PAUL HASTINGS

PH PERSPECTIVES

May 2019

Follow **@Paul_Hastings**

Married Bliss or Headed for Divorce? Happy Anniversary GDPR!

By Sarah Pearce & Ashley Webber

The first year of marriage is often considered a year of adjustment—to make a marriage work, changes have to be made. Now, one year on from 25 May 2018, a day that will forever be known to data privacy lawyers as "GDPR D-Day", we would like to take a look back at the year to see what has been achieved, whether expectations have been met and, most importantly, what can be learned and taken forward into the future. More to the point, has the much anticipated regulation lived up to the hype? Will it be a marriage new couples aspire to have and look up to? Or is it going to be fraught with lessons on what not to do?

Quick Refresher

Before beginning our "couples counselling" style analysis of the past year, let's remind ourselves of the foundations of the marriage.

The GDPR (General Data Protection Regulation) is an EU regulation with direct effect in all EU member states regulating the processing of personal data (information which directly or indirectly identifies an individual). The GDPR has extra-territorial scope meaning it can apply when: (i) the personal data being processed belongs to a person outside the EU; (ii) the personal data is being processed outside of the EU; or (iii) the organisation processing the personal data is not itself established in the EU.

The GDPR was implemented to protect the rights and freedoms of individuals and their personal data, and to harmonize data protection legislation across the EU. It built on previous legislation whilst also introducing new principles, rights, and obligations to ensure increased protection of individuals' data. Amongst the most notable changes were the headline-grabbing financial penalties: a regulator can impose a fine of up to €20 million or 4% of annual global turnover, a staggering increase from the position pre-GDPR which, for example in the U.K., meant fines were capped at £500,000. The GDPR also sought to increase the focus and attention on security of data, strengthening the obligations upon organisations holding data and introducing a mandatory reporting obligation for personal data breaches.

So What Has Happened Since the Wedding?

The build-up to the wedding was intense with guests on a daily countdown until the big event. For many, nerves were running at an all-time high, wondering "have we remembered everyone and everything on our list?" Given the press coverage during the weeks running up to 25 May 2018, it may seem like not very much has happened since. Rather like the hopeful, engaged couple predicting a year as newlyweds filled with exciting new experiences and fireworks, the press predicted a wave of enforcement actions by newly empowered regulators wanting to show their muscle and a multitude of very large fines being issued across Europe shortly following

implementation with the large tech "giants" being on the receiving end. That has simply not happened—yet. We will look at fines shortly but it's worth noting that while the predicted "exciting" phase of this new marriage has yet to occur, the second year of marriage looks set to be much more eventful.

Public Awareness

While not everyone will know what "GDPR" stands for, nor will they know exactly what it means for them, the public awareness of data and the need for it to be protected, not only in the EU but globally, is at an all-time high. The EU Commission recently revealed that during the peak month of May 2018, the GDPR was searched more often on Google than Beyoncé or Kim Kardashian. Furthermore, since May 2018, the Commission reported it had received a significant rise in the number of complaints made by individuals believing their rights had been violated, with the current figure standing at over 100,000. This increased public awareness may stem from a genuine concern over how data is being used or simply be the result of the flood of emails in the lead-up to 25 May 2018 with subject lines such as, "GDPR—Consent Needed Now" or "Please See Our Updated Privacy Policy".

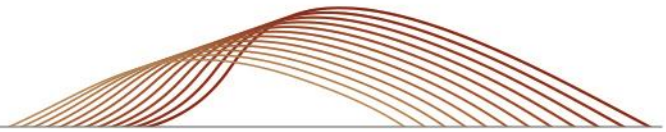
Without a doubt, and for whatever the reason, the GDPR has immensely helped in bringing the issue of data protection to the surface, to a point where it is openly discussed in public forums and people are really starting to consider—and question—whether their data is being handled correctly.

Personal Data Breaches

With the introduction of a mandatory reporting requirement, we have seen a substantial increase in the number of personal data breaches reported to data protection authorities across Europe. Between May 2018 and January 2019, the EU Commission reported that approximately 42,000 personal data breaches had been notified. The Information Commissioner's Office (the "ICO") in the U.K. stated roughly one third of the 500 weekly reports of personal data breaches are unnecessary and do not meet the threshold required for reporting. Reporting breaches unnecessarily was an inevitable consequence of the new obligation: assessing whether a breach "*is unlikely to result in a risk to the rights and freedoms*" of individuals can be difficult in the absence of good guidance, expert knowledge, and experience. Whilst the European Data Protection Board (previously the Article 29 Working Party) provided guidance in August 2018, organisations are still very nervous around the reporting requirement and many will feel it is the "lesser of two evils" to report the breach rather than not and possibly being in breach of the reporting obligation, as the fine for doing so could be up to €10 million or 2% of annual global turnover. It is expected that, with time, the quality and availability of guidance will improve—we will start to see many more self-help marriage books on the shelves over coming months and years. However, it is important that when an organisation is considering whether to report a personal data breach, it should apply careful consideration and judgement to the facts in hand. Guidance is just that—guidance, not rules. It is unlikely any published guidance will contain an example that exactly fits the circumstances and therefore an in-depth deliberation of the facts on a case-by-case basis will always be required.

Enforcement Actions

In light of the press coverage, or possible misplaced expectations of marriage, the rate and number of enforcement actions under the GDPR to date may appear anti-climactic. However, there are several key reasons for this including the usual length of time it takes for new legislation to be applied and, as Stephen Eckersley (Director of Investigations at the ICO) indicated at a recent conference, a large proportion of the work since May 2018 has been on "legacy cases" meaning the regulator has been dealing with a pre-GDPR backlog before even starting to tackle post-implementation issues. More specifically, certain notifications made post-GDPR relate to personal



data breaches arising prior to the GDPR implementation date and are therefore subject to—and are assessed under—the old regime. In fact, while it may not be as clear on the face of it, the enforcement actions taken to date across Europe are showing steady progress with this specific pillar of marriage beginning to show its growth: in due course, it will be "business as usual" with the GDPR for data protection authorities.

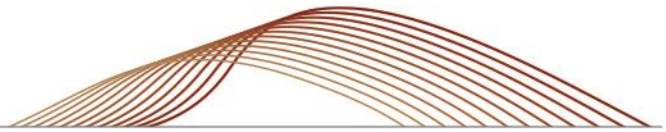
The first enforcement action under the GDPR was taken by the ICO in the U.K. in October 2018. The ICO issued an enforcement notice against Aggregate IQ Data Services Ltd which processed personal data on behalf of U.K. political organisations. To the surprise of many, the company is actually based outside the EU in Canada yet the company was found to have breached the GDPR on several counts including the principle of transparency and the obligation to process personal data lawfully. The ICO ordered the company to erase all personal data of individuals in the U.K. either processed or retained by the company on its servers within 30 days or face a fine of up to €20 million or 4% of its annual global turnover. Since issuing this enforcement notice in October 2018, the ICO has only issued one further public enforcement action under the GDPR. This was against HMRC in May 2019 and related to a breach of Article 6 in processing biometric data. HMRC has 28 days to comply with the terms of the enforcement notice or face the same financial penalties as were threatened to Aggregate IQ. Is this new enforcement action a sign we are about to see the ICO ramping up its actions?

Taking a step back in time again, the first three fines were issued by the data protection authorities of Austria, Germany and Portugal, for €4,800, €20,000 and €400,000, respectively. The fine imposed by the Portuguese regulator, being the largest of the three by a significant margin, was imposed on a hospital for violating its obligation to ensure adequate security measures were in place to protect personal data. When assessing the German and Portuguese fines together, it appears as though a much stricter stance was taken towards the latter for breaching the same obligation.

While there are different factors to each case, diverging approaches by regulators have often been criticised as a potential issue with the GDPR, especially given the raft of powers available to them and the financial sums potentially involved. Regulators should seek to work together and learn from each other or we may well see a rise in abuse of the "one stop mechanism" by "jurisdiction shopping", i.e., choosing to bring actions in jurisdictions which will benefit the relevant party. The "one stop mechanism", established by the GDPR, provides one enforcing entity for an organisation with several EU entities in the jurisdiction of its main establishment. While "main establishment" is defined in the GDPR, as with any definition, it is open to interpretation allowing parties to argue their case to better their position.

The fines had appeared to increase at a fairly steady pace with many regulatory authorities becoming slightly bolder with their sanctions. Then came 21 January 2019, the day the press had been waiting for: Google were fined €50million by the French data protection authority, the CNIL, for breaching the GDPR—let the matrimonial excitement begin. The fine was based on Google having violated: (i) its obligations of transparency and information; and (ii) its obligation to have a legal basis for personalised advertisements. The decision is interesting not only for the legal basis on which the fine was imposed, but also that this was the largest fine to be imposed under the GDPR to date and on a key tech "giant" with significant reputational considerations.

The message here is therefore twofold: not only is the French authority saying that action will be taken for non-compliance, but the case also provides a sign that fines of this magnitude—and larger—can, and will, be imposed. Whilst regulators are not bound to follow the decisions made by other regulators and each complaint or breach is to be considered on its own merits, if a regulator is faced with a complaint that is similar to one that has already been publically enforced by another regulator, is the likelihood not that the first regulator will look to the second regulator's



decision for possible guidance, maybe even encouragement to propose a fine of the same magnitude?

On a slightly separate note, another element of this action which has been widely discussed is the CNIL's application of the "one stop mechanism", as discussed above. In this case, even though Google's EU headquarters are in Ireland, the CNIL applied its analysis to Google's presence in the EU and determined that its main establishment was not in Ireland and therefore the CNIL was competent to initiate proceedings. In addition to "jurisdiction shopping", can this also be seen as an abuse of the "one stop mechanism"? Should it have been for the Irish authority to consider taking actions? How can one hope for a successful marriage if the parties are not working together?

Future Challenges?

Increase in the Number of Enforcement Actions and Complaints

Over the course of the next year we anticipate a clear rise in the number of enforcement actions across the EU. Regulatory authorities will have had a year to catch up on the pre-GDPR outstanding actions and get to grips with the GDPR and all its nuances. Authorities will also likely start to learn from and take the lead from one another.

With the increase in publicity, further increase in complaints from data subjects is inevitable. In addition to complaining to the regulator, we have already seen a rise in data subjects complaining directly to organisations they believe have unlawfully processed their data, and the frequency will only continue to rise. Many individuals in this scenario will be pursuing compensation in the form of damages. To ensure organisations are prepared for a rise in complaints against them and possibly claims for damages, organisations, particularly those processing a high volume of personal data, should ensure they have appropriate practices and procedures in place to handle them as efficiently and effectively as possible. Dedicated mailboxes, for example, are useful to ensure nothing is missed. Another valuable tool is pre-prepared responses.

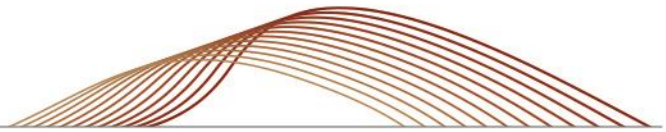
Brexit

The first year of marriage is to some extent uncharted territory for any couple. Add in the looming uncertainty of Brexit and hurdles abound.

At this stage, almost three years on from the vote, we're sure most of us expected to at least have certainty about the form Brexit would take. However, as we all know only too well, this is not the position we find ourselves in, thus leaving us in a state of flux as to how to approach a variety of legal issues, namely, for the purposes of this article, the application of EU legislation in the U.K.

Certain EU legislation, including the GDPR, has direct effect in all EU Member States meaning it is automatically applicable. This of course includes the U.K. When the U.K. leaves the EU, it will no longer be a Member State and therefore all directly applicable legislation, including the GDPR, will no longer have effect in the U.K. However this does not mean the U.K. will divorce the GDPR and change its relationship status to single. The ICO has confirmed a U.K. version of the GDPR will be brought into effect upon Brexit: day-to-day compliance will not therefore be hugely affected.

However, whilst this is the case, one potential challenge which must be addressed by any organisation processing personal data is that, when the U.K. leaves the EU, it will be considered a third country under the GDPR. This means that transfers of personal data from an EU country to the U.K. will be prohibited without additional steps being taken. A number of organisations operating globally transfer personal data on a daily basis so it is crucial that each such organisation identifies the transfers of data which will be affected by Brexit and reassess these



data flows to confirm whether further steps are required to ensure compliance with the GDPR post-Brexit and, if required, what these steps should be.

For further information on lawfully transferring personal data post-Brexit, please see International Data Transfers in the Limbo of Brexit and Brexit Update – What does this mean for data privacy?

New and Emerging Technologies

With new technology emerging every day, there is a risk the GDPR, as with any legislation, will quickly fall behind in its relevance and applicability to the technology industry: the world—and technology in particular—is advancing at such a rate that it is becoming increasingly difficult for legislators to keep up. The GDPR was enacted as an "all-industry" applicable piece of legislation, applying to every organisation that processes personal data. The GDPR will never be able to combat every risk that new types of technology, however deployed across multiple industries, will bring. Without specific industry guidance led by industry experts, industry-specific differences and quirks cannot all be catered for.

So how does the marriage survive this issue? To keep up with new technology, it is crucial that data protection authorities produce more detailed guidance on how the GDPR applies to specific types of technology and indeed, industries. This will assist organisations producing and operating technologies to ensure they are building compliant technology from the outset. The ICO recently launched one of the first initiatives focused on new and emerging technologies known as Sandbox. The initiative has been well received and will act as a support service for those organisations developing products and services that use personal data in innovative and safe ways.

Moreover, in the next five years, we are likely to start to see more legislation governing specific technologies. Already, pockets of legislation are being drafted and enacted around the world focusing on the development and manufacturing of IoT devices. Similarly, the development and deployment of artificial intelligence is starting to come to the forefront of legislators' minds, for example with the recent publication of the Principles on Artificial Intelligence by the Organization for Economic Cooperation and Development. Legislation, guidance, and other support of this nature will build on the work the GDPR has already done by regulating technology at the source and we believe that, over the next few years, we will begin to see such developments in legislation occur more regularly and on a global scale.

What Can Be Done to Ensure a Happy, Long-Lasting Marriage?

Whilst we are not convinced there is a one golden key that will ensure this marriage succeeds, we do believe there are several factors which can certainly help it achieve success, including:

- Authorities co-operating and working together, particularly in relation to the application of enforcement actions; and
- More industry-specific legislation and guidance that tackles nuances.

We are confident the future is bright for the GDPR: the marriage is solid and will only continue to blossom. Organisations therefore need to take it seriously.

It is crucial that organisations continually reassess their compliance with the GDPR. Internal audits, privacy impact assessments, and general data mapping are key tools in driving towards compliance. They also need to take note of what led to the enforcement actions and use this as a technique for their own compliance with the GDPR.

However, instead of just waiting to see how mistakes by other businesses are handled, organisations should be proactive and attempt to curb possible risks before they become actual

risks—and ultimately legislative violations. To do so, organisations need to understand exactly how they process personal data, why they process it in the way they do, and whether the processing they do is actually necessary. Policies are a very effective tool for cross-business awareness and application; for example, internal employee policies about handling personal data and reporting personal data breaches can be very useful in the event of a breach since there will likely be employee involvement therein (whether or not intentional).

In addition, vendor management policies are vital to promote compliance down the chain. If an organisation chooses to appoint a third party, for example, to process personal data on its behalf, it is still at significant risk and a policy regulating the appointment of vendors will provide evidence of it taking steps to ensure compliance with its own GDPR obligations.

Thankfully, more and more organisations are now viewing GDPR and broader data privacy and cyber-security as an organisation-wide risk. No longer are issues just for the IT team, they touch almost every part of an organisation. It is therefore crucial that the risks around, and compliance with, data privacy and security are met with a unified approach across the entire organisation, including amongst senior executives and the board. When the most influential persons in the organisation begin to take heed, the rest will follow.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

London

Sarah Pearce
44.020.3023.5168
sarahpearce@paulhastings.com

Ashley Webber
44.020.3023.5197
ashleywebber@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com