Client Alert: GDPR One Year On

Date : May 23, 2019

https://youtu.be/D3i9Lm9n_bc

Introduction

This weekend sees the first anniversary of the coming into force of the General Data Protection Regulation (GDPR) and indeed the UK Data Protection Act 2018 (DPA 2018). You can find out more about GDPR in our FAQs here www.bit.ly/gdprfaq and more about DPA 2018 in our alert here: http://www.corderycompliance.com/client-alert-data-protection-act-2018/

Has GDPR been used?

The first thing to say is that those who predicted that GDPR would not be used are simply wrong. Since last May there have been, according to estimates from the European Data Protection Board (EDPB), some 144,376 complaints under GDPR and 89,271 data breach notifications. Whilst hard figures are difficult to obtain, the UK probably tops the table for complaints with around 19,000 compared to the level of complaints in France, Germany and The Netherlands reported as being in excess of 10,000. The likely top of the table as far as data breaches are concerned is The Netherlands with 20,881 breaches reported in 2018 alone.

Regulators have also been proactively taking action to enforce the law. In Germany, even a relatively small Data Protection Authority (DPA) in North Rhine-Westphalia has imposed more than 30 fines. Regulators have done audits too with, for example, 75 compliance checks in Lithuania and 150 in Italy. Italy also reports having processed 707 administrative violations in 2018. The courts have also been busy – the chair of the EDPB also recently said that 950 GDPR complaints have reached the courts.

So what are the most popular areas of activity?

Again, it's difficult to get hard and fast data but our intelligence from the cases we have seen, statements from DPAs and Cordery GDPR Navigator would indicate that the activities probably fall into 4 general areas; security, the six principles of GDPR, data subject rights and finally data protection impact assessments (DPIAs).

Security

Security has also been one of the most talked about aspects of GDPR. We have not seen many cases on large data breaches but we know there are on-going investigations. In The Netherlands as at January 2019, the Dutch DPA had taken action against 298 organisations that had reported a data breach and one of the most widely reported cases from Portugal was one of the first GDPR cases involving a fine of €400,000 for Centro Hospitalar Barrerio Montigo for breaching the security provisions of GDPR (amongst other violations). The DPA's findings included the fact that there were 985 users of the hospital's IT systems associated with the profile 'doctor' for a hospital that employed only 296 doctors.

We haven't had the large fines for security breaches that some predicted but that was never likely to happen in the early days of GDPR partly because these cases take time to investigate.

The 6 Principles

We have seen a number of cases concentrating on aspects of the 6 principles of GDPR, in particular the obligation to use data lawfully, fairly and transparently. The cases include the French DPA's findings against Google, the UK ICO's Stop Processing Notice against HMRC, and the ICO's investigation into Bounty. It seems that a number of regulators are paying particular attention to transparency and that emphasises the need for people to be open and upfront with the data they are collecting and what they are doing with it. There is more information on some of the requirements of the transparency principle in our alert on the Google case here:

http://www.corderycompliance.com/french-data-protection-authority-fines-google-e50m-for-violations/ and the ICO's investigation into Bounty here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/04/bounty-uk-fined-400-000-for-sharing-personal-data-unlawfully/

Data Subject Rights

We have seen a large number of data subject requests in our practice and some especially challenging subject access requests from employees and aggrieved customers in particular. Awareness of the ability to make a subject access request is on the up, even if some people are mistaken about what they can ask for. Organisations do need to treat data subject rights properly and to deal with regulators appropriately when they seek to enforce the law on behalf of data subjects. A pre-GDPR case recently brought by the UK ICO against Cambridge Analytica, in some respects, illustrates how not to do it. http://www.corderycompliance.com/ico-secures-criminal-convictions-against-ca-in-sar-case/

DPIAs

We see a great deal of activity around data protection impact assessments which in many respects are the most opportune way of identifying and dealing with GDPR risks. In many of the cases we deal with, regulators are asking to see a DPIA upon receiving a complaint and it is clear that they will expect a risk assessment to be done, particularly when new technology is being employed. There is more on data protection impact assessments in our 2018 alert here http://www.corderycompliance.com/data-protection-impact-assessment/

Conclusion

What's clear then is that there certainly has been a great deal of GDPR activity and it is no surprise that, with one exception, the fines have not been huge. There are some interesting cases heading to court particularly over the one-stop-shop mechanism which was a subject of debate in the Google case in France and is likely to see a number of cases head to the ECJ.

It is clear that GDPR is still a hot compliance topic and that it is here to stay.

For more information regarding GDPR, see details of Cordery GDPR Navigator here: www.bit.ly/gdprnav

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.