AN FTI CONSULTING REPORT – PUBLISHED 11/15/2022

Privacy as a Lingua Franca?

Translating the Increasing Alignment and Divergence in Global Data Protection Regulation.

By FTI Technology authors:

- **Ben Crew**, Senior Director, Middle East & North Africa
- **Tim de Sousa**, Senior Director, Australia & New Zealand
- **Eric Pulsipher**, Senior Director, North America
- **Ana Jankov**, Senior Director, Europe
- **Frances Chen**, Senior Director, Asia Pacific

Two years from now, roughly 75% of the world's population will be protected by at least one data privacy or data protection law (Gartner). With more than 130 data protection regulations already in place and more emerging all the time, achieving and maintaining privacy compliance has become one of the most challenging imperatives in global business today. Few issues in modern society have achieved such widespread attention and global turbulence and the rate of change doesn't show any signs of slowing.

In many ways, the evolution of data privacy laws is driving a common language, a shared approach recognised and welcomed by regulatory bodies, governments and citizens in nearly every country. Indeed, jurisdictions with federal data privacy and protection laws in place now outnumber those that do not. However the privacy landscape is not static and for all the alignment between jurisdictions, a significant measure of inconsistency remains.

Across continents, there are several countries in the preparation or implementation phases of their own iterations of federal privacy laws, including Egypt, UAE, Saudi Arabia, Oman, and numerous jurisdictions in Africa, Asia and the Americas. Notably, the American Data Privacy and Protection Act (ADPPA), a landmark U.S. federal privacy bill, is advancing through the legislature. Its adoption would bring the first federal privacy law in the U.S. Adding to the assortment of federal laws is a labyrinth of sector-specific or regional privacy laws.

Common Fundamentals

In this landscape, the question for most multi-national organisations becomes, "how can our organisation keep pace with the growing number of laws?" and "is compliance possible?".

The answer is a tentative yes, but reaching such level of compliance requires a look at the fundamentals. Broadly, the conceptual structure of all the laws is similar. If organisations address these foundational concepts at a global level, then they will only need to face relatively minor variations at the applicable local levels. Key fundamentals that persist across most major data privacy and data protection regulations include:

— **Transparency** regarding how data is collected, accessed, managed and used. Privacy policies and notices are standard in most jurisdictions, so addressing this at a global level provides a consistent baseline.

— **Data protection.** Every single data privacy law globally requires that organisations ensure the security of the personal data the process, store and collect.

— **Knowledge and documentation of data processing activities.** Organisations that collect personal data are obligated to understand, properly classify and record use of all personal data that is captured. Under GDPR and many other laws, this is accounted for in the mandatory Record of Processing Activity (ROPA) requirement.

— **Notification** of data subjects and/or data privacy authorities in the event of a data breach. In jurisdictions where this is not required, it is highly likely that a notification will still be required to some data subjects due to the extra-territorial nature of certain laws, including GDPR.

— **Data minimization.** The concept that data may only be retained for as long as it is being used for the reason it was collected, or another legally justifiable reason, is persistent across data privacy laws.

— **Privacy by default and privacy by design.** While this requirement does not currently apply globally, a privacy by default and design strategy ensures that data privacy considerations are baked into products and business practices at the foundation, which avoids the need to retrofit them later on.

— **Data subject rights.** The vast majority of laws provide individual rights to data subjects, including the right to know what information has been collected from/about them and, depending on the jurisdiction, the right to request that organisations storing their data amend, correct, delete, transfer or provide a copy of the data.

— **Basis of processing.** Organisations must have a legitimate reason for processing personal data and/or obtain explicit consent from the data subject to use it.

— **Cross-border restrictions.** Every organisation transfers data, passively or actively, to multiple jurisdictions around the world. Doing so, however, is highly regulated in nearly every major jurisdiction and must be addressed in an organisation's broader data privacy programme.

— **Training.** Organisations are also obligated to provide training for their staff on data privacy and data protection.

Understanding Local Nuances

While there are many common threads between global privacy laws, organisations operating in regulated jurisdictions must also account for the nuances. Below is an overview of some of the key differences between laws across major regions.

Europe and the U.K.

GDPR is often regarded as the baseline regulation of modern data protection. The spill over of GDPR-like protections is notable in a multitude of jurisdictions across the globe, including Brazil, South Korea, UAE, California and Canada. Notable points in data protection regulation across Europe and the U.K. include:

— Extra-territoriality is an important feature of GDPR. Companies located outside the EU can be caught by GDPR if they offer goods or services to individuals in the EU, or if they monitor the behaviour of such individuals (e.g., through cookies).

— Despite Brexit, GDPR has been retained in U.K. domestic law as the UK GDPR. Initiatives to reform UK's privacy landscape, with the aim to move away from the stringent GDPR-like rules and establish more business-friendly solutions were underway, however, the U.K. government recently announced that it is pausing its data reform bill to reevaluate the GDPR replacement.

— In Russia, the data protection framework is based on the Federal Law on the Protection of Personal Data (2006) and applies to legal entities processing the personal data of Russian data subjects, including foreign companies provided that their offices are located in Russia and that they process personal data in Russia. A somewhat controversial segment of the Russian privacy law concerns the localisation rules (introduced in 2014), which require operators to store personal data of Russian nationals on servers located in Russia before any cross-border transfers.

Australia and New Zealand

Australia's Privacy Act 1988 (Cth) stands out for its broad ranging exemptions for employee records and for small businesses (i.e., businesses with a turnover of less than $3 million AUD). These exemptions are an outlier in today's

privacy landscape. However, the Act is currently under review, and there is increasing pressure to eliminate these exceptions to keep pace with global standards. Additional key nuances in the region include:

- Part IIIC of the Act establishes a mandatory data breach notification scheme, where breaches that give rise to a "likely risk" or "serious harm" must be notified to affected individuals and the regulator. In cases where the organisation is unsure of whether a data breach requires notification, the organisation must take reasonable steps to determine this within 30 days.
- New Zealand's Privacy Act was revamped in December 2020 and generally conforms to the fundamentals.

The Americas

To date, the U.S. has taken a state-by-state and industry-based approach, however the ADPPA is gaining momentum to provide privacy regulation at a federal level. Canada has long maintained its Personal Information Protection and Electronic Documents Act (PIPEDA), a federal-level privacy law that regulates cross-border data transfers and requires opt-in consent for collection, processing and disclosure of personal data.

Additional notable regulation in the Americas includes:

- President Biden recently signed an Executive Order regarding the steps the U.S. will take to implement commitments to reinstate a data privacy framework with the EU. According to the White House, these steps strengthen "an already rigorous array of privacy and civil liberties safeguards for U.S. signals intelligence activities…[it] also creates an independent and binding mechanism enabling individuals in qualifying states and regional economic integration organizations…to seek redress if they believe their personal data was collected… in a manner that violated applicable U.S. law."
- California's Privacy Acts, including the CCPA and the California Privacy Rights Act, which together offer extensive data subject rights, as well as strict definitions around what constitutes the sale of data and the establishment of the California Privacy Protection Agency.
- Colorado, Connecticut, Utah and Virginia have all passed legislation to impose certain obligations on businesses to protect the personal information of residents.
- In Canada, the provinces of Alberta, British Columbia and Quebec have their own provincial iterations of Personal Information Privacy Acts that follow PIPEDA closely but add nuances to consent. More provinces have privacy laws underway and Quebec's updated privacy laws go live in 2023.
- Most Latin American countries do not have specific or enforced privacy regulations in place yet (though more are likely on the way), with the exception of Brazil's General Data Protection Law (LGPD), which includes aggressive obligations and impacts all sectors of the country's economy.

Asia

One of the most significant developments in Asia was the enactment of China's Personal Information Protection Law (PIPL) as part of the country's data protection legal regime, which includes a myriad of other laws and industry-specific regulations. Organisations in China will also need to prepare for the following:

- Like GDPR, PIPL includes extraterritorial reach, extends to any organization or individual irrespective of the covered individual's or organisation's location in the world that handles the personal information of natural persons who are within the jurisdiction of China.
- The Cyberspace Administration of China recently unveiled the Measures for Security Assessment of Data Exports to regulate the transfer of data outside of mainland China. These measures clarify the substantive requirements in terms of the scope of application, assessment process, criteria and legal consequences of not conducting a security assessment prior to data export.
- The new data transfer measures also come with the possibility of legal liability for failure to properly comply and fulfill the assessment requirements.

Middle East

The Middle East is arguably one of the most complicated regions when it comes to data privacy regulation. In the Kingdom of Saudi Arabia, the Personal Data Protection Law has strict data localisation provisions with all personal data being required to stay in country and permission applied to transfer it outside country. Qatar's privacy regulation states that data can be transferred internationally unless there is a likelihood that the data would not be subject to the same levels of protection as those in Qatar. This places added burden on organisations to conduct transfer impact assessments thoroughly, as the responsibility is on

them to ensure the same level of protection. Additional considerations include:

- The United Arab Emirates Personal Data Protection Law (PDPL 2021) does not have a basis for processing of "legitimate business interest," which will require organisations to implement additional controls within their privacy processes and procedures. Additionally, the UAE law requires generated or derived data (including via AI) to be considered as personal data and subject to the same criteria as other personal data. The UAE is also unique in having three separate jurisdictions within the geographic constraints of the country each with unique privacy laws.
- In Egypt, the yet-to-be implemented Data Privacy Law has a requirement for all companies to appoint a data protection officer and includes criminal liabilities for the DPO in the event of a breach or incident involving personal data.

Building Blocks for Global Privacy

With an understanding of the foundational principles and major nuances around the world, organisations can begin building a resilient privacy programme that is responsive to multiple overlapping regulatory regimes. Critical steps to building such a programme include:

1. Develop an action plan. Privacy and information governance is a strategic endeavour that must be planned for the long term. Organisations can begin with a gap assessment, first in a single regime that sets a "high bar" for the baseline requirements. An action plan can be developed around the fundamentals at that high bar level.
2. Take a data inventory. It is impossible for organisations to protect data they don't know they have or data stored in unknown repositories. This is why it is critical to build a data inventory that accounts for key data assets and maps out the various flows of data in, through and out of the organisation. From there, processes and procedures can be implemented to keep the inventory accurate and up to date.
3. Classify data and develop a retention schedule. Data classification enables triage — it helps privacy teams work out what security controls should be applied to what data and what data needs to be saved. With properly classified data, a retention schedule can be set to collect and codify legal and regulatory retention obligations and operational needs and dispose of data as its use expires.
4. Minimise data holdings. Organisations can significantly reduce the risks around their data and save costs by destroying or de-identifying personal data that is no longer required for lawful business purposes.

5. Evolve the policy framework. Once the debt of legacy data has been cleared policies and processes must be established to prevent data from pilling up again in the future. Develop collection and minimisation strategies, archiving and end of life strategies and evolve them as the data landscape evolves. Teams must also ensure that the policy framework documents how the organisation is maintaining compliance across the entire data lifecycle.
6. Plan for failure. Even the best programmes can fail. So, it is critical to plan for data breaches. Develop a data breach response plan and train responders on how to use it. Running regular simulation training with the plan and reviewing and updating it annually will enable the organisation to limit the harm caused by a breach and make a full recovery.
7. Design trustworthy automation. Artificial intelligence and machine learning can be valuable tools, but like all tools, they need to be used with care. Establish processes to assess for the appropriateness of AI and ensure that decisions are explainable and aligned with best practices and local regulation.

CONCLUSION

Data privacy has become a universal concept and a universal risk in the global regulatory landscape. While it's difficult to stay apace with the changes and translate the similarities and differences from region to region, focusing on foundational principles can give organisations a baseline from which to develop their data protection strategy and policies. Working from a strong foundation, it's possible to design a programme that sets a high standard for compliance and allows for the flexibility needed to address the nuances within each jurisdiction.

About the Authors

Ben Crew is a Senior Director within FTI Consulting's Technology segment. He is a renowned expert in information governance and data privacy. He is an acknowledged privacy evangelist, with a focus on the GCC region.

Tim de Sousa is a Senior Director within FTI Consulting's Technology segment. He is a strategic privacy expert with more than 15 years' experience. He works at the intersection of privacy and information governance and his expertise spans Australia, the Asia Pacific region and Europe.

Eric Pulsipher, MBA, CEDS, CIPP/E, CIPM, is a Senior Director within FTI Consulting's Technology segment based in the U.S. He was formerly part of NBCUniversal's Privacy & Compliance team under NBCUniversal's Global Legal division. He is passionate about leveraging relevant data and tech across e-discovery, data privacy and compliance programs.

Ana Jankov is a Senior Director within FTI Consulting's Technology segment, based in Brussels. She is a data protection lawyer with 15 years' experience and has worked as an attorney at numerous top-tier law firms.

Frances Chen is a Senior Director within FTI Consulting's Technology segment, based in Shanghai. Since 2011, she has advised corporations and international law firms in developing strategies and formulating workflows for cross-border litigation and investigations and data privacy matters.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

BEN CREW
Senior Director
+971 50 286 7553
ben.crew@fticonsulting.com

TIM DE SOUSA
Senior Director
+61 2 9235 9305
tim.desousa@fticonsulting.com

ERIC PULSIPHER
Senior Director
+1 (347) 205-7515
eric.pulsipher@fticonsulting.com

ANA JANKOV
Senior Director
+32 2 289 18 04
ana.jankov@fticonsulting.com

FRANCES CHEN
Senior Director
+86 21 2315 1188
frances.chen@fticonsulting.com

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. FTI Technology is a segment within the FTI Consulting (NYSE: FCN) network of affiliated entities worldwide and is operated as a distinct legal entity in certain jurisdictions, including the U.S. and Australia. ©2022 FTI Consulting, Inc. All rights reserved. **www.fticonsulting.com**