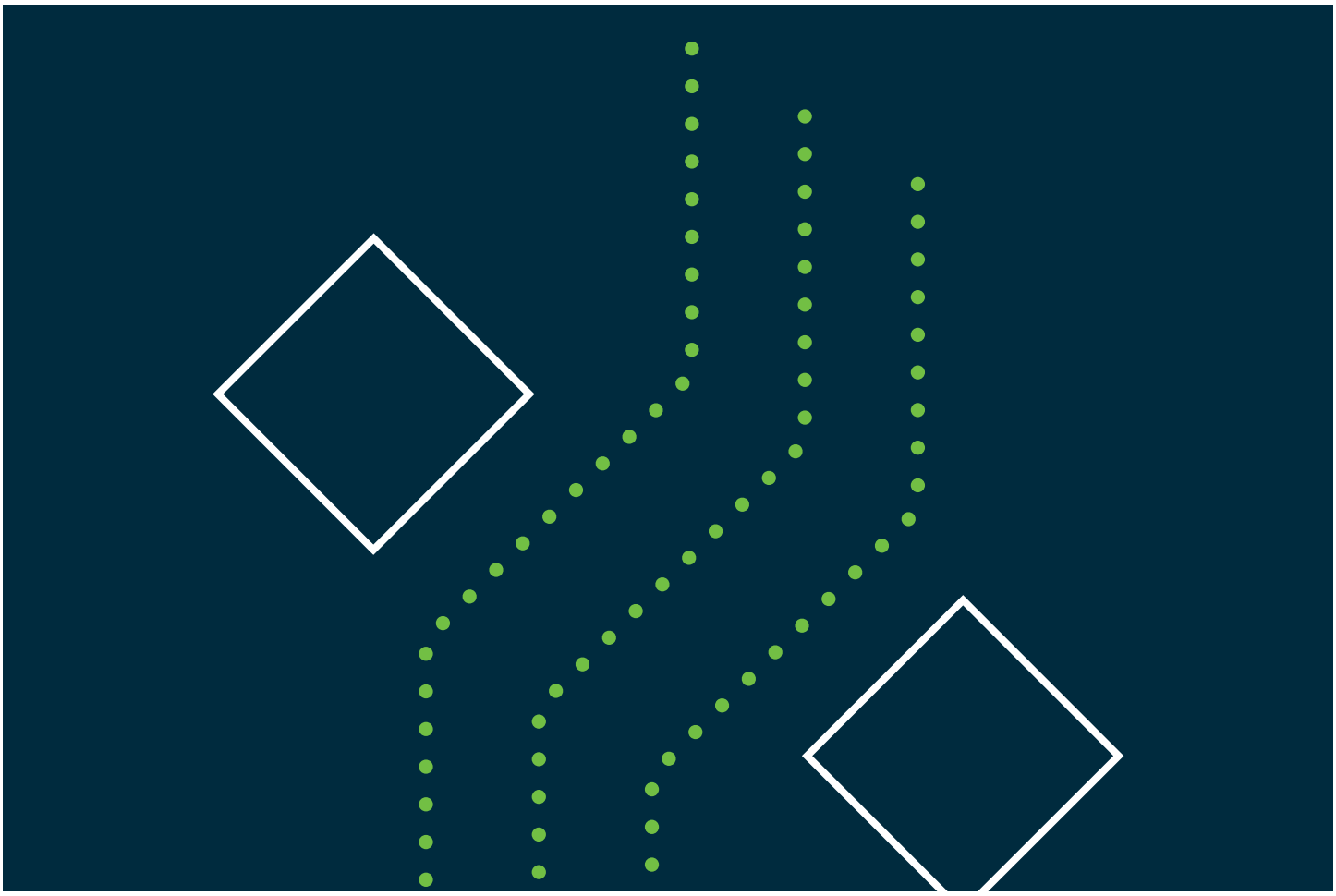
Collibra

Whitepaper

Data privacy regulation

Preparing for change

Written January 2019, Refreshed December 2019



Suddenly it seems as though everyone is worried about data privacy. A wave of scandals has hit companies around the world, including cyberattacks in which personal data was stolen and instances when personal data was misused within an organization, or by a third-party supplier. As well, individuals are starting to realize that they may have certain rights associated with their own personal data, and that their data needs to be protected.

GDPR builds on work that the OECD has been doing for a long time

In response, governments and politicians are working fast to create or update their regulatory programs to cope with these seismic changes in the data privacy ecosystem. This whitepaper explores how data privacy regulation has evolved over the past few years, including initiatives such as the EU's General Data Protection Regulation (GDPR). Next, the paper looks at the way in which jurisdictions around the world are implementing these new data privacy regulatory frameworks. Lastly, the paper examines some nascent trends that are shaping the data privacy regulatory environment.

In this area of regulation, it is almost impossible to make solid predictions about how data privacy rules will evolve, even over just the next five years. However, it's clear that companies are going to have to be nimble – prepared for rapid regulatory change within their data privacy programs – to accommodate an ecosystem that will probably develop in some unexpected ways.

The rules on the books

While it can sometimes seem as if the EU's GDPR is portrayed as a surprise asteroid smashing into Earth, the truth is that these rules are the outcome of years of work by both governments and the private sector on three related themes – data privacy, protecting individual rights related to data and ensuring data security for personal data. All three of these themes are found within what are normally called "data privacy rules."

For example, GDPR builds on work that the OECD has been doing for a long time. Because the OECD's membership is composed of governments, the body's work has a public policy perspective, with particular emphasis on protecting the rights of the individual. In 2013, the international body published its OECD Privacy Framework, which significantly updated a previous document from 1980. Many of the ideas in this document – such as data breach reporting, privacy by design and privacy risk assessments were included in the GDPR.

The World Economic Forum (WEF) – which meets each winter in Davos, Switzerland – has also put considerable focus on data privacy, alongside related issues such as digital identity and cybersecurity. The WEF is a forum for the world's 1000 largest companies to come together and discuss significant global issues, so the issue of data privacy is talked about in a broad context of both technological innovation and social good. For example, in December 2018 the WEF published *Our Shared Digital Future: Building an Inclusive, Trustworthy and Sustainable Digital Society*. In the report, the WEF says it wishes to work with governments and regulators to create "a common and consistent risk-based framework" by helping "policy-makers identify and understand objective privacy risks to individuals" as well as support "policy-makers with insights and tools that enable outcome-based policy approaches with measurable results rather than rigid compliance checklists."

Like many other new regulatory frameworks today, the GDPR says it is structured on a risk-based approach

Certainly, to date the EU's GDPR is the most well-known result of the work that governments and the private sector have completed on data privacy. The regulation is substantial and complex, and although the compliance deadline was May 2018, many companies are still struggling to meet its requirements. According to the recent IAPP-EY Annual Governance Report 2018, fewer than 50% of survey respondents said they are "fully compliant" with the GDPR. Key elements of the GDPR include:

- The extraterritoriality – all organizations that process the personal data of EU citizens are impacted
- Data protection impact assessments
- Privacy by design
- Data breach reporting
- Rights of individuals around their personal data, such as access requests
- Data protection officers
- Significant fines for compliance failures

Like many other new regulatory frameworks today, the GDPR says it is structured on a risk-based approach, which means the rules were developed based on the risks that companies, governments and individuals face around data privacy. The California Consumer Privacy Act (CCPA), which goes into effect on January 1, 2020, is the next big piece of personal data privacy regulation to hit companies. Measured on its own, the state of California's economy is the fifth largest in the world, so the new regulation will be impactful. There are numerous differences between the CCPA and the GDPR, although overall the two regulations are similar and are fairly consistent in their general approach.

Other recent data privacy regulations include:

- Argentina – A data privacy law that updates its existing legal framework, and brings it more into alignment with the GDPR, is in the process of passage.
- Australia – At the moment, the country has a patchwork of data privacy rules, but it implemented a data breach reporting law in 2017.
- Brazil – The country updated its data privacy regulations in August 2018.
- New York State – The American state has a new cybersecurity regulation for financial institutions; the regulation has data privacy elements such as data breach reporting and data privacy policies.
- South Africa – The Protection of Personal Information Act, which has many elements of the GDPR, has taken the government some time to fully roll out, but it looks like the regulator will be up and running during 2019.

Over the next few years most countries are expected to work on updating their data privacy regulatory frameworks

Although many of these new data privacy rules are said to be very much like the GDPR, most have significant national differences from the EU's regulation, making multi-jurisdictional compliance a real headache for many companies.

In short, there is an international effort to improve data privacy, ensure citizens retain their rights around their own personal data and enhance data security around personal data. The EU's GDPR represents the first big success of this movement, although other jurisdictions have also begun to implement either the entire GDPR framework or chunks of it. For data privacy regulation, it is still very early days.

The rules in the pipeline

Over the next few years most countries are expected to work on updating their data privacy regulatory frameworks, spurred on by the growing global momentum to do so. However, international companies need to be prepared for these changes to be piecemeal and complex. While people may speak of a country implementing "GDPR," the reality of what is being done can often be much more complicated.

To begin, the updating of national rules needs to be taken in the context of the three strands of the greater international initiative – data privacy, protection of individual rights related to data and assurance of the data security of personal data. How these strands are enacted in individual jurisdictions could be radically different. For example, some GDPR-like rules may be found within cybersecurity regulation in some countries or in industry standards about the treatment of customers in other countries. Each company will have to discern where data privacy rules are housed within each jurisdiction it operates.

Secondly, organizations should be prepared for jurisdictions to implement pieces of data privacy separately. For example, over the past two years, many countries have adopted data breach reporting rules, and this remains a very fast developing area of data privacy law. However, the majority of jurisdictions that have brought in a data breach reporting rule have not adopted most other aspects of a GDPR-like approach yet. For instance, it was only in March of 2018 that all 50 US states had data breach reporting rules and only California has adopted the rest of a GDPR-style data privacy framework. Organizations should expect more countries to adopt data breach reporting requirements – it is a straightforward aspect of data privacy regulation to put in place and it supports both international regulatory cooperation and cybersecurity initiatives. Still, other aspects of a data privacy framework in a particular country could arrive later, in pieces.

Thirdly, most countries will claim their new rules are like the GDPR, and in conceptualization they may be. However, in practice individual jurisdictions will tweak the legal template that the GDPR provides to fit their own culture, legal framework and technological sophistication. For example, some countries – like Singapore – are already thinking about how to regulate personal data when used in artificial intelligence (AI). In other countries, internet use may still be relatively low among the population as a whole. Data privacy regulations need to reflect these contexts. Countries that seek to update their personal data privacy frameworks include:

- **Canada** – The country's privacy commissioner issued **updated guidelines for obtaining meaningful consent** that took effect on January 1, 2019. The regulator is also pushing for the **government to update** its data privacy legislation.
- **Hong Kong** – The **Privacy Commissioner for Personal Data** is reviewing the jurisdiction's regulations in the wake of the Cathay Pacific data breach. New regulations could be put forward in 2019.
- **India** – A new draft bill, which has many GDPR-like elements, is scheduled to be put in front of its parliament in the summer of 2019.
- **Singapore** – The country issued **two consultations** over the past two years with a view to eventually overhauling chunks of its existing data privacy framework.
- **United States** – A patchwork of data privacy regulation exists across the US, putting pressure on the federal government to get a more coherent, nationwide framework in place. Currently, all states have some form of data privacy regulation and industry regulators at both the state and national levels also often have their own rules. This is a complex and expensive environment for firms to seek compliance within. Recently, big technology companies have started lobbying the federal government to try and shape **potential national data privacy legislation**. However, timing remains uncertain due to the current domestic political climate. In the meantime, expect individual states and industry regulators to update their own approaches.

In summary, international companies can expect regulatory change around data privacy rules to be fairly constant over the next few years. Adoption of "GDPR-like" frameworks will happen at different speeds and in different ways in each jurisdiction. Nonetheless, the general direction is towards GDPR-style frameworks and, over time, these will become predominant.

Data privacy in 5 years' time

The general direction is towards GDPR-style frameworks and, over time, these will become predominant

Just what data privacy regulation will look like in five years' time is difficult to predict. However, key themes that will impact the way regulations take shape include:

- **Increased collaboration among regulators** – Data privacy regulators around the globe are actively seeking to work more closely together both in terms of the rules they write, and the way they enforce them. This momentum for closer collaboration is supported by both the OECD and the World Economic Forum – both say that data privacy is a global issue that needs a more coordinated approach. Within this larger trend, some sub-themes include:
  - **Similar regulations** – Business communities and information commissioners are interested in having a more joined-up approach to data privacy regulation. Today's diverse mix of rules is costly for businesses to comply with and complex to enforce. However, it may take some time to achieve the practice of aligning regulation.
  - **National coordination** – The OECD is keen to ensure that individual countries have a national privacy strategy that is coordinated at the top of government. As a result, organizations can expect to see more communication between their industry regulators and their national data privacy regulator, for example.
  - **Communication on enforcement** – Several initiatives are already underway – for instance, in 2017 the International Conference of Data Privacy and Protection Commissioners adopted a new Enforcement Cooperation Arrangement, which addresses information sharing of enforcement related information among members.
- Having regulators act in a more coordinated way can have significant benefits for business, because it can reduce compliance cost and complexity. However, more coordination could also result in a stronger expression of enforcement, as regulators share information and insights about the international companies they regulate.
- **Greater understanding of personal data risks among the public** – Awareness of the risks associated with data privacy is growing among the general public. Organizations can expect to see this awareness escalate significantly in the next five years for several reasons:
  - **Awareness as a policy goal** – The OECD is actively encouraging governments to educate citizens about data privacy risks. Many governments have either started or enhanced their awareness campaigns over the past couple of years.

  - **Expansion of pressure groups** – Organizations are being founded, or expanded, with a focus on campaigning for greater data privacy rights for individuals and uncovering misuse of personal data. **Privacy International** is one such organization. Expect the number and impact of these groups on the regulatory environment to grow.

  - **Attention in the media** – Traditional media, online media and social media all spread stories of personal data misuse and the regulatory activities associated with them. The general public pays a lot of attention to allegations and this attention will only grow as a result of the above two trends.

- The greater understanding of personal data risks that these trends will foster will create new expectations that companies will be ethical in their approach to data privacy. It will also increase pressure on regulators to punish wrongdoing and evolve data privacy rules where they are deemed to be insufficient to safeguard the public.

- **Acceleration of technological innovation** – Exciting new applications of machine learning (ML), artificial intelligence (AI) and Internet of Things (IoT) technologies are creating regulatory challenges. Rule makers and standard-setters are working to get to grips with what data privacy regulation within these innovative technologies should look like. For example, the EU is developing **Ethics Guidelines for Trustworthy AI** and expects to have the final document published in March 2019. This initiative is rooted in the concept of the Single Digital Market, which also yielded the GDPR. For all governments looking at the risks new technology might bring, worries include:

  - Misuse of personal data on purpose within an innovation

  - Unintended consequences of a mistake that involves personal data in innovation

  - Potential vulnerability of personal data in an innovation to criminal activity

- In some industries, regulators have chosen to engage in dialog – for example, the UK's Financial Conduct Authority (FCA) Fintech program, **FCA Innovate** – to try and work through the challenges that innovation can create. However, this level of positive engagement between industry and rule-setters doesn't exist everywhere. Companies should be prepared for increased interest from regulators in the innovations they are pursuing. Organizations should also expect additional regulations around personal data use in innovations over the next five years – particularly if there is a high-profile negative incident.

- On the positive side of things, emerging technologies could also help companies better manage data privacy, protect personal data rights and keep personal data secure. Companies that embrace technological approaches to better manage data privacy may very well see their proactive engagement transform into increased customer trust and improved revenues. One such program is the **Platform for Good Digital Identity**, which seeks to develop new, safer forms of digital identities. Another, launched by Tim Berners-Lee in September, is called **Solid**. This approach seeks to help individuals truly own their personal data and exercise their rights around it.

- **Rising expectation of an ethical, strategic approach among companies** – The OECD is actively pursuing the concept of "privacy management programs" within companies, in the development of data privacy regulation. These programs should have a focus on accountability for data privacy through a governance, risk and compliance (GRC) approach. Boards and senior management should own data privacy within a company, and be strategic in their thinking about it. Taking this further, regulators and other standard-setters are beginning to talk about the "data culture" that an organization has, particularly around data privacy. For organizations, having the right data privacy culture will mean being perceived as treating personal data ethically and being able to demonstrate to regulators, customers, third party suppliers, and others that they are doing so. Organizations should expect regulators to not just review evidence of compliance, but also to begin to evaluate data culture, too.

Taking this further, regulators and other standard-setters are beginning to talk about the "data culture" that an organization has

In summary, over the next five years, companies can expect data privacy regulation to evolve in new and provocative ways in response to a number of changing conditions. It can be difficult to predict just how regulation will evolve – many of these factors are still in the infancy stage of development. However, companies need to be prepared for change to happen quickly at times, in response to technological disruption, crime associated with personal data, and other factors. Organizations will need to be nimble in their overall approach to data privacy to thrive in this environment.

Conclusion

Regulation of data privacy, individuals' rights around their personal data and personal data security are evolving rapidly and will continue to do so. Although there is a perception that jurisdictions are adopting GDPR-style frameworks – and most probably will – on closer inspection, the reality is more complex. Adoption is fragmented in many ways and is likely to create significant challenges around regulatory change for companies. The medium-term outlook for data privacy regulation is also unclear because the full impact of significant trends that will shape rulemaking has yet to be felt.

For companies to thrive in this climate, they will need to adopt a best practice approach to data privacy that is flexible enough to support ongoing regulatory change across the jurisdictions within they operate – with minimal operational disruption. Traditional, manual approaches to managing data privacy or project-based compliance efforts will, over time, extract a high price from the organizations that choose such a methodology. Instead, companies should seek to take a more proactive approach that is underpinned by positive engagement with regulators, technological solutions that will support the business and a data culture that emphasizes the ethical treatment of personal data.

For additional questions, contact us at:

United States
+1 646 893 3042

United Kingdom
+44 203 695 6965

All other locations
+32 2 894 79 60

By email
info@collibra.com