Navigating data protection and cybersecurity issues in mergers and acquisitions in Asia-Pacific

November 2022

Hogan Lovells

Overview

Mergers and acquisition (M&A) transactions raise special challenges for data protection and cyber security compliance. Data, including personal data, is increasingly one of the most valuable assets of a target for acquisition. Acquirers wish to ensure that applicable laws and regulations will allow the target to continue to use its data. In many cases, the acquirer will be seeking to expand data usage, in particular to integrate the target's customer base with its own customer data holdings and to better exploit the target's data for competitive advantage.

Data protection and cyber security regulations have become increasingly complex in the Asia-Pacific (APAC) region, meaning that managing and mitigating data-related risks becomes paramount in any corporate transaction.

This guide provides an overview of the compliance pressure points in APAC for M&A transactions and our recommended best practices for addressing them, covering the whole lifecycle of an M&A transaction from the preliminary planning and due diligence through to the post-closing phase.

The value of data and its risks

It goes without saying that data is of critical importance to businesses. This is especially the case in the digital economy, where data can be a target's single most valuable asset. Looking beyond the technology sector, businesses across a wide range of industries are increasingly leveraging on technology and data to reduce costs, raise efficiency and drive competitive advantage. Information about customers and business prospects, contact information, transaction data and insights and trends on businesses derived from digital platforms often represents a key target asset. Use of this information will be critical to maintaining existing customers and the prospects of expanding and driving synergies to other combined businesses will be dependent on the flexibility that data protection laws permit. As data protection laws in APAC increasingly impose consent as a basic requirement for transferring personal data from one organization to another, expanding the use of the data to new business lines and using the data for direct marketing purposes, effective due diligence into the target's data holdings is key.

Significantly, China's introduction of its Personal Information Protection Law (PIPL) in 2021 represents a significant step-change for compliance, with a broad focus on holding organizations accountable for data protection compliance, including greater management oversight, more rigorous procedures directed at achieving compliance in fact and forward-looking policies that seek to ensure that all functional areas of the organization carry out their roles with data protection considerations in mind. There is also a shift in recent data protection regulations changes in the APAC region to provide individuals with a broader range of rights and tougher penalties on organizations failing to comply with the law. Whereas the introduction of the European Union's GDPR in 2018 led to a number of organizations in APAC upgrading their data protection compliance programs, the impact of China's PIPL is much broader based, with so many businesses in the region dependent on China as a key market. Like GDPR, China's PIPL imposes extra-territorial effect, applying to businesses outside of China that collect data as part of business with individuals in China. The effect has been palpable, with many organizations taking steps now to ensure compliance.

For sellers, it is important to consider applicable data protection and cybersecurity regulations at an early stage so as to identify and (if needed) remediate compliance issues so as to ensure that they do not impact valuation of transaction mechanics. From the purchaser's perspective, the target's state of compliance (or non-compliance) will directly correlate with business risks in the area, including potential remediation that will be a cost of doing business going forward.

We have structured the guide in the form of a timeline, analyzing data and cybersecurity related issues at each stage of the transaction: preliminary matters, due diligence, signing to closing, and post-closing.

Stage I: Preliminary

The due diligence process

At the preliminary stage, it will be important for the seller to consider how the due diligence process will be conducted and what kinds of data could and should be disclosed as part of the exercise. The use of virtual data rooms to support due diligence is now commonplace in M&A transactions. Selecting a competent service provider and having the ability to control and limit access to the data room will be of particular importance.

Before any document is disclosed by the seller to the purchaser, it is customary for the seller and prospective purchasers to put in place confidentiality agreements to provide for the rights and obligations as regards the data disclosed during the transaction and more importantly, to limit the access of the data. If the prospective purchasers have advisers, it is also important for the seller to take note of such advisers and consider the need to put in place back-to-back confidentiality agreements. Where certain information is of particular sensitivity, a clean team arrangement may be adopted to further restrict the disclosure of data.

The parties' documentation concerning the due diligence process should address data protection compliance considerations in addition to the usual terms addressing disclosures of the target's confidential information. It is vital that such agreement includes provisions on personal information security and/or standard data transferring clauses, if there is cross-border transfer of personal information. There is an increasing threat of data localization in APAC, particularly with respect to business data in sensitive business sectors. These risks must be taken into account in designing effective due diligence arrangements for an M&A transaction.

Lawful basis to disclose the data

Due diligence often involves transferring and/or disclosing sensitive data and personal information relating to the target's business and its employees. It is important to evaluate at what stage due diligence should be so granular as to include personal data. At early stages of due diligence, management information and more general or aggregate data should be sufficient the purposes of a buyer evaluating a preliminary bid for the target. However, as due diligence advances and a deal starts to take shape, due diligence will sharpen its focus and there may be a need to disclose personal details of key personnel and other individuals having significant importance to the business. If this is the case, it will be important to consider whether there is legal basis to disclose the data to bidders in compliance with the data protection laws in the relevant jurisdictions. The exercise requires a thorough understanding of the data protection law in the jurisdiction(s) in which the target is based and a review of applicable privacy policies. Express consent (or in certain cases, a “separate” or “unbundled” consent) is often a threshold requirement for disclosure of personal information, but there are jurisdictions where notification alone is sufficient. There are also some jurisdictions in which data protection laws have specific exemptions from consent requirements for transactional due diligence. Accordingly, the lawful basis in which the seller is disclosing its data needs to be carefully considered and managed.

Populating the data room

Whether or not consent is required, most APAC data protection laws include a concept of data minimization, which requires organizations handling personal information to limit processing and disclosing of personal information to the minimum extent necessary for the purpose. It follows that the need to disclose employee and/or customer personal information should be

carefully assessed at each stage of the due diligence process. At the early stages of due diligence, the purchaser will likely seek to understand costs and potential redundancy liabilities on an aggregate basis. Information relating to individual employees are generally not going to be relevant to this stage. At later stages in due diligence, it may be important to understand details about arrangements entered into by the target and certain key employees (such as bonus schemes for managerial staff, golden parachutes contained in employment agreements) or specific employee-related disputes, but even so, personal information pertaining to the relevant employee may not be necessary and thus should be redacted before disclosure.

If the sale occurs on an auction basis, it will be important to limit the amount of personal and sensitive information disclosed in the earlier stages, and keep the biggest volume and highest sensitivity of data to be disclosed at the final or near-final stages when a final bidder is selected and exclusivity agreements entered into.

Best practices:

- Consider how the due diligence process will be conducted in light of security and data protection concerns.
- Carefully evaluate the need to disclose personal information at each stage of due diligence and whether aggregate data or redacted data will suffice.
- Consider the lawful basis for disclosure of personal information, consent requirements and applicable exemptions under data protection.
- Redact or limit personal information (e.g., names and addresses) in the documents available in the data room. For an auction sale, consider segregating the data room and disclosing the highest sensitivity of data only at the final or near-final stages.
- Provide model employment contracts rather than executed contracts for all employees and limit the disclosure of sensitive personal information.
- Choose a secure data room provider, complying with data protection and cybersecurity laws, and be mindful of additional security measures for sensitive sectors (for example, critical (information) infrastructure operators).
- Ensure that all persons accessing the data room are bound by confidentiality. Consider the need to put in place clean team arrangements.
- Document and record all compliance efforts (e.g., the data transfer agreements with the data room provider, with cybersecurity and data protection accountability embedded; consent records from data subjects, etc.).

Stage II: Due-diligence

Identifying material risks and liabilities

The target's holding of certain data can be key to the transaction and its valuation. For the purchaser, it is important to conduct thorough and adequate due diligence into the target's data-related policies and practices to reveal existing and potential liabilities from a data protection and cybersecurity perspective.

The purchaser should prioritize its efforts by first understanding the nature, volume and flows of the target's data and then identify the applicable data laws and regulations which apply, both on a general basis and specific basis (for example, additional security measures may be required for more sensitive sectors like the financial or life science industries). The due diligence questionnaire should then be formulated on this basis, tailoring the questions to cover both general and specific aspects applicable to the target.

Key questions for the purchaser to consider include:

- Are we buying the data we think we are buying? Can we use it for the intended purposes?
- Are there any compliance risks which may arise in the course of due diligence or pre-closing integration?
- Is the target compliant with its data protection and cybersecurity obligations under applicable laws and agreements?
- If not, what needs to be done? What are the risks for us as the purchaser? Do we need an indemnity, adjust the valuation, or require the seller to remediate prior to sale?
- Has the target invested sufficiently in data protection and cybersecurity compliance? If not, will this be extra costs for us post-closing?
- Are there pending complaints and investigations that could compromise the purchaser's ability to use the data as intended, or result in significant fines and remediation costs?

Navigating these issues in the myriad of different data protection laws in the APAC region can often be challenging, especially for target groups with operations across multiple regions. Comprehensive data protection laws are now in force in Australia, China, Hong Kong, Indonesia, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Taiwan, and Thailand,. Taking cues from the GDPR and the PIPL, regulators in the APAC region are prompted to modernize and tighten their data protection regimes, making the compliance challenge greater than ever before.

Whilst cybersecurity regulation as a type of regulation separate from data protection has been slower to come to APAC, China's introduction of a cybersecurity law in 2017 and a recent proposal in September 2022 to impose revenue-based penalties for specific sectors, has spearheaded a regional move towards tighter regulation of IT systems and networks. In Singapore, the authorities have in 2022 initiated a review of Singapore's cybersecurity legislation to update it for the fast changing digital world.

With the increasing focus on compliance in the region, it is clear that the target's policies and practices in relation to data protection and cybersecurity should be evaluated as part of due diligence.

The target should be applying appropriate security measures to its processing of personal information and should have appropriate policies

in place dealing with areas such as access to personal data, data processing by third parties, data sharing arrangements, data breach and incident response and data retention, and appointment of data protection officers. Particular areas of focus that can have a direct material impact on the target's acquisition value include the target's compliance with direct marketing requirements, which vary across the APAC region but in many cases involve obtaining specific "tick box" forms of consent and consulting "do not call" registries before contacting consumers by phone, fax, or SMS. In the context of asset transfers in particular, it is key to understand if the target can transfer personal information to the purchaser for direct marketing purposes. Whatever the transaction structure, the ability for the target to transfer personal information to its new affiliates for marketing purposes will likely be a consideration for the integration of the target with the purchaser's existing businesses.

Recent enforcement action by Hong Kong's Privacy Commissioner for Personal Data against EC Healthcare shows increasing scrutiny of businesses that share data across brands in a way that may be confusing or unfair to consumers. Data protection and cybersecurity due diligence should also look into past incidences of non-compliance, including material complaints, data security breaches, and regulatory queries and enforcement action. Depending on the context and importance of the target's date repository to the acquirer, it may also be important to examine outsourcing and data processing agreements to understand if the target is complying with secure processing, cybersecurity, and international transfer restrictions that increasingly apply to regional and global transfers of personal information within and from APAC.

Due diligence of data-related policies, data incidents, and necessary remediation efforts is typically undertaken as a collaborative effort between legal and IT professionals.

Best practices:

- Use a due diligence questionnaire that adequately considers data protection and cybersecurity issues, and requests for information showing compliance.
- Consider which data protection and cybersecurity legislations are applicable depending on the target's operating jurisdictions.
- Ensure that data protection policies and procedures are reviewed by relevant subject matter experts on the due diligence team.
- Pay particular attention to direct marketing practices to ensure the data can be used by the purchaser and its affiliate post-closing.
- Consider whether any of the due diligence findings are material enough to impact valuation, require indemnification or remediation work by the seller as part of the transaction prior to completion.

Stage III – Signing and Closing

Due diligence often discloses that the target has under-invested in data protection and cybersecurity compliance. As the complexity and sophistication of data breaches and cyberattacks increase, organizations' data security practices are under heightened scrutiny from consumers, private litigants, and regulators. A data breach may expose the data of millions of individual consumers, resulting in potentially direct (financial) and indirect (brand reputation and diminished customer loyalty) liability for the organization. With mandatory data breach notification obligations now in force in many APAC jurisdictions and a worrying increase in well-orchestrated ransomware attacks, data incidents are an increasingly public affair, with consequential reputational impact in jurisdictions where fines continue to be inadequate.

If the target has not been allocating sufficient resources to the protection of its data, the purchaser may be left with an expensive remediation some years down the line. Purchasers are often surprised to learn that significant additional IT spending is required to remediate data-related incidents and wish to have understood these commitments at the deal-making stage so as to make appropriate adjustments to the purchase price or require the seller to implement improvements prior to closing. It may be that these risks are mitigated in cases where the purchaser intends to migrate the target's data to its own systems and infrastructure at a later stage, but this too will entail costs which should be taken into account as part of the overall valuation of the transaction.

The impact of deal structure

Personal data cannot be treated as a conventional asset that may be bought and sold. Data subjects often have the right to consent to any transfer of their personal information. Well-drafted privacy policies would typically address the possibility of a future merger, acquisition, or restructuring, eliminating the need to obtain new consents, but this drafting is often missed. As a consequence, it will be necessary to conduct a careful review of the privacy policies against the requirements of applicable data protection laws at the due diligence stage and if needed, the transaction documents should allocate the responsibilities in the remediation actions.

Acquisitions structured as share transfers do not generally give rise to the same challenges as there is less likely to be a "controller-controller" transfer. However, the purchaser's integration plans may nevertheless involve data sharing between the target and the merged group of companies, which can raise data sharing issues under data protection laws. Some jurisdictions have specific exemptions under data protection laws for corporate transactions, but these are relatively rare and do not stand up as an APAC-wide solution.

Documentation

The allocation of risks and responsibilities relating to data should be done through the negotiation of appropriate representations and warranties (R&W) in the transaction documents. Standards on R&W vary by industry and region but often include representations regarding:

- Compliance with data protection and cybersecurity laws and contractual requirements.
- Security of information technology assets.
- Disclosure of data related claims and compliance investigations.
- Disclosure of arrangements under which data is shared with or by third parties.

- Security assessments and remediation of any gaps.

These R&W should also address any significant due diligence findings, which may need to be reinforced by indemnities provided by the seller, or rectified by sellers prior to completion if specific risks or incidents of non-compliance are identified through due diligence.

Depending on the results of the due diligence, a number of other provisions may be considered. These include special indemnities for data-related liabilities; closing conditions to address implementation of missing IT safeguards or compliance gaps; and covenants to address ongoing safeguards of sensitive information.

The transaction may also require different types of ancillary agreements which will address various aspects of personal information, for example:

- Transitional services agreement dealing with post-closing data integration and services.
- Data sharing agreement to govern data transfers pre-closing.
- Other licensing and data processing agreements for operation of the business post-closing.

Best practices:

- Check capex forecasts to make sure adequate IT investments are budgeted for cybersecurity.
- Consider any necessary investment arising from failure to comply and how this investment is impacted by the purchaser's integration plans for the target.
- Incorporate strategy for data integration into the transaction documents.
- Assess the strategy against data protection requirements to understand if they can be achieved.
- Transfer of certain personal information may be subject to restrictions. Consideration may need to be given to obtaining consents from data subjects as part of the interim steps before completion. These restrictions may affect deal structures.
- Consider treating data protection and cybersecurity similarly to environmental risks in the share purchase agreement (SPA), including a potential audit to establish a baseline and remediation steps.
- Employee-related data protection issues may require additional R&W, conditions precedent, and covenants between signing and closing.
- Drafters of the SPA should think through data transfers, sharing, and use to ensure that they are covered by appropriate ancillary agreements.
- From completion, responsibility for data compliance shifts to the purchaser, meaning that ancillary agreements such as transitional services agreements should address secure processing and international transfer restrictions, including the arrangement to obtain government approval or registration if applicable.

Stage IV – Post-closing

Employee integration

To integrate the target businesses post-closing, the purchaser's team will need to have developed plans as to how the employee and customer data and other information of the acquired businesses will be integrated into the purchaser's own organization. Integration planning may require the transfer of significant personal information between the target and the purchaser prior to closing.

Transferring employee data to the purchaser prior to closing raises particular data protection issues. Before closing, the purchaser or the purchaser's group is a third party vis-à-vis the target. Therefore:

- The target may have to make filings with relevant data protection authorities in connection with the transfer.
- The target must be able to justify that the transfer only involves data that is absolutely necessary for the integration task, and that the recipients of the data are limited to the integration teams within the purchaser's organization.
- The purchaser should undertake to return or destroy the data in the event the closing does not occur for any reason, and should naturally be bound by a confidentiality obligation and an obligation not to use the data for any purpose other than for integration planning.

For complex integration projects involving large amounts of data, the purchaser and the target may consider creating a governance framework to ensure that data protection concerns are reflected during each stage of the process.

Data and database integration

As data becomes an increasingly valuable strategic corporate asset, businesses may look to combine customer databases to maximize synergy. Integrating databases will often raise data protection compliance concerns. The target's existing data subjects' consents and other compliance measures such as privacy notices may not fully address the intended scope of the combined business. The purpose of use of personal information as originally intended may also differ after the integration, making it necessary for the purchaser to notify the data subjects and/or seek new consents (which may be challenging).

The operating efficiencies envisaged for an integrated business may be further challenged by cross-border data transfer controls that prevent or restrict consolidation of data center and other operations, especially when more APAC jurisdictions are adopting stricter personal information cross-border transfer controls.

Apart from the regulatory compliance issues, the costs of integrating databases may be substantial and create transactional risks, raising concerns that data may be damaged by the exercise.

Acquiring data assets through an acquisition does not give a purchaser unrestricted rights to use the data post-closing. Most APAC data protection laws restrict transfers of personal information within a group of companies in the same way they restrict transfers between unrelated parties, and any limitations on the purposes and/or processing methods for which the target was permitted to use personal information will "flow through" to the purchaser. Digital interactions with consumers may provide opportunities to ease the integration of the organizations' databases, but these proposals must be carefully checked against data protection laws, particularly if the purchaser plans on using the data for marketing purposes.

Transitional services agreements

Post-closing, the purchaser and the seller may have to continue collaborating on migration and integration efforts for a period of time. During this period, the seller may continue to conduct a number of data processing operations on behalf of the purchaser.

These post-closing data processing operations may form part of a broader set of technical and operational services covered by a transitional services agreement (TSA). From a data protection standpoint, the TSA will be considered a data processing agreement between the purchaser, as data controller, and the target, as data processor. The TSA shall settle the data processing responsibilities of parties (e.g., coordination mechanism between the parties for responding to data subject rights during this period) and detail the security measures such as data separation arrangement. Data protection laws in APAC jurisdictions impose secure processing requirements when data controllers engage data processors, and many jurisdictions impose international transfer restrictions that may be relevant.

Post-closing restructuring and remediation

One of the most challenging post-closing tasks will be to integrate the acquired businesses into the purchaser's data protection governance arrangements. The process will be similar to rolling-out the purchaser's global compliance program into the newly acquired businesses.

Best practices:

- Put in place a data protection framework agreement between the purchaser and the target to govern and secure the transfers of data pre-closing.
- Limit disclosure of data to integration teams.
- If one party will be processing personal information on behalf of another pre-closing (e.g., in respect of employees being transferred in an asset sale), put in place a data processing agreement.
- Specific training measures would have to be introduced into the new businesses, data protection officers will have to be named, and compliance gaps identified and corrected.

Authored by: Mark Parsons, Sherry Gong, Tommy Liu, Mark Vincent, Nicola Choi and Flora Feng.

Contacts

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Sherry Gong
Partner, Hong Kong
T +86 (10) 6582 9516
sherry.gong@hoganlovells.com

Tommy Liu
Counsel, Hong Kong
T +852 2840 5072
tommy.liu@hoganlovells.com

Mark Vincent
Senior Associate, Singapore
T +65 6302 2574
mark.vincent@hoganlovells.com

Nicola Choi
Associate, Hong Kong
T +852 2840 5636
nicola.choi@hoganlovells.com

Flora Feng
Junior Associate, Beijing
T +86 (10) 6582 9546
flora.feng@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com