The global landscape of data privacy: Important points about new laws in three key jurisdictions

PRACTICAL COMPLIANCE

Practical Compliance

21 September 2021
By: Harry P. Rudo | Amy Reagan

Welcome to the latest issue of *Practical Compliance*, where we look at issues facing company leadership and counsel regarding some of the latest changes to data privacy laws in key jurisdictions around the world. As countries – as well as US states – address privacy concerns, they are taking an array of approaches, resulting in a patchwork of differing laws and regulations. Companies based in the United States with international operations must monitor continually changing privacy laws that apply to those operations.

In this issue, we highlight key points about new data privacy requirements in three important jurisdictions – the European Union, China, and Brazil – with an emphasis on action steps for compliance officers.

In the **European Union**, the **General Data Protection Regulation (GDPR)** has been in force since May 2018. In summer 2021, the European Commission published new Standard Contractual Clauses for transfers of personal data from the European Union to third countries, such as the United States.

In August 2021, **China** finalized its **Personal Information Protection Law (PIPL)**, which will enter into force on November 1, 2021. PIPL consolidates and clarifies requirements regarding use of the personal information of Chinese

residents.

Brazil's General Data Protection Law (LGPD) has been in force for a year, although the penalties provided by the law did not become enforceable until August 2021. This is Brazil's first comprehensive data protection regulation and is similar to the EU's GDPR.

European Union: New Standard Contractual Clauses for data transfers

- On June 4, 2021, the European Commission released its final Implementing Decision on standard contractual clauses (New SCCs) for the transfer of personal data from the EU to "third countries," such as the United States. These New SCCs are required for new transfer agreements entered on or after September 27, 2021. Agreements currently in effect must be replaced with the new SCCs by December 27, 2022.
- The New SCCs include significant new obligations for data importers, particularly importers acting as data controllers (entities who obtain possession of others' personal data). Adopting and complying with the New SCCs may require considerable effort for these importers, particularly those that are not otherwise directly subject to GDPR.
- Of particular concern for compliance officers, and especially group officers for US-headquartered multinationals, is the fact that commonly in the course of an investigation (whether internal or in conjunction with a government request), the US parent will be acting as a controller. The New SCCs will require those controllers to satisfy new transparency requirements, for example.
- Critically, the New SCCs require the parties – whether or not the data importer is a controller, a processor or a sub-processor – to conduct a detailed, written assessment of the risks associated with the transfer, including risks specific to the destination country.
- The New SCCs cannot be modified and will take precedence over other contract provisions. Contracts should be reviewed to remove conflicting provisions.
- Due to Brexit, the New SCCs do not apply for transfers of personal data *from the UK* to a third country. Data exports from the UK should continue to be based on the existing SCCs until the UK publishes its own SCCs. The UK released draft SCCs in August 2021, which will likely be finalized in late 2021 or early 2022.
- The New SCCs themselves can be found here; different clauses are required for different types of data transfers.
- Additional detail regarding the GDPR's New SCCs can be found here.

China: Personal Information Protection Law

- China's PIPL was finalized on August 20, 2021 and will enter force on November 1, 2021. PIPL is a set of high-level principles that will be supplemented with additional guidelines outlining specific steps organizations should take to update their data protection programs regarding Chinese data. PIPL *clarifies and enhances* – rather than replaces – existing Chinese data privacy and cyber laws, and so should be read alongside the Cybersecurity Law, Data Security Law, Personal Information Security Specification and other national, provincial, and industry-specific laws and regulations that impose data protection rules.
- Some of the principles in the PIPL may look similar to GDPR (and CCPA and other nations' laws), but in practice interpretation and enforcement are very different.
- PIPL applies extraterritorially to both data processing activities within the PRC, as well as to processing PRC residents' data outside of the PRC.
- PIPL makes the transfer out of China of most types of personal data by most organizations more straightforward than under the existing Chinese data protection framework, but there are still significant pockets of data localization requiring certain (personal and non-personal) data to be kept inside of China. *Data mapping to identify data flows in and out of China should be a priority* to identify and address data localization risks.
- Consent remains the primary basis for lawfully collecting personal data in or from China. *Express, informed consent must generally be obtained from data subjects* for all processing of personal information. Additional "separate," explicit informed consent must be obtained for: (a) processing sensitive personal information; (b) overseas transfers; (c) public disclosure of personal information; (d) data provided to another data controller for processing; and (e) use of image or identification data collected in public for any purposes other than maintaining public security.
- Personal information stored within China cannot be shared with overseas legal or enforcement authorities without Chinese authority approval.
- Local data security standards must be complied with. Compliance with international standards may not be sufficient per se to meet these local requirements.

- The PIPL significantly extends the governance obligations on data controllers, including requirements to appoint and register a Data Protection Officer or (if outside of China) a local representative; manage data classification; conduct Data Protection Impact Assessments and training; and oversee record-keeping and internal policies.
- Additional requirements will be imposed on certain organizations, including certain platform providers, Critical Information Infrastructure Operators, those that process large volumes of user data, are a "complex business," or process sensitive personal data or minors' data.
- Potential sanctions for PIPL violations include administrative fines of up to 5% of the previous year's annual revenue and criminal sanctions. In practice, operational sanctions (such as loss of operating licenses, shut down of systems or blocking of apps), and contractual risks require active management.
- Additional detail regarding China's PIPL can be found here.

Brazil: Lei Geral de Proteção de Dados Pessoais

- The LGPD, Brazil's first comprehensive data protection regulation, is based in large part on the EU's GDPR. It entered into force on September 28, 2020, after several discussions and postponements. The penalties set out by the law only became enforceable on August 1, 2021.
- The Brazilian National Authority is the supervisory authority responsible for further regulating data protection in Brazil (also known as the ANPD). The LGPD has several provisions yet to be regulated and interpreted by the ANPD, which may require further localization and adjustments for compliance in the future.
- The LGPD applies to any data processing operation where (1) the purpose of the processing activity is to offer or provide goods or services in Brazil, or the processing of data of individuals localized in Brazil; (2) the personal data was collected in Brazil; *or* (3) the processing operation is carried out in Brazil.
- The LGPD does not apply to personal data (i) processed by a natural person exclusively for private and non-economic purposes; (ii) for other purposes unrelated to business activity (journalistic, artistic or academic purposes); (iii) carried out for purposes of public safety, national security and defense or activities for investigation and deterrence of crimes (which will be the subject of a specific law); or (iv) with foreign provenance and that are not the target of communication, shares use with Brazilian data processing agents, or the object of transfer of data with another country other than the country of provenance, provided such country provides an adequate degree of protection.
- The LGPD regulates the cross-border transfer of personal data from Brazil to other countries and jurisdictions in a manner similar to the GDPR. Such transfers can only occur in the cases set forth in law, such as: (i) with the specific consent of the data subject; (ii) if the receiving jurisdiction has adequate levels of data protection, as specified in law or determined by the National Authority; (iii) when the controller of the data proves it has guarantees of compliance with the principles, rights, and data protection regime set forth in Brazilian law in the form of appropriate standard contractual clauses, global corporate norms, seals, certificates, and codes of conduct regularly issued, the analysis of which will be carried out by ANPD; or the transfer is necessary for various legal reasons. Most of the content of such standard forms will be defined and further regulated by the ANPD.
- Similar to the GDPR, the LGPD offers individuals rights over their personal data, which can be exercised against both public and private organizations. These rights include the right to access their data; to correct incomplete, inaccurate, or out-of-date data; to anonymize, block, or delete unnecessary or excessive data or non-compliant data; and to revoke consent, among others.
- Data controllers (entities or individuals who make decisions regarding the processing of personal data) must appoint a *Data Protection Officer* (DPO) to act as a channel of communication between the controller, the subjects of such data, and the National Data Protection Authority, as well as to organize and monitor data protection compliance programs, oversee LGPD adoption within the organization, and accept complaints and other communications from data subjects and the National Authority, among other attributions. Further regulation in this matter will be issued by the National Authority, including situations in which the appointment of the DPO may be waived, according to the nature and the size of the entity or the volume of data processing operations.
- Processing agents shall adopt security, technical, and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication, or any type of improper or unlawful processing. Although the LGPD does not specifically inform the security measures to be adopted by the controllers and processors, it is recommended that data controllers control who has data access and identify responsibilities for those individuals. The minimum technical standards must be provided by the National Authority, considering the specifics of the personal data and their respective processing. Due to the lack of guidelines, the organizations may follow the international standards.
- Data controllers must, in a reasonable time period, notify affected data subjects and Brazil's regulatory authority (the

ANPD) of security incidents that may create risk or relevant damage to the data subjects. According to guidance published by the National Authority on February 22, 2021, while pending regulation, such period is being considered as two business days, counted from the date of the knowledge of the incident, and must contain specific requirements established in the LGPD.

- Although specific requirements of the Data Protection Impact Assessments (DPIA) will be decided by the National Authority, organizations should conduct DPIAs to assess the security of any particularly "higher risk" processing activities, such as when the legal basis is a legitimate interest, the treatment of data from minors, sensitive personal data, and/or new technologies and systems.
- There is no obligation to sign a contract between controllers/processors and sub-processors, but the LGPD provides that the processor must conduct the processing activities according to the controller's instructions and the controller is responsible for verifying compliance with and fulfillment of these obligations. Therefore, organizations should enter data processing agreements with those who process company data and conduct regular audits to ensure compliance.
- Privacy policies should be reviewed to ensure alignment with LGPD standards. Although there is no express provision about privacy notice under the LGPD, the law guarantees to the data subjects the right to clear, precise, and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy. Therefore, data subjects shall be provided with transparent privacy notice information in an easy-to-understand way.
- Potential sanctions for LGPD violations include administrative fines, simple or daily, of up to 2 percent of the previous year's annual revenue of a private legal entity, group, or conglomerate in Brazil, up to a total maximum of R$50 million (US$10 million) per infraction.
- Additional details regarding Brazil's LGPD can be found here.

Learn more about the implications of these compliance issues by contacting Carol Umhoefer for GDPR questions, Carolyn Bigg for PIPL questions, Paula Mena Barreto of independent law firm Campos Mello Advogados for LGPD questions, or your DLA Piper relationship attorney.

AUTHORS

Harry P. Rudo
Associate
Baltimore (Mount Washington) | T: +1 410 580 3000
harry.rudo@dlapiper.com

Amy Reagan
Associate
Miami | T: +1 305 423 8500
amy.reagan@dlapiper.com