ESG Viewpoint

January 2019

Daniel Jarman
Responsible Investment Team

David Sneyd
Responsible Investment Team

Contact us

Institutional business:

+44 (0)20 7011 4444

institutional.enquiries@bmogam.com

Discretionary Sales:

+44 (0)20 7011 4444

client.service@bmogam.com

UK Adviser Sales:

0800 085 0383

sales.support@bmogam.com

bmogam.com/responsible-investing

Telephone calls may be recorded.

Raising the bar on data privacy

Technology is central to how we live our everyday lives in the world today. From the way we shop or monitor our health, to how we keep in touch with loved ones, it has enabled us to be more connected, more productive and more informed than ever before. Fuelling this is a reliance upon substantial amounts of personal data, which has become such a critical component within modern business that it has itself become a commodity.

This pace of change in technology and its leveraging of personal data has significantly outpaced that of data privacy regulation, meaning that individuals can no longer be sure who has personal information on them, what it is used for or how well it is protected. Somewhat inevitably companies have not always got this right, with highly publicised data breaches and privacy scandals hitting the headlines this past year. This has contributed to the current 'techlash', as both regulators and end-user question the power held by technology giants.

Regulators have been working to keep up with the rapid pace of change. The most significant regulatory development at a global level was the introduction of European legislation in the form of the General Data Protection Regulation (GDPR). This came into effect in May 2018, with the aim of giving EU citizens more control of their personal data . Unlike most other regulations, GDPR explicitly has extra-territorial reach, meaning that any company which does business with EU citizens must be compliant. Many other countries including Canada, Argentina and Brazil, as well as the State of California, have recently introduced new legislation or toughened up on implementation, picking up on elements from the GDPR model.

> It's time to face facts. We will never achieve technology's true potential without the full faith and confidence of the people who use it.
>
> **Apple CEO Tim Cook**

Over this past year we have seen the introduction of GDPR as a catalyst for companies to clean house and update their interaction with personal data to ensure that it is fit for purpose. Reflecting the broad demands of the regulation, this work goes beyond just the IT department, extending into how the board oversees the issue, how on-going compliance is monitored by a data protection officer (DPO), the culture amongst employees to prioritise data privacy and relationships with suppliers. But there are questions over how this is implemented in practice, with different governance structures offering a variety of risks and opportunities.

Engagement action

To better understand the challenge that the implementation of GDPR-consistent data privacy and security measures presents, we engaged with a group of 28 global companies from sectors we considered to handle significant amounts of EU citizens' personal data within their business model, particularly those in the technology, pharmaceuticals, finance and consumer industries.

As part of our engagement we requested to speak with either the company's DPO directly, or someone with operational oversight of the area, to focus on what they had done to prepare for GDPR's introduction, any impacts on its business model, what governance arrangements are in place to manage the risk, as well as any innovation in this area.

Engagement Responses and Findings

Given the sensitive nature of this topic, the level of access we were given within companies exceeded our expectations. We spoke directly to individuals directly responsible or data privacy in the majority of cases. Most conversations with companies were frank and open, with companies honestly presenting the progress that they had made, as well as their shortcomings. Our key findings are detailed below:

Preparedness

About half of the companies that we engaged with have established the requirements of GDPR as their global standard for data privacy across their entire business, with others generally opting to enforce the spirit of the regulation outside of their Europe operations without implementing more strenuous parts, such as the 72-hour breach notification procedure.

Given the scale of the task at hand and relatively short time frame, we were not surprised that only one company claimed to be 'fully compliant' by the time that GDPR had come into force. Nearly all companies reported having adopted a risk-based approach to achieving compliance, having completed the most material parts that posed the highest risk. The most common areas of work remaining were contracts with third-party suppliers and adapting legacy systems to allow for new features for which they were never designed, such as data deletion.

Implications for products and services

In general companies said that the more restrictive aspects of GDPR, such as requiring explicit consent and ensuring data minimisation, had not prevented them from continuing to provide any of their existing core products or services, only adding to the cost of doing so. An outlier to this was one company who commented that it felt that it was at a disadvantage compared to their American counterparts, as there were restrictions on how they could further monetise customer data beyond agreed purposes.

Role of data protection officers (DPOs)

GDPR expects companies to have one or more designated Data Protection Officers (DPOs). DPOs are expected to operate on an independent basis, acting as the primary contact for regulators, and for individuals seeking information on how their data is being held or used.

Nearly every company we spoke with had appointed a senior figure to be responsible for data protection and privacy compliance, with an assigned group-level DPO taking this key position at only half of those that we spoke with. An equally popular choice of operating model was a 'hub and spoke' approach, whereby they appoint a centrally based Global Privacy Officer, into which regionally based DPOs would report.

In terms of meeting the requirements for the DPO to operate independently, but also report into highest management, most DPOs or privacy officers were based within the legal compliance or risk functions of the business. The most common reporting line was into either the General Counsel, Chief Compliance Officer or Chief Risk Officer, although at smaller companies they would often report directly into the CEO.

Governance Oversight

The role of overseeing a company's GDPR compliance was most commonly assigned to the board's Audit Committee, which is to be expected given its function in monitoring the company's risk management process. However only a few companies appear to have provided formalised training to board directors to help them monitor what can be a complicated and technical issue, and even fewer clearly identified who has relevant skills on the board to provide effective oversight.

Training and company culture

Nearly all of the companies in our sample had provided training to employees on GDPR around the time of its implementation, generally on a mandatory basis and through the use of online courses. In addition to this, some provided further extensive training to more specialised roles where there was greater handling of sensitive personal data.

GDPR requires companies to ensure that data privacy is not an afterthought, or that they collect more personal data than

Continued

"Disclosure on data privacy standards is limited and inconsistent. This contrasts with the relatively high level of internal awareness on data privacy at the companies that we engaged with."

what is really necessary. From talking with companies from a wide range of sectors, this poses not only a compliance point but a deeper cultural challenge, particularly in science based industries like pharmaceuticals where the mass collection of data has been standard practice:

"The difficult thing is that humans love data and they like to keep it.

Pharmaceutical company, in discussion with BMO GAM

Only a small number of companies were able to give examples of how they have raised awareness of privacy matters though targeted internal campaigns. A more common approach was the use of data privacy champions or ambassadors, who were selected employees in different business functions that either advocated for raising awareness on data privacy or were a day-to-day contact for related enquiries. In general companies were not clear on how they would address the task of shaping company culture to match the expectations of their clients and regulators.

Collaborations

Another common theme among companies was that there has been a high level of industry collaboration on how to best comply with GDPR through trade groups and industry networks. In some instances, we heard of companies rising above their competitive interests, with DPOs from rival firms maintaining open dialogue and sharing ideas with one another on how to best achieve compliance.

Further action

One overarching finding is that disclosure on data privacy standards is limited and inconsistent. This contrasts with the relatively high level of internal awareness on data privacy at the companies that we engaged with. Where disclosure was provided, it was often anecdotal in nature, making a comparison between companies difficult to achieve.

In order to move beyond this, we have formulated a high-level disclosure framework, which we think covers the most important areas of compliance. We have shared this with those companies within our sample and have encouraged them to consider adopting it in their future reporting. The principal areas of disclosure should include:

- **Acknowledge of the importance of data privacy**, particularly by senior management in setting the tone from the top, as well as detailing any implications on company strategy and formal recognition within the risk register;
- **Governance arrangements for data privacy**, including where the DPO function sits within the organisation, who they report to, and how they interact within the organisation;
- **Formal oversight of data privacy**, including any delegated responsibility at executive management and non-executive board level, as well as how performance is monitored;
- **Recent and relevant experience on the assigned oversight committee**, including which director is considered to hold this experience;
- **Company culture on data privacy**, including formal staff training, any inclusion within a code of conduct and other initiatives such as employee-level data privacy champions

Continued

Conclusion

The overall impression that we got from our conversations with companies is that data privacy is being taken seriously, with the introduction of GDPR being a key factor in significant investments in upgrading their processes and oversight of how they handle personal data. At the same time, given the scale of the task at hand in fully complying with GDPR, this transformation is not yet complete with few claiming 100% compliance. Our expectation would be for this to change over this year as the tail end of low-risk compliance work is completed.

The variety of responses that we received also confirmed that there is no one-size-fits-all model for GDPR compliance, with company responses being crafted to reflect their business model and existing governance structures. What is consistent across the board is that disclosure on the issue remains limited and inconsistent, making the monitoring of preparedness and ongoing improvements more difficult, for which we will continue to push for improvement over the coming year.

Pressure from regulators on one side, and their customers on the other, means that data privacy is an issue that neither companies nor their investors can afford to ignore. More consistent disclosure will be critical in order to spread the adoption of best practice, and to allow investors to differentiate between leaders and laggards.

Key risks

The value of investments and any income derived from them can go down as well as up as a result of market or currency movements and investors may not get back the original amount invested.

reo® is a registered trademark of BMO Asset Management (Holdings) PLC.

How BMO Global Asset Management can help you

BMO Global Asset Management incorporates material ESG issues into its investment processes across asset classes. We also offer our Responsible Funds range, which invests in companies operating sustainably and excludes those not meeting our ethical and ESG criteria, and our ***reo***® engagement service, through which we provide engagement and voting services covering global equities and credit.

Best ESG Research Team 2018

INVESTMENT WEEK
SUSTAINABLE & ESG INVESTMENT AWARDS 2018
WINNER
Best ESG Research Team

BMO Global Asset Management