-25th May status quo, using an informative cookie banner but assuming consent rather than requiring a specific opt-in. Others still have taken a more conservative approach, going so far as describing every cookie being dropped on their website and obtaining specific opt-in consent.

Vendor management has proven to be another challenging area of compliance. There is some predictability to this – these issues require a consensus between parties as to controllership, and we are seeing many organizations having to push back against parties characterizing themselves as a data controller or a processor, when these characterizations do not correspond with the way in which they are using the personal data in question. It has proven particularly difficult to obtain efficient execution of Article 28 agreements, and we would expect many such agreements to require signature for the foreseeable future.

There has also been inconsistency in the practical implementation of the GDPR across Member States. For instance, some Member States' regulators have already produced their own lists of factors that trigger a data protection impact assessment (DPIA), but variable terminology and even inconsistent criteria is likely to leave those operating in multiple jurisdictions unsure of whether a DPIA is necessary in relation to their processing. Poland's Data Protection Authority, for example, has included international data transfers outside the European Union on their list of DPIA criteria, despite the fact that this was removed from the final version of the Article 29 Working Party's guidance on DPIAs under the GDPR.

And keeping supervisory authorities onside should be a priority given the potential consequences of non-compliance. The Information Commissioner's Office in the UK has already made something of an example of Facebook, announcing this month that it intends to fine the company £500,000 for its part in the Cambridge Analytica scandal, which is the maximum fine available under the old UK Data Protection Act which was applicable to this alleged behavior. The European Data Protection Board (formerly the Article 29 Working Party) has been equally unsympathetic with US firm ICANN in its attempts to extract personal data from German domain registrar EPAG.

It is still too early to predict how severe supervisory authorities will be in their enforcement, particularly whether or not they will take pity on companies still struggling to find their feet in this new legal landscape, but the fact that the ICO intends to fine Facebook the maximum amount possible under the old regime sends a signal that regulators will be willing to flex their significantly expanded muscles given the opportunity and incentive.

It will not only be regulators causing concern for businesses - data subjects also have been quick to make use of their rights. Some companies have reported receiving as many requests to exercise data subject rights in two weeks as they previously received in a year, no doubt partially attributable to the mainstream media coverage that the GDPR received compared to preceding legislation.

We would hope to see some guidance on these topics in the coming months. Given that the e-Privacy Regulation remains in draft form, it will likely be some time before there is anything definitive on the cookie front, and it may be enforcement actions from which we learn the most. What is clear is that the journey to compliance did not end on 25th May, and if we are being realistic, it is likely that the end is not even yet in sight. **LM**

About Aaron Simpson
Aaron Simpson is the Managing Partner of Hunton Andrews Kurth's London office and advises clients on a broad range of complex privacy, data protection and cybersecurity matters, including international and US federal and state privacy and data security requirements. As a leader on the firm's privacy team, Aaron's work ranges from advising clients on large-scale cybersecurity incidents to the development of cross-border data transfer solutions, compliance with existing and emerging data protection requirements in Europe, and negotiating data-driven commercial agreements. James Henderson and Olivia Lee are associates in the Hunton Andrews Kurth global technology, outsourcing and privacy team.