PIPA calls the tune

How Bermuda is meeting the global data protection challenge

By Michael Bahar, Tony Ficarrotta and Trevor Satnick

This has been a watershed year for privacy. The EU General Data Protection Regulation (GDPR) came into force in May; in June, California passed the *Consumer Privacy Act of 2018* (CCPA), to take effect in January 2020; and, in December, Bermuda's *Personal Information Protection Act* (PIPA) will take effect.

This article is an overview of the laws' key similarities and differences.

Jurisdictional reach

The jurisdictional reach of GDPR, CCPA, and PIPA differs in important ways:

- PIPA applies to organisations that use personal information (PI) in Bermuda, even if that information is not about Bermudians.
- GDPR applies to the processing of personal data in the EU, even if that information is not about EU citizens, and it also covers businesses outside the EU which either: (i) offer goods or services to EU data subjects; or (ii) monitor their behaviour.
- CCPA's protections apply only to California residents; however, CCPA can cover businesses outside California that do business in California and meet any one of the following conditions: (i) they have annual gross revenue of USD25 million; (ii) they use the PI of 50,000 or more California residents, households or devices annually; or (iii) they derive at least 50 per cent of their annual revenue from selling California PI.

Covered activities

The laws all take expansive views of the kind of information processing covered.

- GDPR applies broadly to any kind of PI 'processing', including collection, use, sharing, storage and destruction of PI.
- PIPA applies broadly to any 'use' of PI, essentially the same as under GDPR.
- CCPA generally applies to the 'collection' or 'sale' of PI, rather than 'use' or 'processing'. But this approach will encompass many of the same activities, as CCPA defines 'collection' broadly to include 'buying, renting, gathering, obtaining, receiving or accessing any [PI] pertaining to a consumer by any means', and includes 'observing' the consumer's behaviour. CCPA also defines 'sale' broadly to include 'selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating' a consumer's PI not only for money, but also for any other 'valuable consideration'.

Covered PI

The laws have broad definitions of PI, and, while US laws typically have had narrower definitions, CCPA has the most expansive.

- Under GDPR, personal data is 'any information relating to an identified or identifiable natural person'.
- Under PIPA, PI is 'any information about an identified or identifiable individual'.
- Under CCPA, PI is 'any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household'. Because PI includes household-level information, even electricity usage may be covered PI. It also specifically covers certain online metadata.

GDPR and PIPA provide further protection for 'sensitive' PI, such as race or sexual orientation. CCPA does not similarly treat these types of PI to heightened scrutiny and, with the exception of minor children's PI, treats all PI the same.

Cross-border data transfers

Companies subject to GDPR seeking to transfer PI to a non-EU jurisdiction face additional hurdles unless the European Commission has determined that the jurisdiction to which the personal data is being transferred has 'adequate' data protection rules. In fact, PIPA may represent Bermuda's attempt to obtain such an adequacy determination to ease transfers from the EU to Bermuda.

Still, under PIPA, data transfers from Bermuda to the US will remain closely regulated. Under PIPA, transfers of PI outside Bermuda may be freely made to those jurisdictions the Privacy Commissioner has determined to have a level of privacy protection comparable to Bermuda's. Neither the European Commission nor the Bermuda Privacy Commissioner has determined that the US offers 'adequate' or 'comparable' privacy protections; US companies must rely on other mechanisms for cross-border transfers, including model contract clauses and binding corporate rules. Bermuda, unlike GDPR, does allow companies to reasonably self-determine that an overseas third party provides 'comparable' privacy protections.

CCPA does not govern cross-border transfers of PI per se, except to the extent that such transfers involve the sale of a California resident's PI.

Conclusion

As the global regulatory environment continues to evolve and grow in complexity, companies operating internationally should have a global regulatory strategy for data privacy and protection. The most efficient and effective strategies should account for both important similarities and differences with respect to GDPR, PIPA, CCPA and privacy regulations in other jurisdictions. ■

Michael Bahar is a Partner, **Tony Ficarrotta** is an Associate, and **Trevor Satnick** is Staff Attorney, at Eversheds Sutherland