ESG Viewpoint

February 2018

General Data Protection Regulation (GDPR) – What does it mean for companies?

David Sneyd
Senior Associate
Governance and Sustainable Investment

Summary

- The General Data Protection Regulation (GDPR) comes into effect on 25 May 2018 with the aim of strengthening cybersecurity, increasing privacy for EU citizens and unifying data legislation from across the European Union. It replaces the Data Protection Directive (1995). Unlike its predecessor, it has extra territorial reach, which effectively makes it the first global data law.
- Since that time there have been vast technological advances impacting all parts of our lives, affecting the way that personal data is collected, processed and stored. In parallel, modern day businesses have never been more reliant on using data in all aspects of what they do.
- Within this context, GDPR aims to enshrine EU citizens' right to privacy by giving them back control of who holds their personal data, how it is used and how well it is protected. This is alongside a backdrop of escalating threats of cyber-attacks, as personal information is valuable for criminals.
- Although GDPR will benefit companies through streamlining the data regulatory landscape, we foresee it capturing a broader range of global companies than present, increasing the cost of compliance and requiring widespread governance and cultural reform to ensure that data protection and privacy is a priority. Few businesses are fully prepared, but we think that an initial period of grace from regulators will reduce compliance risk.

Contact Us

Institutional business:

1.844.855.7034

bmoam.institutional@bmo.com

bmo.com/institutional

Continued

Background

Over the past two decades there has been a dramatic gear-change in how society uses technology, with your average business now more reliant on the processing of data than ever before. This applies to not only how their business operates, but for some of today's most highly valued companies it sits at the core of their product offering. Meanwhile, consumers in both developed and emerging markets are integrating digital services into their lives at an unprecedented rate, with the resulting data being both personal and increasingly valuable in nature.

Somewhat inevitably this has led to a similar increase in cybercrime, as hackers look to take advantage of personal information being inadvertently accessible through company systems being put online without the required security provisions to keep them out. In addition to this, with companies so reliant upon technology for their day-to-day operations, there are increased disruption risks as criminals look to profit by holding companies for ransom. Finally, the use of hacking by nation states means that those companies that can be considered as part of a country's critical infrastructure or of strategic importance, such as utilities, banks and telecommunications being at particular risk.

"Cybersecurity risks are growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace."

The Global Risks Report 2018, World Economic Forum

Within this context, the European Union has updated its rules on data protection that were first introduced in 1995. Originally this process focused on looking to enshrine the right to privacy as a universal human right for its citizens; however during the drafting process this remit was broadened to also include the security of data as the threat level increased over that time.

Although the new data rules are much more far reaching and demanding than those that came before them, the EU has put forward GDPR as more beneficial to business than burdensome. This is primarily due to it streamlining the compliance process by putting an end to the patchwork of overlapping data protection rules that currently exist within individual member states, as well as introducing a "one stop shop" principle where companies can work with one local data authority, with the understanding that any agreements will passport to all others. Given its expanded territorial reach (detailed below), it will also offer a more balanced treatment between EU and non-EU companies on how they handle personal data.

"These new pan-European rules are good for citizens and good for businesses. Citizens and businesses will profit from clear rules that are fit for the digital age, that give strong protection and at the same time create opportunities and encourage innovation in a European Digital Single Market"

Věra Jourová, Commissioner for Justice, Consumers and Gender Equality

That being said, despite these advantages there are still substantial challenges for companies to comply with GDPR. In this viewpoint we will examine what is new under this legislation and what the implications will be for companies.

How is GDPR different from existing data regulation?

- **Potentially applies to all companies globally:** Unlike the rather ambiguous regulation that went before it, the scope of GDPR is not defined by where companies that use personal data are located, but rather where their current or potential customers are based. The new regulation will apply to any company that handles personal data of a European Union citizen, irrespective of whether this activity takes place inside the EU, making it the first global data protection law.
- **Widens the definition of personal data:** While the definition of personal data is pretty broad under existing data laws, it will be further extended under GDPR to include any data that can be used to identify an individual. This includes information that might seem quite generic or mundane in isolation, but could become unique and personal when viewed in combination. New types of information will include the geographical, physiological, genetic, economic, cultural or social identity of someone. In addition to this, under certain circumstances, personal data now includes online identifiers such as IP addresses and mobile device IDs.
- **More significant penalties:** The most severe breach of

Continued

GDPR, such as having insufficient consent to process customer data or a data leak resulting from inadequate security provisions, can be fined by up to 4% of annual global turnover or $30 million[1] (whichever is higher). This is substantially higher than what is possible under current legislation, i.e. $872,000[1] in the UK or $1,374,000[1] in the Netherlands. Overall, there is a tiered approach for fines, with a fine of up to 2% of annual global revenue possible for minor breaches such as not having records in order or not notifying a data subject about a breach.

- **Gives less control to companies and more rights to data subjects:** Unlike the current consent regime for companies to use customers' personal data (which is implicit and opt-out in nature), individual customers will need to explicitly opt-in for how their data will be used going forward. Companies will no longer be able to use long illegible terms and conditions full of legalese to attain consent. In addition it introduces the right to be forgotten, for data subjects to see what data is held on them in an easy and free manner, alongside an overall restriction on using personal data for anything other than what it is originally collected for.
- **Mandates the appointment of a Data Protection Officer (DPO):** Companies that either systematically "monitor data subjects on a large scale" or "process on a large scale specific categories of data" will have to appoint a DPO. The DPO must have expert knowledge of data protection laws, must report to the highest level of management and can either be a staff member or outsourced to an external service provider.
- **Introduces a common data breach notification requirement:** Companies can no longer hide data breaches and inform customers or the market when they are ready to do so, but rather will be required to notify both supervisory bodies and the individual who is the subject of the data within 72 hours of any breach that is likely to 'result in a risk for the rights and freedoms of individuals'. This is more specifically defined as where a breach could (rather than has) lead to, amongst other things, an individual being subject to discrimination, identify theft or fraud, financial loss or reputational damage.
- **Extends liability beyond companies to third-party providers:** Under current regulations the responsibility for keeping data safe and private sits with the "data controller", which is the company that wishes to use the data somehow and decides how it is processed. By comparison, "data processors" are those that actually process the data on behalf of the company, such as third-party software vendors or a cloud-computing provider. Responsibility for data protection currently sits wholly with these "data controllers", but under GDPR this liability will also be extended to all third-party organizations that touch personal data.
- **Allows any European data authority to take action:** By means of example, Ireland is currently popular with US corporations as a residence for their data controllers because it has a relatively lenient local data protection authority, but under GDPR any European authority can take action against an organization. The benefit for companies is that they will have to deal with only one supervisory body as compliance/agreements with them passports to all others, but at the same time there is a stronger enforcement regime, as data subjects in any member state can approach their locally based regulator with any concerns.
- **Requires companies to be pro-active and intentional on data protection:** The new legislation will mandate the principle of 'privacy by design', which requires that data protection be an integrated part of how systems are designed, rather than an additional feature or afterthought. Before projects are even started, companies will also be required to conduct a privacy impact assessment (PIA), which sets out what data points will be collected, how it is maintained, how it will be protected and how this data will be shared. The DPO will be responsible for ensuring that the PIA is complied with throughout the build and use of such systems.

What are the consequences for companies?

With modern day businesses having never been more reliant on processing personal data, few will escape the implications of GDPR requirements. We think that the main consequences of this new data legislation can be summarized into three different areas:

- **Wider scope of data compliance**
  At present those companies who are based outside of the EU and process data of its citizens in their home territory are not required to comply with EU data protection laws. GDPR extends its qualifying criteria to also include not just how data is processed, but who the data concerns, meaning that a wide variety of companies based outside the EU will now be subject to this new standard that is much more stringent than

[1] Source: BMO Global Asset Management exchange rate as at January 31, 2018

Continued

what is seen in some other regions. For example, a Chinese flower delivery company allowing EU citizens to make orders for fulfilment only in China is currently not in scope, but under GDPR it will be.

Scope has also been increased to include a wider range of data uses through either direct reference, such as profiling through big data algorithms, or through the broadening of the definition of personal data to include location data or online identifiers. Any business that is reliant upon profiling its customers will now be subject to further procedural checks, which will reduce the efficiency of these processes. In addition, individuals will have the right to refuse to be subject to these processes all together, meaning that companies need to have a contingency operation in place to accommodate these requests.

Finally the new data regulation extends responsibility from just data controllers (i.e. the company who uses the data for its business) to those who only process data. Given the recent move towards 'cloud computing' and the out-sourcing of technology infrastructures provided to third parties, those companies that provide such services will now be exposed to high regulatory risk across their client base. In addition, data controllers will need to ensure that everyone who interacts with their customers' data on their behalf, be that transferring, storing or processing, handles the data appropriately and securely. This introduces the concept of data supply chain management, which similar to conventional supply chain management, sets in place due diligence procedures to ensure that all those involved are robust and do not expose them to undue compliance risks.

- **Increase in cost of data compliance**
The most obvious potential cost from GDPR is the substantially increased penalties for non-compliance, where companies can be fined by up to 4% of annual global turnover or $30 million[1] (whichever is higher). Given GDPR's extended territorial reach, it is also foreseen that EU data authorities will be able to enforce penalties through local authorities, including many regions where it already has history of co-operation.

  This was seen when the UK telecommunications company TalkTalk was fined just £400,000 in 2016 for a poor cybersecurity controls that allowed the leaking of personal data on 21,000 customers the year before, being near the maximum permissible under current UK data laws. By comparison, this fine could have been up to £72 million (4% of its global annual turnover for that year) under GDPR. The risk here is only made worse by the increased difficulty in complying with GDPR and the large penalties for not doing so.

"If a business can't show that good data protection is a cornerstone of their practices, they're leaving themselves open to a fine or other enforcement action that could damage bank balance or business reputation."

Elizabeth Denham, UK Information Commissioner

Alongside this, there is the substantial compliance costs that will be associated with the new requirements of GDPR. The systems and procedures that companies use to process data will need to be upgraded to be able to meet new requirements, including audit procedures that prove proper consent or facilitating requests by data subjects to see what data is held or exercise their right to be forgotten. For those companies that have not already invested in good data governance or robust processing procedures, there will be a substantial amount of capital investment required to catch up with the standards now expected of them. In addition, there will be a slowing down of productivity as resource is allocated to dealing with these requests as part of business-as-usual processes.

- **Revenue impact on data-reliant products and services**
The other main cost will come in the form of loss of revenue from existing business practices. For years, companies have used customer data in an unrestricted way through obtaining implicit consent from users on an opt-out basis.

"More than 8 in 10 firms falling under the scope of GDPR say they'll need to adapt products to comply"

IAPP-EY Annual Privacy Governance Report 2017

[1] Exchange rate source: BMO Global Asset Management as at January 31, 2018

Continued

Some sectors, such as retail, have become dependent upon this to curate the online experience of their customers based on personal data and their purchase history. Under GDPR individuals will not only have to opt-in for their data to be collected, but also what it can specifically be used for. Given that consumers are becoming more aware of keeping their personal data private and protected, the expectation is that many will not provide the consent needed for retailers to maximize customer spend under their current established business practices. By further means of example, a 2017 survey by PageFair discovered that only a very small proportion (3%) of those asked believed that the average user would explicitly consent to "web-wide" tracking for the purposes of advertising (tracking by any party, anywhere on the web). By comparison, under current legislation this practice is permissible without consent and widely adopted.

- **Cultural/governance reform on data compliance**
An underlying principle of the new legislation is that companies should work to create a culture of privacy within their organizations. Like any successful effort to shape corporate culture, it needs to be led by those in a position of authority by 'setting the tone from the top'. However, anecdotal evidence has suggested that senior ranks getting a proper grasp of the issue has proven to be a challenge for companies, as data privacy and security has historically been viewed more of an operational issue rather than of strategic importance for consideration at board level.

> "The survey of almost 900 members of the Institute of Directors… shows that nearly a third of company directors have not heard of GDPR, while four in 10 don't know if their company will be affected by the new regulations."
>
> **UK Institute of Directors, October 2017**

In addition to this, there is the requirement for certain companies that are data processing intensive to appoint a Data Protection Officer (DPO) who must report to the highest level of management. For those companies that do not already have governance procedures in place for considering data privacy and security issues, work will be needed to fully establish this new role and ensure that it has the internal authority and correct reporting-line to be effective.

The same is true for having procedures in place for reporting data breaches, which under GDPR companies will need to do within 72 hours of discovery. Those companies that already have reporting lines establishing and procedures in place for doing so will be at an advantage, such as banks who go as far as playing 'cyber war games' to rehearse the process. However, recent incidents at Equifax and Uber have demonstrated that in practice some companies prefer to conduct a full investigation that can take several months before informing those outside the company. Such action will be impermissible under GDPR. For those companies for which this is a new concept will have to face a steep learning curve.

Finally, this cultural shift will need to manifest in GDPR's privacy by design principle. In practice, this will require companies to take such considerations into account early on within their strategic planning or product development process rather than as a factor to take into account after the fact.

Conclusions and next steps

Although GDPR provides an opportunity for global companies to have a simpler and more productive relationship with data regulators in Europe, in an area that is increasingly relevant for all businesses, it does pose challenges. EU lawmakers have established a high watermark for global data protection regulation, the cost of which getting to a point of full compliance and ensuring that they stay there will be substantial. At the same time, for those companies that embrace the challenge and implement the requirements effectively, we consider that they will be more secure, have a better understanding of the cyber-risk exposure and be able to leverage brand loyalty through taking customer privacy seriously giving them a competitive advantage.

Initially, the primary winners of GDPR will be consumers rather than business, but in the long-run there is an opportunity that it will incentivize increased transparency and competition in the market. Those companies that operate across several different jurisdictions will also benefit for the streamlined compliance process. By fully embracing such a high standard of practice on data governance, international companies can be confident that their compliance will passport to all of their global operations, thereby avoiding the headache of patchwork regulatory requirements that are currently in place.

It has been reported that a minority of companies will be ready for GDPR on 25 May 2018, but similarly data regulators have said that they will not be conducting a witch-hunt come "G-day", but rather giving an initial grace period

Continued

to accommodate for this. At the same time, given the scale of change that may be required for those companies that have not taken data protection seriously up until now, the time it will take to reform practices and become fully compliant may extend beyond this grace period.

Top engagement questions for companies:

- Will you be fully GDPR compliant by 25 May 2018?
- If not, where is there still work to do? When will this work be completed?

Governance/Oversight:

- How does the Board monitor data privacy / cybersecurity issues?
- Is there to be sufficient Board expertise on data issues to be able to provide effective oversight?
- Have you appointed a Data Protection Officer? Who do they report to?
- Do you have a breach notification procedure established? Have you rehearsed it?

Products/Operations:

- Do you foresee any product lines being adversely affected by new restrictions on data use?
- Are you able to meet potential demands to report on data use to customers or delete data altogether?
- Do you have a policy of 'privacy by design'?

Cybersecurity:

- Who is responsible for cybersecurity? Is it included within your Enterprise Risk Management system?
- Have you adopted any industry standards for cyber risk management, i.e. ISO 27001?
- Do you stress-test your data security systems?

What due diligence do you undertake on third-party data processors / technology vendors?

Given the stakes involved, a key question as far as we are concerned is how companies, and in particular their boards, will effectively oversee their GDPR compliance and data protection procedures. In particular, explicit provisions regarding the introduction of a DPO role need to be tailored by each company into its existing management reporting lines. Other requirements, such as injecting data privacy into company culture and the 72 hour breach reporting requirement, also have immediate corporate governance implications on its cyber-risk management.

Cyber risk is an important and emerging consideration across all sectors, with GDPR drawing a clear line in the sand on what is expected from companies to navigate these waters. Therefore, we will continue engaging with both leading and lagging companies to help drive stronger practices across in this area.

Continued

How can BMO Global Asset Management help?

BMO Global Asset Management has a range of approaches that can help clients to address climate change risks and opportunities in their portfolios.

- We offer an engagement service, ***reo***®, which can be applied as an overlay to any existing equities or bonds portfolios. Within this, we are running a multi-year engagement program focused on climate risk, asking companies to develop and disclose strategies on climate transition, in line with the Taskforce recommendations.
- Our **Responsible Funds range** have a comprehensive strategy which sets out how they support the transition to a low-carbon global economy, including divestment of companies with fossil fuel reserves, positive investment in solutions, engagement, and carbon footprinting.
- We also run **green bonds mandates** for clients, investing in a carefully-screened selection of bonds where revenues are directed towards climate and environmental solutions, so allowing clients to direct capital directly toward the low-carbon transition.

Contact us to find out more.

Awards

F&C Responsible Global Equity Fund* named:

- Best Sustainable Investment Fund by Investment Week
- Best Ethical/SRI Equity Fund by Money Observer

* The BMO AM Responsible Global Equity ESG Fund is available to Canadian institutional investors and managed using a similar strategy to the F&C Responsible Global Equity Fund.