MARSH

INSIGHTS | JULY 2020

Two Years On, the GDPR Continues to Shape Global Data Privacy Regulation

When the EU General Data Protection Regulation (GDPR) took effect on May 25, 2018, it marked a turning point in data privacy regulation. Two years on, the GDPR has undergone its first major review, and its report card is mixed. At the same time, the GDPR has been a catalyst for privacy regulation in other global jurisdictions.

Evaluation cites successes, and need to improve harmonization

The scheduled two-year evaluation report by the European Commission (EC), published June 24, 2020, heralds the GDPR's success in strengthening individuals' rights to personal data protection. It also finds that the GDPR is proving flexible to support digital solutions in unforeseen circumstances, such as the development of tracing apps during the COVID-19 pandemic.

The report does not call for revising the regulations, but does say it is too soon to draw definitive conclusions about application of the GDPR, and acknowledges a number of areas for improvement.

One such area is harmonization across member states. While coordination is increasing, the report finds continued fragmentation between data protection authorities, and notes that the development of a common European data-protection culture is ongoing.

"Further progress is needed to make the handling of cross-border cases more efficient and harmonized," the report states. It adds that there have been occasions when "finding a common approach" to joint operations and investigations "meant moving to the lowest common denominator" and resulted in missed opportunities to foster harmonization.

Additionally, the evaluation notes the existence of "inconsistencies" between guidelines provided by the European Data Protection Board (EDPB) and at the national level, and emphasizes the need for Member States to "allocate sufficient human, financial and technical resources to national data protection authorities" so that they can effectively perform their work and to ensure that national guidelines are fully consistent with those issued by the EDPB.

It also recognizes the challenges the GDPR may present for small and medium sized enterprises (SMEs), and calls for "intensified and widespread" provision of tools and initiatives by data protection authorities to help support SME compliance efforts.

Pragmatic enforcement

When introduced in 2018, the GDPR was a ground-breaking data privacy law, marking a global shift towards more aggressive data privacy laws and enforcement. In addition to harmonizing data protection laws in the EU, the GDPR significantly raised the bar for privacy rights, and armed data protection and privacy regulators with new enforcement powers and penalties – fines can be up to €20m or up to 4% of an organization's annual worldwide turnover, whichever is greater.

However, early fears of widespread mega-GDPR fines have yet to be realized. There have been a few large penalties – such as a €50 million fine in France and two yet to be finalized fines in the UK of £183 and £99 million – but these have been the exception, not the rule.

In the first 18 months that the GDPR was effective, regulators have generally demonstrated a pragmatic approach. Between May 2018 and November 2019, 22 European Union/European Economic Area (EEA) data protection authorities issued 785 fines, according to the EC's report.

While regulators have the power to levy significant penalties, the majority of data breaches are being resolved without large penalties. However, although regulators were initially lenient while the new rules were being absorbed and adapted to, stricter enforcement is to be expected going forward.

The impact of the GDPR can be seen in cyber insurance claims. There has been an uptick in data privacy losses in Europe, based on Marsh clients' experience, but business interruption incidents like ransomware attacks continue to account for the lion's share of large cyber event losses in Europe. Still, data breaches, while generally resulting in lower losses than other cyber events such as business interruption, require more work by organizations to prepare for and respond to under GDPR requirements.

Interpreting principle-based regulation

While far-reaching, the GDPR is principle-based, not prescriptive. As a result, the past two years have been a learning curve for both businesses and regulators as the rules are calibrated. There remains a degree of uncertainty as to how the rules are interpreted and how fines are calculated and imposed under GDPR. GDPR enforcement is not yet uniform across EU member states, and national regulators have taken divergent approaches to equivalent breaches.

There is also uncertainty around the business exposure risk posed by data privacy litigation under GDPR. In the UK, several high profile data breaches under the GDPR have resulted in collective legal actions, although Continental Europe does not currently mirror this trend. It also remains to be seen whether data breach litigation will ultimately be successful and how courts will interpret the law and calculate damages, in particular regarding non-material damage, such as distress.

Overall, the EC report finds that citizens are empowered and aware of their rights under the GDPR, but that more can be done to help individuals exercise their rights, notably the right to data portability. The jury is still out on whether the GDPR will ultimately be as effective as intended in protecting the fundamental rights of individuals and giving them greater control and choice over how their personal data is used.

Even as the process of calibrating the GDPR continues, new interpretations or changes to international data privacy laws are likely, in particular with increasing business reliance on technology and continued changes in consumer behavior. For example, COVID-19 is widely expected to accelerate the use of technology and personal data by public and private sector institutions, while challenges posed by Artificial Intelligence and machine learning still lie ahead. Where businesses previously may have had years to adapt to the GDPR, with the changes that COVID-19 is bringing to business operations and virtual workplaces, they may find that timeframe to be significantly shorter.

Spurring Global Regulations

Even as interpretation and enforcement of the GDPR continues to evolve, it has put data privacy squarely on the global map. In nearly every region around the world, regulators are drafting or implementing new and enhanced rules, increasing their enforcement powers along with individuals' rights. In its evaluation report, the EC called the GDPR a "reference point" and a "catalyst" for many countries and states around the world considering how to introduce or modernize their privacy rules.

Some countries are establishing new data privacy laws and enforcement agencies for the first time, while others are overhauling existing laws, which in some instances are decades old. While there are variations, these data protection laws follow common themes — increased privacy rights for consumers, new and/or stricter obligations for businesses, and greater powers for regulators. Following is a summary of notable developments in a number of countries. (Please note this is not an exhaustive list.)

US/California

While there is no overarching federal data privacy law in the US, individual states are beefing up their laws. One of the most significant data privacy laws passed after GDPR implementation is the California Consumer Privacy Act (CCPA). The CCPA became effective on January 1 and enforced as of July 1, 2020, and enacts some of the broadest privacy protections in the US. Much like the GDPR, the CCPA introduces new privacy rights for consumers, with significant financial implications for non-compliance and the risk of legal private right of action in the event of a data breach. Other states are expected to eventually adopt similar laws.

Following its recent enactment, California is already considering steps to amend the CCPA. A California ballot initiative for November 2020 — the California Privacy Rights Act (CPRA) — would strengthen the CCPA. The measure would expand and add rights for individuals, including establishing a new category of protected "sensitive personal information," granting right of data correction, and tripling fines for violations of children's data, as well as adding requirements for businesses. If passed, the CPRA would establish a separate enforcement agency, whereas the CCPA is enforceable by the California Attorney General.

Canada

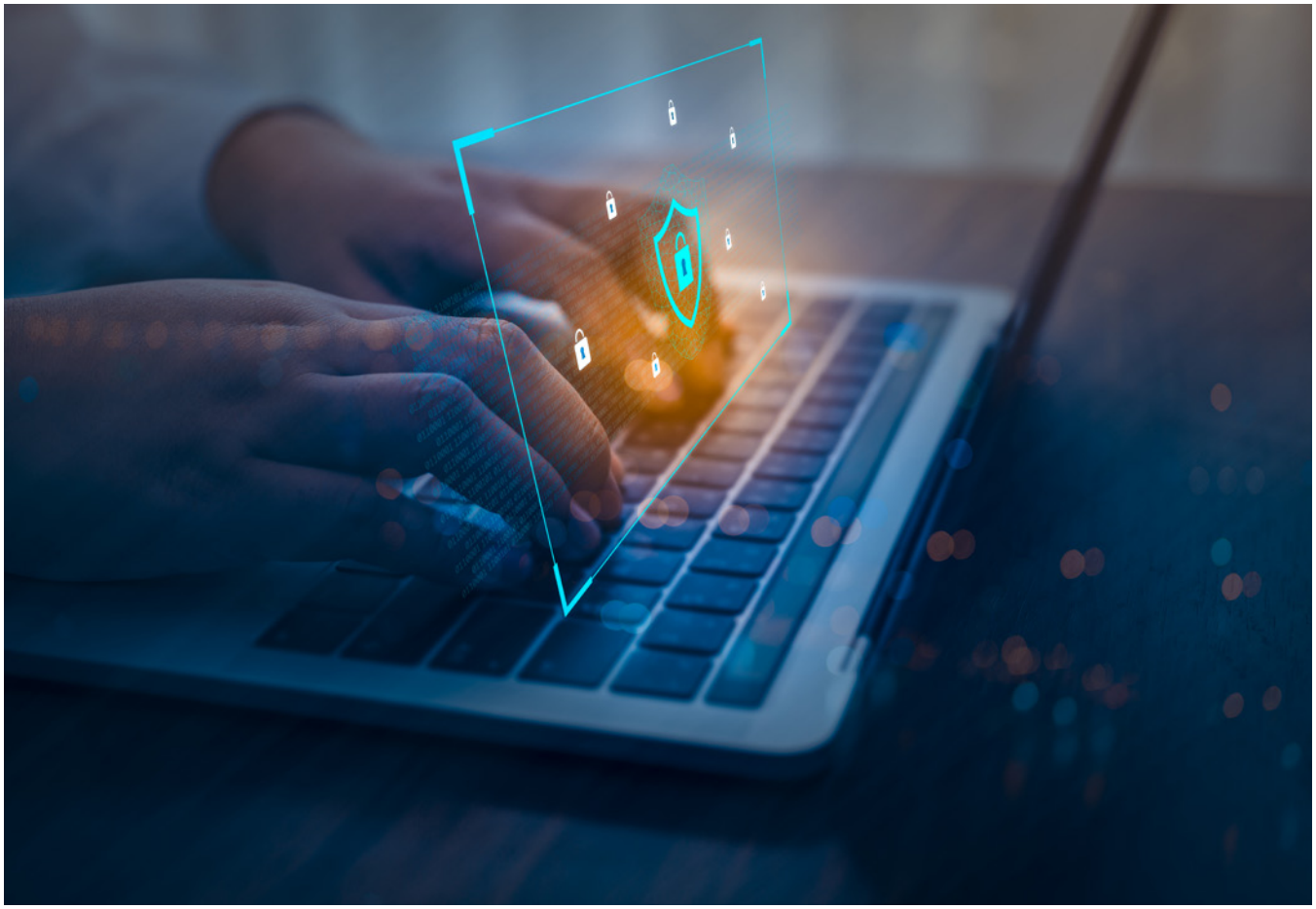
Canada is in the process of updating its federal data privacy laws in what is likely to be the biggest change to the country's data protection and privacy laws in almost 20 years. Last year the government published its landmark *Digital Charter*, which kick-started the process of modernizing the country's main data privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA). The drafting of legislation and implementation will likely take years, not months. However, current proposals would significantly broaden the scope of federal privacy law in Canada and give far greater enforcement powers and resources to the regulator, the Privacy Commissioner of Canada.

There are also significant proposed changes to certain provincial privacy laws, notably in British Columbia and Quebec.

Significant privacy legislation reforms have been tabled at the National Assembly of Quebec. If passed, Bill 64, *'An Act To Modernize Legislative Provisions As Regards The Protection Of Personal Information'*, would impose potentially severe monetary penalties, statutory damages, a security incident reporting regime, new statutory rights, and a range of other amendments affecting private sector organizations. The British Columbia Legislature also has appointed a special committee to review the province's Personal Information Protection Act, the private sector privacy law applicable to British Columbia organizations.

Brazil

Brazil was one of the first countries to closely emulate the EU's GDPR when it passed Lei Geral de Proteção de Dados (LGPD), its first comprehensive data protection regulation, in August 2018. The legislation was due to come into force this year, but will be delayed until 2021 because of COVID-19 related regulatory changes. It will establish a new National Data Protection Authority, create fundamental rights for individuals, and require businesses to report data breaches. Like the GDPR, the LGPD is extra-territorial in its reach, as it applies to any business processing the personal data of Brazilians, regardless of where the organization is located.



Australia

In December 2019, the Australian government committed to a review of the country's data privacy law, the Privacy Act 1988. Australia introduced tough data breach notification requirements in 2018. The latest proposals would establish more stringent laws regarding organizations' use of data. The review, due to be completed in 2021, will, for example, consider broadening the definition of personal information under the Privacy Act, and consider concepts such as consent and the right to be forgotten. In February 2020, the Office of the Australian Information Commissioner — which has long called for a reform of privacy laws and greater enforcement powers — released guidelines for the Consumer Data Right system, which has strengthened consumers' rights to control and use their data, starting with the banking sector.

New Zealand

New Zealand's long-awaited Privacy Bill was passed through Parliament in late June and is due to be implemented on December 1, 2020. The bill ushers in a new era for privacy in New Zealand that will promote data transparency and accountability across the whole economy. Among the key reforms is the introduction of mandatory notification of harmful privacy breaches which follows data protection standards in overseas jurisdictions, such as the GDPR. This measure means that if organizations have a privacy breach that poses a risk of serious harm, they are required by law to notify the Privacy Commissioner and affected parties; a data breach would require much more attention, time, and resources to both investigate and respond to.

India

India introduced its first-ever comprehensive data privacy law, the Personal Data Protection Bill, in 2018, although the proposed legislation has undergone material changes since. The bill, yet to pass, is based largely on the GDPR and contains many similar concepts, including breach notification requirements, rights for data subjects, and an extra-territorial scope. It also envisages the creation of a new regulator, the Data Protection Authority of India, with substantial enforcement powers.

Singapore

Singapore's Ministry of Communications and Information (MCI) and the Personal Data Protection Commission (PDPC) launched a public consultation in May 2020, on proposed amendments to the Personal Data Protection Act (PDPA), the first comprehensive review of the PDPA since its enactment in 2012.

Key proposed amendments include the increment of financial penalties and enhanced enforcement powers for the PDPC. Currently, organizations in breach of the PDPA are liable for financial penalties of up to S$1 million. The draft bill outlines a maximum financial penalty of the greater of 10% of an organization's annual turnover or S$1 million.

Currently there is no express requirement in the PDPA for organizations to notify the PDPC or any other party of a data breach. Proposed changes include a mandatory notification regime which requires organizations to notify the PDPC and the affected individuals of notifiable data breaches within a specified timeline.

Thailand

Thailand's Personal Data Protection Act (PDPA) was published on May 27, 2019, with most provisions effective a year later, although the government has temporarily postponed its application due to COVID-19. The PDPA, which has extra-territorial jurisdiction, includes provisions on collecting, consent, use, and disclosure of personal data; rights of data subjects; liabilities; and penalties. The PDPA allows for fines ranging from THB 500,000 to THB 5 million, as well as criminal penalties — including up to one year imprisonment — and civil liabilities, including punitive damages of up to twice the value of the actual damage.

China

There is no single comprehensive law on data privacy in China. Data privacy and regulation is covered under a number of sector-specific, consumer, and cybersecurity laws and regulations regarding data handling practices, supplemented by a number of non-binding national standards. However, in December 2019, Chinese authorities announced that the enactment of new Personal Data Protection Law and a new Data Security Law would be a matter of priority in 2020. It is expected that the legislation will consolidate existing data protection principles in China.

Vietnam

In December 2019, Vietnam's Ministry of Public Security (MPS) published a draft Decree on Personal Data Protection, which sets out some principles of personal data protection and the obligations of personal data processors. Future versions are expected to include the rights and obligations of data subjects, scope of activities, measures to protect personal data, and establishment of competent authorities responsible for personal information protection.

Data localization is a requirement for both foreign and domestic online service providers that store the personal data of Vietnamese citizens, requiring them to hold such data in Vietnam. Offshore service providers are required to open branches or representative offices in Vietnam to meet the data localization laws and comply with cybersecurity laws. The scope of the law encompasses disparaging or anti-government posts and content deemed as "prohibitive"— violators could face censorship under the law.

South Korea

South Korea's Personal Information Protection Act (PIPA) imposes strict security requirements on organizations that hold or process personal data, and places tight limits on the sharing and use of such data. In January 2020, the government amended PIPA to clarify the concept of personal data and strengthened the regulator's powers. The country is in the process of rolling out the Cyber Liability Insurance Regulation, which requires companies operating in certain sectors — including financial institutions and information communication service providers — to carry cyber liability insurance or alternative means to compensate damages.

Monitoring and preparing for more regulation

It's likely that the wave of regulatory momentum will continue as nations respond to consumers' expectations and demands for protection and control of personal data. The standards and requirements in the many of these national and regional privacy regulations are not uniform.

In this fast evolving regulatory landscape, organizations must stay informed, continually assess which regulations they are subject to, and implement compliance action plans that include an assessment of related enterprise risk. Doing so for new regulations may be a lighter lift for those organizations that have already performed this exercise for GDPR, CCPA, or other regulations. Even companies that are not subject to individual new regulations should assess their data collection practices as there is a strong likelihood that more nations and states may soon pass their own legislation.

Risk professionals should consult their advisors and insurance brokers about adopting insurance policy terms and conditions to address their organizations' widening exposures. Companies should review applicable insurance wordings, with a particular focus on the potential insurability of fines, penalties, and financial liabilities. While the ultimate determination of insurability will likely be determined by the courts, organizations should seek policy wording that offers the best chance for recovery.

For more information on how increasing privacy and data regulation may affect your risk profile, or for market-leading advisory and solutions to manage cyber risk, contact cyber.risk@marsh.com or your local Marsh representative.

Marsh Cyber Risk Management By the Numbers