THOMSON REUTERS

REGULATORY INTELLIGENCE

Where does privacy go from here: California, EU and Indian data privacy laws and global compliance programs

Published 05-Aug-2019 by
Alan Charles Raul, William Long, Vishnu Shankar, and Sheri Porath Rockwell

The summer of 2018 may be regarded as a pivotal time in the history of data privacy laws. The European Union's General Data Protection Regulation (GDPR) came into effect in May 2018, the California Consumer Privacy Act (CCPA) was signed into law in June 2018 (and comes into effect on January 1, 2020), and a draft of India's Personal Data Protection Bill (India DP Bill) was released in July 2018 (and is now under review by India's government).

These developments, and more generally, the recent proliferation of data privacy laws around the world (notably, in Australia, China, Brazil, Hong Kong, and Singapore) represent a compliance challenge for many multinational organizations.

Critically, many of these laws (in particular, GDPR, CCPA and the India DP bill) impose not only new and substantive obligations on organizations, but also contain real enforcement "teeth" when compared to their predecessors. For example, the GDPR, CCPA and the India DP bill all allow for the imposition of significant regulatory fines (in the case of the GDPR and India DP Bill, fines that are linked to global revenues). Indeed, recently, British Airways was fined in excess of $200 million under the GDPR by the UK data privacy regulator for cybersecurity breaches.

For many organizations, these risks are compounded by a substantial growth in:

- the volume and velocity of data that they collect from around the world;
- their globalized customer and supply chains that broaden their sources of cyber risks;
- overseas cyber threats that can unexpectedly cause "bet the company" crises; and
- the level of sensitivity regarding data misuse among their stakeholders around the world.

Collectively, these demonstrate that an organization may wish to address, as far as possible, global data privacy risks globally - rather than locally - by designing and implementing an enterprise-wide global data privacy compliance program (GDPC program). An effective GDPC program would steer away from both expensive and inefficient "bespoke" local solutions, and inflexible and potentially risky "one-size-fits-all" global solutions – all while respecting the organization's business objectives.

A key step in designing a GDPC program is to analyse the key requirements between various applicable global privacy laws to determine whether there is scope for any regulatory "arbitrage". By way of illustration, there are useful similarities between the GDPR, CCPA and the India DP Bill as the table below demonstrates. (In fact, the India DP Bill was specifically modelled on the GDPR.). For example:

- the GDPR, CCPA and the India DP Bill apply to personal information (i.e., information that directly or indirectly identifies a natural person) rather than to business confidential information;
- the GDPR and the India DP Bill contain similar rules in certain respects regarding international data transfers and legal grounds for processing (the CCPA has no particular requirements in this regard).

Yet there are some key differences: for example, the India DP Bill contains "hard" and "soft" data localization obligations that are absent in both the GDPR and CCPA. While the territorial jurisdictional tests in the GDPR and the India DP Bill are similar, the comparable tests in the CCPA are different. Where there are strong similarities in regulatory requirements between different data privacy laws, an organization may in its GDPC program elect to design its policies and procedures around the requirement that is the most burdensome (the "ceiling" approach) (for example, with respect to cybersecurity).

By contrast, in areas where there are significant differences (such as data localization), an organization may in its GDPC program elect to only comply with those requirements that represent the baseline across various data privacy laws (the "lowest common denominator" approach), while complying with any incremental local requirements in excess of the baseline locally rather than internationally.

The vital steps to designing and implementing a GDPC program include:

- conducting a data flow analysis to map how data is collected, used and transferred by the organization interationally;
- analysing key privacy regulatory requirements in the various countries that the organization operates in (including assessing any scope for regulatory "arbitrage" as discussed above);

• analysing the "gaps" between the organization's existing compliance posture and the target level of compliance that it wishes to achieve;

• developing internal policies and procedures that bridge any compliance "gap", and this step would constitute the substantive element of the GDPC program; and

• ensuring continuing compliance by the organization (such as through regular audits of its compliance by reference to the current regulatory requirements).

High-level summary of key differences between GDPR, CCPA and India DP Bill

	GDPR	CCPA	India DP Bill (2018)
Territorial application	Yes, if there a nexus to the European Economic Area by reference to specific jurisdictional tests.	Some aspect of collection or sale of personal information must take place within California. If every aspect of the collection or sale takes place outside of California, the CCPA does not apply.	Yes, if there a nexus to India by reference to specific jurisdictional tests.
Covered data	"Personal data": Information relating to an identified or identifiable natural person ('data subject').	Any information that "is capable of being associated with" or could "reasonably be linked, directly or indirectly," with a particular California resident or household.	"Personal data": Any information relating to a natural person which directly or indirectly (on its own or in combination with other information) is capable of identifying an individual.
Specially-protected categories of data?	Yes.	Yes. Personal information of children under 16 years of age: Requires opt-in consent before a business can sell such information.	Yes.
Covered entities	Applies to "controllers" (majority of obligations), and "processors" (certain specified obligations).	Applies to: • Any for-profit entity doing business in California that annually: exceeds $25 million in gross revenue; handles the personal information of 50,000 or more California residents, households, or devices; or derives more than 50% of its annual revenue from selling California residents' personal information; or • Any for-profit entity that (a) controls or is controlled by an entity that meets the definition of a "business" in (1) above; and (b) shares common branding (e.g., shared name, service mark, or trademark).	Applies to "data fiduciaries" (majority of obligations), and "processors" (certain specified obligations).
Data localization requirements	No.	No.	Yes.
Legal grounds for processing	• Consent	Not applicable.	• Consent

	GDPR	CCPA	India DP Bill (2018)
	• Compliance with legal obligation • Task in public interest or exercise of official authority of controller • Performance of contract • Vital interests of the data subject • Legitimate interests of controller or third party.		• Compliance with law or any order of the court • Prompt action • Functions of the state • Purposes related to employment • Reasonable purposes
Cross-border transfers restrictions	Yes.	No.	Yes.
Data breach notification requirements	Yes.	Provided for in other California laws; not in CCPA.	Yes.
Data subject rights	• Right of access • Right to data portability • Right to erasure • Right to be informed • Right to object • Right to rectification • Right to restrict processing	• Right of access • Right to data portability • Right to deletion (with exceptions) • Right to be informed • Right to non-discrimination • Right to object to sale of personal information (right to opt-out) • Right to reasonable security practices	• Right of access • Right to data portability • Right to be forgotten • Right to rectification
Protection for children's data?	Yes.	Yes.	Yes.
Regulator	Regulator in each member state in the EEA.	California's Attorney General is charged with enforcing all aspects of CCPA.	National regulator: Data Privacy Authority of India.
Civil penalties	Up to 4% of annual global turnover or 20 million euros.	For actions brought by the Attorney General's office: Up to $2,500 per violation for negligent violations and up to $7,500 per violation for intentional violations. For actions brought by California residents (individually or as a class): Between $100 and $750 per consumer per incident, or actual damages if greater.	Up to approximately $2.7 million or 4% of a company's global turnover.