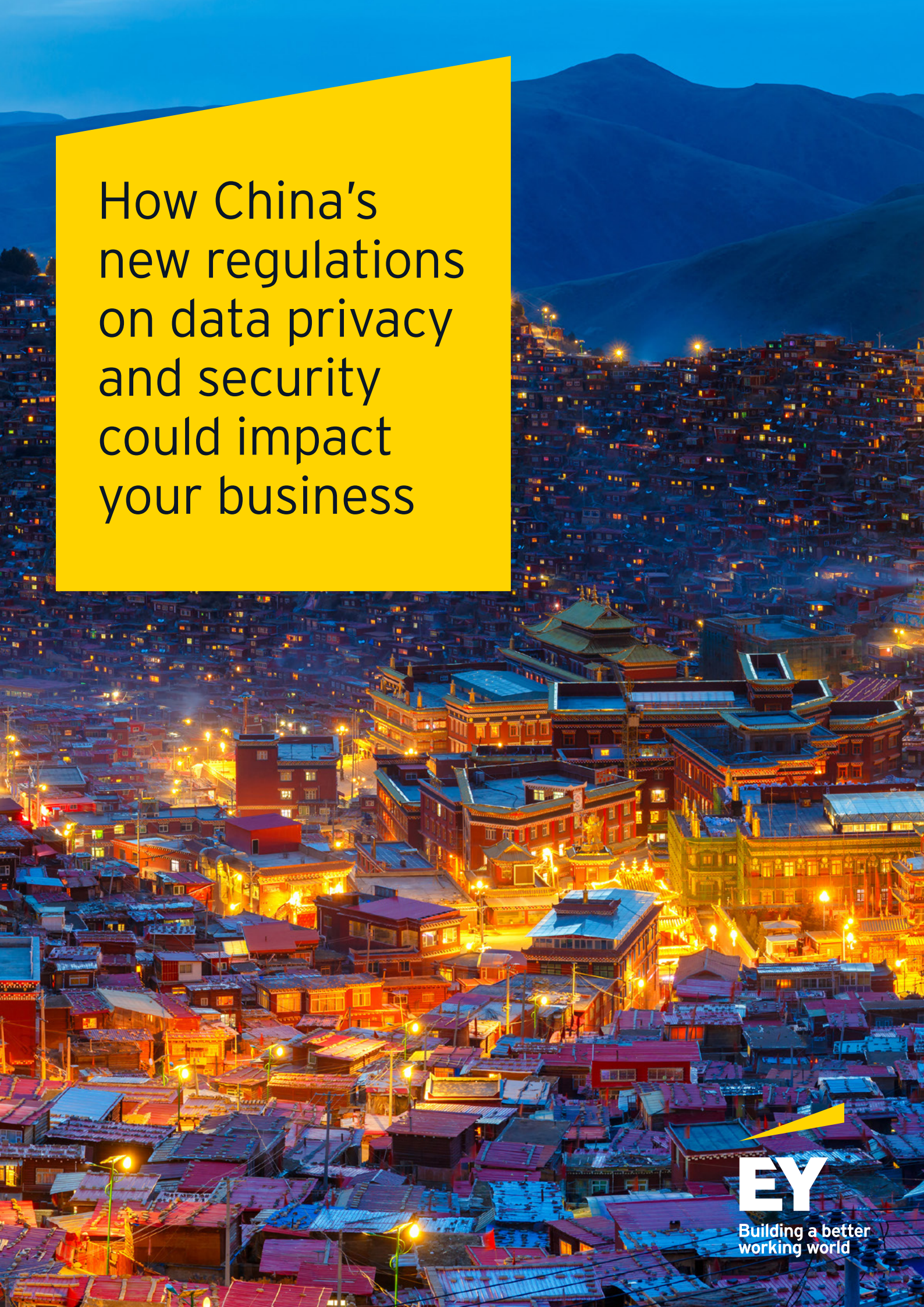
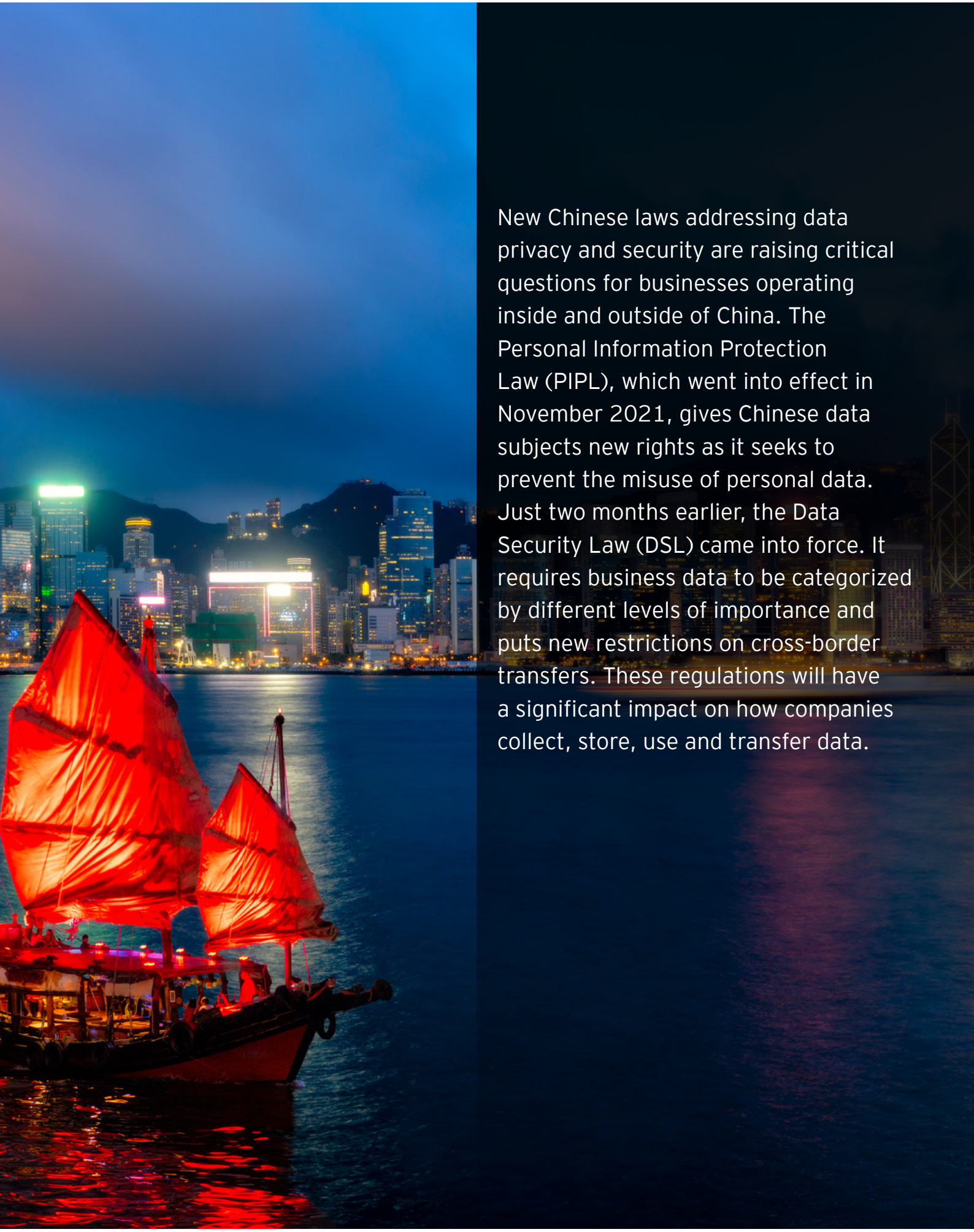
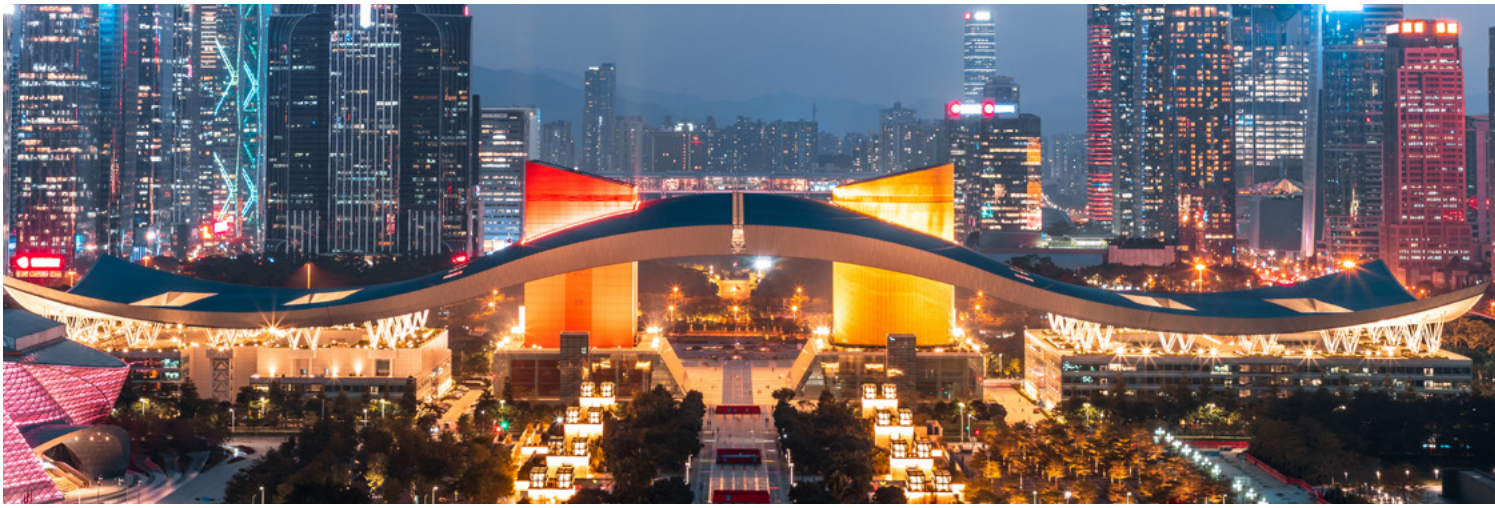
How China's new regulations on data privacy and security could impact your business



EY
Building a better working world



New Chinese laws addressing data privacy and security are raising critical questions for businesses operating inside and outside of China. The Personal Information Protection Law (PIPL), which went into effect in November 2021, gives Chinese data subjects new rights as it seeks to prevent the misuse of personal data. Just two months earlier, the Data Security Law (DSL) came into force. It requires business data to be categorized by different levels of importance and puts new restrictions on cross-border transfers. These regulations will have a significant impact on how companies collect, store, use and transfer data.



New protections for Chinese data subjects

The PIPL is similar to the EU's General Data Protection Regulation (GDPR) in that it gives Chinese consumers the right to access, correct and delete their personal data gathered by businesses. It also impacts offshore data processors that deliver goods and services or analyze individuals in China. Data exporters must ensure that foreign processors provide the standard of protection mandated by the PIPL.

Key PIPL provisions include:

- Separate individual consent is required for third-party data transfers and the processing of sensitive personal information.
- Data can only be retained for a specified period, and only if necessary.
- If civil claims are being made, the burden of proof rests with the data controllers who must prove that they are not at fault for liability to be mitigated.
- Businesses cannot use analytics to treat consumers differently.
- Consumers can opt out of automated decision-making.

The law includes stringent penalties. Fines can be as much as RMB50 million or up to 5% of a company's turnover from the previous financial year. Businesses may also be required to suspend operations until they demonstrate compliance. There are also impacts on individuals, with anyone directly responsible for data protection personally facing fines of up to RMB1 million.

Chinese authorities aren't waiting to crack down on violators. In December 2021, more than 100 apps were removed from the country's app stores for failing to rectify practices prohibited by the DSL and PIPL, such as collecting excessive user data.[1]

Considering the public interest to classify business data

The new DSL requires that business data be classified according to its relevance to national security and the public interest. Companies looking to transfer "important" data outside of China must perform an internal security review before applying for a security assessment and approval from the Cyberspace Administration of China (CAC) and other relevant authorities.

The law also prohibits companies and individuals in China from transferring any data to foreign judicial or law enforcement bodies without prior approval from the relevant Chinese authority. This will pose challenges for companies subject to both the DSL and the GDPR, impacting cross-border litigation.

As with the PIPL, the DSL is also broadly worded, with implementation specifications to follow. For example, two months after the law went into effect, the CAC released a draft regulation requiring companies to inform the agency of data breaches affecting more than 100,000 people or involving any important data within eight hours.

Companies that mishandle data under the DSL face severe penalties, including fines up to RMB10 million and suspension of operations within China. Individuals can be fined up to RMB1 million.

[1]Josh Ye and Coco Feng, "China internet crackdown: Beijing orders app stores to remove Douban and 105 other apps," 9 December 2021, https://www.scmp.com/tech/policy/article/3159091/china-internet-crackdown-beijing-orders-app-stores-remove-douban-and.

Regulating predictive algorithms

While the DSL and PIPL have many parallels with the GDPR and other data protection statutes around the world, China is taking the lead on restricting how companies use algorithms to increase sales. In September 2021, the CAC announced a three-year plan to regulate predictive algorithms used by online content providers.

The draft rules prohibit algorithms that encourage online addiction, a main issue in China. The proposed regulations also require that users be told about algorithmic recommendation services and be given a way to switch them off. Because these regulations are enabled by the PIPL, they can impact foreign businesses as well as Chinese companies.

What should companies do while awaiting further guidance?

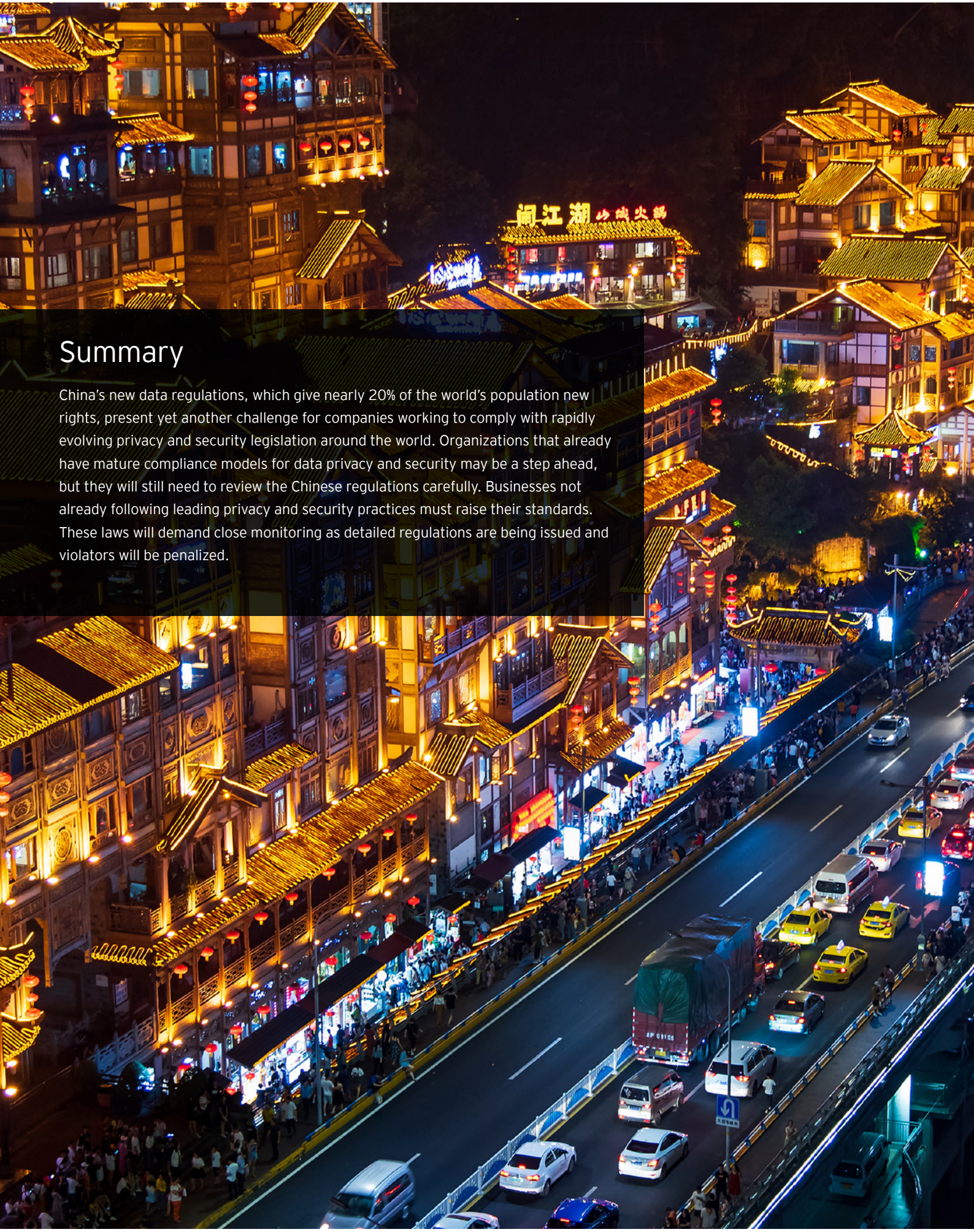
Complying with China's new data regulations won't be easy as companies wait for more information from regulators and standard-setting organizations. But with serious penalties already in play, many Chinese and global operating companies are hastening to assess their data compliance maturity levels and improve their processes.

Foreign data processors in compliance with GDPR or similar statutes have work to do as well — even highly mature processes will need to be analyzed, adjusted and supplemented. Risks arising from cross-border data transfers could force some firms to overhaul their entire IT infrastructure.

Key areas for compliance professionals to consider include:

- **Data collection and consent:** Is your business collecting only necessary personal data? Are you providing clear, separate, individual consent? Are you obtaining consent for location tracking and identifying individuals by collecting images in public venues?
- **Data retention and processing:** Is data kept only if necessary and for a specified period of time? Is data transferred to third parties? Where are those parties located?
- **Data security:** How are you managing cyber risk? Are there sufficient technical measures to guard against unauthorized or accidental access, processing, loss or use of data? Are there emergency plans and backup measures if a data breach occurs? Are you providing prompt notification of a breach to regulators and data subjects?
- **Cross-border transfer of data:** Does your organization's data mapping provide a full inventory of data previously sent to and from China? Do you know the types of data (e.g., personal, "important" under the DSL) that could be transferred? Do you know how to obtain the necessary government approvals?
- **Data subject rights:** Do you have a standard workflow design and the necessary tools for fulfilling data access, correction and erasure requests on a timely basis?
- **Compliance inventory and monitoring:** Is your businesses staying up to date as new laws emerge around the world and guidance evolves? Are you using advanced technologies to continuously screen for possible violations and quickly address your biggest risks?
- **Algorithmic recommendations:** Are your algorithms for online content fair and transparent? Do they remove harmful information, protect consumer rights and discourage online addiction?

Multinational companies face the dilemma of whether to adopt the most stringent data privacy and security measures wherever they do business or follow the least restrictive guidelines allowed. Based on their current business models and future growth plans, companies are carefully assessing their risks and evaluating their options.



Summary

China's new data regulations, which give nearly 20% of the world's population new rights, present yet another challenge for companies working to comply with rapidly evolving privacy and security legislation around the world. Organizations that already have mature compliance models for data privacy and security may be a step ahead, but they will still need to review the Chinese regulations carefully. Businesses not already following leading privacy and security practices must raise their standards. These laws will demand close monitoring as detailed regulations are being issued and violators will be penalized.

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

This news release has been issued by EYGM Limited, a member of the global EY organization that also does not provide any services to clients.

EYG no. 004889-22Gbl
2203-4001600
ED None

ey.com

Authors

Chi Chen
Partner, EY Forensic & Integrity Services
chi.chen@cn.ey.com

Leo Zhou, Director
EY Forensic & Integrity Services
leo.l.zhou@cn.ey.com