China's data protection officer recruitment drive: are you ready?

Dr Amigo L Xie *and* ***Claude-Etienne Armingaud*** *K&L GATES*

In the digital economy, data is generated locally and processed globally. With that in mind, lawyers dealing with data and privacy protection for clients that have businesses in different jurisdictions need to understand differences between data protection laws in major economies and practical solutions to address such differences.

In 2016, a study of the International Association of Privacy Professionals (IAPP) estimated the General Data Protection Regulation[1] (GDPR) in Europe would create a need for at least 75,000 data protection officers (DPO) worldwide.[2] In fact, an IAPP research in 2019 indicated that around 500,000 organisations had registered DPOs across Europe in the first year after the enactment of GDPR.[3]

Similarly, China's comprehensive data protection legislation from 2017 to 2021 provides unprecedented opportunities for privacy professionals in China. The demand is so great that the IAPP estimated that upwards of 500,000 organisations will appoint DPOs responsible for the Personal Information Protection Law of China (PIPL) in the coming years.[4] In addition to PIPL, the Cybersecurity Law of China (CSL) which took effect in June 2017 and the Data Security Law of China (DSL) which took effect in September 2021 (collectively, the Data Governance System) also created similar requirements.[5]

Although PIPL seems very inspired by GDPR at first glance with a lot of similar concepts, the intents and mechanisms behind these concepts are very different.

China is Australia's largest two-way trading partner in goods and services, accounting for nearly one-third (31%) of Australia's trade with the world in 2020. Strong economic complementarities continue to underpin mutually beneficial trade between Australia and China, and Australian businesses continue to successfully enter the Chinese market.[6] As such, many Australian companies are likely to be subject to China's data privacy and security legal regime.

Overview

This article first examines key distinctions between a DPO under GDPR (GDPR DPO) and a personal information protection officer under PIPL, cybersecurity officer under CSL and data security officer under DSL (collectively, China Data Officers). It explores new dimensions of a China Data Officer.

It also discusses some practical safeguards to address concerns on risks of personal liabilities of the actual China data protection officers (China DPO).

Key takeaways

- Although a similar concept of a DPO is used in both GDPR and PIPL, key distinctions exist between each law's DPO provisions in terms of tasks, governance structure and responsibilities.
- New dimensions of a data officer's role in China reflect different legislative intent and purposes behind China's data privacy and security legal regime, which should be noted by privacy lawyers who are interested in this role in China and organisations who plan to staff this position.
- Due to the lack of independence of a DPO role under PIPL, necessary safeguards to enable the China DPOs to perform their tasks in an independent manner to the most extent are more important for both privacy professionals and data handlers in China. Such safeguards could include appropriate internal corporate and contractual documents, liability insurance and appropriate DPO indemnification agreements.
- When advising clients on data and privacy protection in Europe and China, lawyers in Australia need to note the different characteristics of a DPO in China and develop practical solutions to address concerns from privacy lawyers who are interested in this role and organisations who plan to staff this position in China.

What are the key distinctions and new dimensions you need to know?

Because of the DPO requirement under GDPR and global privacy practices in connection with this role in recent years, global privacy professionals are to some extent familiar with the appointment, position and tasks of a DPO role under GDPR.

However, not only do three pillars that form China's data privacy and security legal regime — PIPL, CSL and DSL — refrain from using the actual same term of "DPO" under GDPR, but they also introduce a broader role of a data officer under the new Data Governance System in China. This might cause some confusion regarding the title, status, position and tasks of a data officer under People's Republic of China law.

China vs GDPR

There are four key distinctions suggesting the criteria of a China Data Officer could be different from the criteria under GDPR:

- ***Role***:
  - — *GDPR*: In addition to facilitating compliance through the implementation of accountability tools (such as facilitating data protection impact assessments and carrying out or facilitating audits), GDPR DPOs act as intermediaries between relevant stakeholders (eg, supervisory authorities, data subjects and business units within an organisation).[7] The autonomy and independence of DPOs is a characteristic of a DPO role under the GDPR, which is further reinforced by the lack of personal liability caused by the employing controller (see section regarding personal responsibilities below).
  - — *Data Governance System:* China Data Officers are required to be responsible for supervising a handler's activities of processing personal information, the protection measures taken, etc.[8] The National Standard of Information Security Technology — Personal Information Security Specification (PIS Specification, which is not mandatory but viewed as national best practice for personal information security in China) provides that a personal information protection officer is a person responsible for personal information protection and, among others, coordinates the internal personal information security efforts of a data handler, and bears direct responsibility for personal information security. The roles of a cybersecurity officer under CSL and a data security officer under DSL are to implement the responsibilities for cyber security protection and data security protection. In short, China Data Officers play a broader role than GDPR DPOs.
- ***Tasks***:
  - — *GDPR*: Although GDPR DPOs are designated for the whole of the processing operations carried out by a given controller or processor and should be involved from the earliest stage possible in all issues relating to data protection, Art 39 of GDPR provides five tasks of DPOs which are consistent with their independent status and role mentioned above.
  - — *Data Governance System*: Neither the PIPL, CSL nor DSL provide tasks of a personal information protection officer, cybersecurity officer or data security officer in detail. PIS Specification provides 10 comprehensive tasks of a China personal information protection officer.[9] In some circumstances, China Data Officers could be part of the business operations and management of a data handler, like a real data officer. As an example, in some recently published provincial regulations, the officer's title is exactly a "chief data officer".[10]
- ***Reporting line***:
  - — *GDPR:* A GDPR DPO shall directly report to the highest management level of the controller or the processor.
  - — *Data Governance System*: A China personal information protection officer shall report directly to the principal of the personal information handlers. Under PIPL, the principal shall take overall responsibility for personal information security.
- ***Personal responsibilities***:
  - — *GDPR*: GDPR DPOs are not personally responsible for non-compliance with data protection requirements under GDPR. It is the controller or the processor who is required to ensure and be able to demonstrate that processing is performed in accordance with GDPR. Data protection compliance is the responsibility of the controller or the processor.[11] Moreover, the GDPR DPO is a protected position and cannot be penalised as a consequence of conducting their GDPR DPO mission.
  - — *Data Governance System*: In the event of processing personal information in violation of PIPL or failing to perform any obligation of personal information protection under PIPL in the processing of personal information, besides a personal information handler's liabilities, PIPL creates personal liabilities for personal information protection officers, including a fine from RMB 10,000 (~AUD2200) to RMB 1,000,000 (~AUD220,000), depending on the severity of the infraction, etc. In addition, personal information protection officers in China could risk being blacklisted from serving in other senior

positions in China, having their social credit files reflect any breaches and having their identity disclosed to the public. In the worst scenario, they could face detention as an administrative penalty or arrest as part of criminal investigation.

Comment on the differences: the two systems are far from equivalent

Based on the foregoing comparison, given the GDPR criteria and in terms of guarantees for independence, China Data Officers under PIPL, CSL or DSL cannot simply be considered and referred to as an equivalent to GDPR DPOs.

It is worth noting that the clear departure of a China Data Officer from a GDPR DPO is caused by additional legislative purposes embedded in China's data privacy and security legal regime.

Besides the protection of natural persons with regard to the processing of personal information, PIPL, CSL and DSL also aim at developing data or cyber sovereignty over China-based individuals and protecting national security.[12]

In addition, data is treated as one of the factors of production in China from a macroeconomics perspective. According to the 14th 5-Year plan for the development of the digital economy, by 2025 the digital economy in China is to enter a phase of full expansion, with the value added of the core sectors of the digital economy accounting for 10% of GDP, and anticipates that a production factor market system for data will have been preliminarily established in China.[13]

Because of these additional purposes, a China Data Officer role has more responsibilities than that of a GDPR DPO.

What to do?

PIS Specification provides that personal information controllers shall provide necessary resources to the person and the department responsible for personal information protection to ensure the independent performance of their duties.[14] However, neither PIPL nor PIS Specification provides what resources and safeguards should be provided to personal information protection officers by a data handler in China.

If privacy professionals do not regard the current protection available as adequate under China's data privacy and security legal regime, they will likely be unwilling to serve in such capacities without necessary fail-safe warranties. Failure to obtain such warranties may in turn result in China's personal information protection officer positions staying vacant, causing further compliance issues for organisations.

Nevertheless, this should by no means be construed as an excuse to postpone action until resources and safeguards are either published by the Cyberspace Administration of China — the national cyber and data protection authority in China — or made available from judicial interpretations of PIPL and other cyber or data security laws. For lawyers who want to help their clients address issues in practice, it is worth exploring corporate or contractual arrangements within or with a data handler that could enable real data protection officers to perform their tasks with necessary resources and in an independent or quasi-independent manner. These corporate or contractual arrangements are not only necessary to induce and encourage highly experienced and capable persons to serve as China DPOs, but also reasonable and necessary to promote and ensure the best interests of an organisation and its investors or members.

At least, the following corporate or contractual measures and arrangements are well worth considering when lawyers advise clients on how to enable a real China DPO to play his or her monitoring and security-oriented role in the context of China's data privacy and security laws:

- ***Corporate governance measures***

  As an arrangement with respect to corporate governance, it is necessary and useful to split tasks of China Data Officers and staff the positions with different people so that a China DPO could specifically avoid conflicts of interest, act independently and focus on providing the advice requested for compliance purposes, monitoring compliance and acting as a key point of contact for regulators.

  Because of the comprehensive role and new dimensions we discussed above, some tasks and duties of a China Data Officer could result in a conflict of interest. For example, when and where China Data Officers hold a position within an organisation that leads them to determine the purposes and the means of the processing of personal information or other data so as to make full use of data as a factor of production, these China Data Officers should ideally be part of the senior management in charge of the organisation's business operations.

  Similarly, tasks relating to the protection of national security could sometimes conflict with those that relate to privacy protection.

  Further, the constitution documents of the organisation may provide certain safeguards to enable the China DPOs to be in a security-oriented position and perform their tasks in an independent manner.

Examples of such safeguards are as follows:

— no instructions by the chief executive or other senior officers regarding the exercise of the China DPO's monitoring and security-oriented tasks

— no dismissal or penalty by the organisation for the performance of the China DPO's monitoring and security-oriented tasks and

— no conflicts of interest with possible other tasks and duties of the China DPO

While not mandated under the Data Governance System, these GDPR-inspired safeguards would seem to be common sense to effectively manage an organisation's operations and to ensure adequate data protection provisions.

- ***D&O liability insurance***

  Directors and officers (D&O) liability insurance is meant to protect the company and its management from financial indemnity that is requested following certain acts by the company's directors and officers. It covers the compensation costs and legal fees that may be requested after being sued by an employee, an investor or a regulatory body.

  The direct personal liability of China Data Officers, including China DPOs, put them at direct risk of potential legal action even if they act diligently. With D&O liability insurance, China DPOs could seek compensation from the insurance if a fine or other economic liabilities are personally imposed on them.

  To the extent an organisation maintains liability insurance applicable to its directors or officers, the organisation may consider using commercially reasonable efforts to provide that a China DPO shall be covered by any such policies in such a manner as to provide the China DPO the same rights and benefits as are accorded to the most favourably insured of the organisation's directors and other officers.

- ***Indemnification agreement***

  In a merger and acquisition market, in the event that the availability and coverage of liability insurance is severely limited, it is common for a company to enter into an indemnification agreement with the candidate directors and officers. In such an agreement, the company agrees to indemnify the director or officer if he or she is a party to or threatened to be made a party to or is otherwise involved in any proceeding by reason of the fact that he or she is or was a director or officer of the company against all expenses, judgments, fines, interest and penalties, etc which are actually and reasonably incurred by him or her in connection with such a proceeding to the fullest extent permitted by applicable law and the constitutional documents of the company.

  Organisations that struggle to hire and retain China DPOs may consider putting such an indemnification agreement in place.[15] It could mitigate the risk of China DPOs and further enable China DPOs to act in a diligent and independent manner to protect the best interests of an organisation and its investors.

Conclusion

As we said at the outset, in the digital economy, data is generated locally and processed globally.

The China Data Officer position in China is unique in many ways and may be unfamiliar to those working in free market economies, such as Australia, where supply and demand regulate production and labor as opposed to government intervention. The role and tasks of China DPOs could be shaped in practice in both global and local contexts.

Understanding the characteristics and unique value of an "independent" China DPO and creating necessary corporate and contractual infrastructures for them in China could not only encourage the development of this position in China, but also provide necessary infrastructures to connect data handlers and regulators. This is critical to data governance.

Ultimately, DPOs, whether in China or in Europe, are the great architects of data compliance — without them, the whole edifice is at risk of crumbling.

Dr Amigo L Xie
Partner and Registered Foreign Lawyer (PRC)
K&L Gates, Hong Kong Office
amigo.xie@klgates.com
www.klgates.com

Claude-Etienne Armingaud
Partner and Practice Group Coordinator for the Data Protection, Privacy, and Security Practice Group
K&L Gates, Paris Office
claude.armingaud@klgates.com
www.klgates.com

Footnotes

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2. R Heimes and S Pfeifle "Study: GDPR's global reach to require at least 75,000 DPOs worldwide" *International Association of Privacy Professionals* 9 November 2016 https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.
3. C Fennessy "Study: An estimated 500K organizations have registered DPOs across Europe" *International Association of Privacy Professionals* 16 May 2019 https://iapp.org/news/a/study-an-estimated-500k-organizations-have-registered-dpos-across-europe/.
4. S Adams "Half a Million DPOs Will Likely Need To Be Appointed in China in 2022: Are Organizations Ready?" *CPO Magazine* 30 December 2021 www.cpomagazine.com/data-protection/half-a-million-dpos-will-likely-need-to-be-appointed-in-china-in-2022-are-organizations-ready/.
5. The appointment of a cybersecurity officer is required by Art 21 of the Cybersecurity Law 2016 (China), and the appointment of a data security officer is required by Art 27 of the Data Security Law 2021 (China).
6. Department of Foreign Affairs and Trade "China country brief" media release www.dfat.gov.au/geo/china/china-country-brief.
7. European Commission *Guidelines on Data Protection Officers ('DPOs')* WP 243 rev 01 (2016) p 4 https://ec.europa.eu/newsroom/article29/redirection/item/612048.
8. Personal Information Protection Law 2021 (China), Art 52.
9. Personal Information Security Specification, Art 11.1(d).
10. Article 6 of the Shanghai Data Regulation, Shenzhen Implementation Plan for the Pilot Program of Chief Data Officers, Guangzhou Implementation Plan for the Pilot Program of Chief Data Officers, Circular on Adopting a Chief Data Officer System in Jiangsu Province.
11. Above n 7, pp 24–25.
12. Above n 8, Art 1; Cybersecurity Law (China), above n 5, Art 1 and Data Security Law (China), above n 5, Art 1.
13. China Government Network Central *Circular of the State Council on Issuing the "14th Five-Year" Plan for the Development of the Digital Economy (in Chinese*: 国务院关于印发"十四五"数字经济发展规划的通知) (2021) www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm.
14. Above n 9, Art 11.1(e).
15. In China, similar to practice in Australia, an agreement to indemnify someone for penalties they receive for breach of law is unenforceable. Care needs to be taken to define the tasks and responsibilities of China Data Protection Officers in corporate documents clearly and ensure that such an indemnity is enforceable under the governing law of the indemnification agreement.