



## Data privacy law: the top global developments in 2018 and what 2019 may bring

Data Protection, Privacy and Security Alert

25 FEB 2019

DLA Piper recently launched the 2019 refresh of the *DLA Piper Data Protection Laws of the World Handbook*. The latest updates to this popular resource shows very clearly that 2018 was a significant year for privacy and data protection laws and that this area will continue to be one of the most dynamic and fast developing areas of law over the course of the next year.

Last year saw a number of significant privacy law developments worldwide: the GDPR took effect after a two-year implementation period; a number of jurisdictions updated or began the process of updating local data protection laws to align to the GDPR; the US and Brazil broke new ground with privacy laws in their respective jurisdictions; and India introduced sweeping new privacy legislation. Moreover, this trend is expected to continue in 2019.

While there are too many developments to cover comprehensively, we highlight some notable developments below.

### GDPR

It has now been eight months since the EU **General Data Protection Regulation** (GDPR) took effect on May 25, 2018, and nearly all member states have introduced local data protection laws that supplement the baseline position under the GDPR. Some of these jurisdictions – among them Spain and Germany – have deviated from the GDPR in ways that go beyond the specifically recognized derogation areas. These developments underscore the fact

that, while there is a high level of harmonization across the EU, there is not complete uniformity.

Also, across the EU, enforcement activity is clearly gathering pace, underscored by the recent €50 million fine imposed on Google, LLC by the French supervisory authority, the CNIL. A record number of data breaches have been reported post GDPR. Then, of course there is Brexit and the uncertainties this has given rise to in the data protection area and well beyond.

## US

The **California Consumer Privacy Act (CCPA)** – a first-of-its-kind US law – passed in California in 2018 and takes effect January 1, 2020.

The CCPA broadly applies to businesses (regardless of location) that collect personal information about California residents, including customers and employees, and meet certain thresholds. One of these thresholds is that the business collects personal information about 50,000 consumers per year. This is a particularly low threshold when you consider that an IP address is considered personal information under the law: thus, businesses that operate websites that see 50,000 unique visitors per year may easily hit this mark, even if they do not hit one of the other thresholds, such as \$25 million in annual revenue.

The CCPA gives California residents new privacy rights, among them the right to access and deletion, the right to know how a business has collected and handled your personal information in the previous 12 months, and the right to opt-out of the “sale” of your personal information (which includes any disclosure of personal information by a business in exchange for anything of value). The CCPA will require significant compliance measures.

In addition, the CCPA introduces a private right of action for breaches of certain unencrypted personal information. This private right of action is expected to lead to a significant number of class actions. There are a number of steps businesses can consider to try to mitigate the potential for class actions under the law.

Several other US states are expected to pass comprehensive privacy laws in 2019, which will vary from the California law in key ways. (See our CCPA page for news on developments)

## Other developments around the world

In **Brazil**, the General Data Protection Law takes effect in February 2020. Like the GDPR, the Brazilian law applies extraterritorially, granting individuals rights of access, rectification, deletion and data portability.

**Bahrain** also passed a new, comprehensive data protection law – making it the first Middle East country to adopt a comprehensive privacy law.

In addition, other jurisdictions, such as **Serbia** and **Jersey**, amended their data protection laws in order to align to the GDPR as well. **Hong Kong** published a “New Ethical Accountability Framework,” which urges businesses operating in Hong Kong to undertake privacy impact assessments similar to those required under the GDPR.

Further, a number of other jurisdictions are also anticipated to pass amended data protection laws in 2019 to align more closely to the GDPR, including **Bosnia and Herzegovina, Ukraine, North Macedonia, Montenegro, Monaco** and potentially **Malaysia. Switzerland** is expected to pass final data protection law amendments in 2020.

Several other jurisdictions, among them **Uruguay** and **Israel**, have also materially amended existing data protection regime to introduce new or amended privacy and security requirements.

**Peru** amended its Consumer Protection Code (Law N° 29571) in 2018 to prohibit telemarketing calls and text and emailing marketing to individuals, without prior, informed, express and unequivocal consent. **Chile** adopted a constitutional amendment establishing an individual's right to the protection of personal data.

## Expected developments

One of the most significant privacy law developments of 2019 is expected from **India**. India's draft bill introduces specific rights for individuals as well as requirements processing entities have to meet. For example, businesses will need to implement organizational and technical safeguards regarding the processing of personal data, including for cross-border data transfers. The law also establishes a Data Protection Authority for overseeing processing

activities.

Other jurisdictions are currently considering and could very likely pass their first comprehensive data protection law, including **Indonesia, Honduras, Kenya** and **Zimbabwe**. The **British Virgin Islands**, which has not enacted a comprehensive data protection to date, is expected to do so in the near future.

Singapore is among other jurisdictions expected to pass new or amended laws on specific privacy issues – Singapore's will focus on breach notification provisions.

Finally, **New Zealand** has introduced a Privacy Amendment Bill that is expected to become law in 2019.

Learn more about these developments by contacting our data privacy team via [PrivacyGroup@dlapiper.com](mailto:PrivacyGroup@dlapiper.com).