GD FINANCIAL MARKETS

INSIGHTS

GDPR:

Data just got personal

Introduction

In July 2019 the Information Commissioner's Office (ICO) issued a notice of its intention to fine British Airways £183.39M for infringements of the General Data Protection Regulation (GDPR)[1]. One day later it announced its intention to fine Marriott International £99.2M for failing to undertake sufficient due diligence when it bought Starwood Hotels and not sufficiently securing its systems[2]. These are by far the most significant fines issued by the ICO since the new regulations came into force in May 2018. While it may seem harsh given that the data breaches resulted from external cyber-attacks, it is a clear indicator of the stance the ICO is likely to take in such situations. In issuing the BA notice the UK Information Commissioner, Elizabeth Denham, said: "People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. "

In our Insight note, published shortly after GDPR came into force last year[3], we discussed the practical implications of GDPR for companies. In particular, we highlighted the areas including data security and third party risk management that companies needed to focus on. As the recent fines have signalled, firms need to be able to demonstrate their adherence to the regulations through their practical policies and procedures. Given the size of recent fines it is clearly also is in their economic interests to do so.

What have we learnt over the last year?

In the run-up to the introduction of the GDPR on May 25th 2018 the most tangible aspect for most people was probably the flurry of emails they received containing privacy notices from companies they had forgotten they had signed up with in the first place. Brief coverage of it in the news over the go-live period highlighted that the majority of members of the public were unaware of what the GDPR stood for or what it would mean for them. It was also clear that, aside from informing their clients, many companies treated it as business as usual. This typified the lack of understanding of what the GDPR meant in practice and the significant ramifications of the new regulations for firm's handling of their clients' data.

---

[1] *Intention to fine British Airways £183.39m under GDPR for data breach*, ICO, 8 July 2019

[2] *Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach*, ICO, 9 July 2019

[3] *May 25th was just the beginning*, GDFM Insight Note, July 2018

More clued-up companies, particularly those whose business models are based on personal data, clearly gave the area more thought. But in many cases and in our experience this seemed to focus on doing the minimum to enable them to continue to harvest personal data, with a focus on getting the user's agreement as opposed to making it easier for people to manage their data and control access to it by third (and fourth) parties. Again, recent fines for social media and search companies have demonstrated that the regulators in the EU and US are losing patience with this form over substance approach to the regulations.

As highlighted in the introduction, the responsibilities that companies take on if they hold personal data have been significantly reinforced by the regulator over the last year. This, together with increased third party and cyber-risks, mean that companies need to think carefully about what data they really need to hold, for how long and who they share it with. Legacy personal data stored with weak security can expose firms to significant fines.

It is clear that the GDPR and increased coverage of consumer rights has significantly raised public awareness of their personal data over the last year. It is dawning on people that the services they thought they were receiving for free were in fact being paid for with their data. More than that, their data has then been sold on to third parties to target and, in extreme cases, manipulate them. Public sentiment around companies' use of their data is clearly hardening. As people become more aware of their rights under the GDPR and related legislation they are making greater use of the tools available to them. In particular, firms have reported a significant increase in the number of Data Subject Access Requests (DSARs) they have received over the past year.

In our Insight paper last year we predicted a number of these trends and going forward they are only likely to strengthen. So, what do firms need to do to get comfortable controlling and processing personal data?

The business of personal data

In the run up to the GDPR many companies satisfied themselves by 'tweaking' their systems, processes and adjusting their data privacy notices. In some case this *de minimis* approach has come back to haunt them. Therefore first and foremost companies need to adopt a mind-set change about their clients' personal data. In particular, they need to understand the value and sensitivity of the data to its ultimate owner, the data subject, and protect it accordingly, just as they would the cash in their bank accounts.

A change in mindset and the associated tone from the top helps companies to get a better focus on what they need to do to manage personal data in a sound way and also to focus on the key practical areas including the investment needed to affect change. The examples below are not a comprehensive list of areas but rather demonstrate the typical questions that companies need to have a response for:

- Use of the data and consents management – has the data subject given clear, informed consent to the use of their data in all its forms (biometric, voice etc.)? Has it been made clear what data is being collected and how it is being used (including who it is being shared with) or is this hidden behind a default cookie acceptance or voice notification message? Have you limited the data collected to only that which is required to support the client relationship or are you harvesting additional data fields 'just in case'?
- Storage and portability of data – is it clear how and where the data is stored and who has access to it? Is the data duplicated across systems and/or processes? If asked by a client to provide a copy or delete their data could you conform and would it be clear what data was involved?

- Processing of data – what processes are using the data collected? Would the client have reasonably expected that this was how their data is being used?
- Data sharing – who is the personal data being shared with and why? Are the data controllers and processors clearly identified? How are you maintaining control over the data being shared, especially with third parties? Where this is cross-border are these equivalent regimes?
- Data security – are you protecting customer data from cyber-attacks or unauthorised access as you would your firm's own proprietary data? Is it covered as part of your penetration testing? Is data deleted when it is no longer required?
- Data Subject Access Requests (DSAR) – do you have embedded procedures for how you would respond to a DSAR? Do you know where you would go to access the information (i.e. email, electronic documents, physical documents, phone records etc.) and are you confident that this would be comprehensive and completed in the required timeframe?
- Sensitive data – have you adequately identified sensitive date in the personal data you are collecting and applied the appropriate controls to it in line with the regulations?
- Training /Testing – it is one thing to have the policies and procedures but have your staff been trained practically on them e.g. in the specific context of their roles? Have you tested your procedures to see that they are embedded and work practically in all situations?

These are just a small fraction of the practical questions that firms need to ask themselves in designing and implementing their policies and procedures around personal data. It is clear that the position of the ICO, and indeed regulators around the globe, with respect to data privacy is hardening. Ultimately, as with all regulation, the best protection is to demonstrate compliance with both the spirit as well as the letter of the rules.

About GD Financial Markets

GD Financial Markets works with clients to solve their operational and regulatory challenges including implementations and reviews of GDPR frameworks. In particular, we have broken down all the articles of the GDPR and developed an associated set of actions for companies. If you would like to know more about this or our other services contact our Business Manager at aartiodonnell@gordondadds.com.

Contact the author

Anthony Fraser is an advisor with GD Financial Markets, working with the partners to develop client solutions. He has extensive experience in financial service operations including technology implementations and regulatory processes. Anthony is a chartered engineer and a member of the Institute of Engineering and Technology. You can contact him at anthonyfraser@gordondadds.com.