How to navigate data protection and cybersecurity issues in mergers and acquisitions in Asia-Pacific

November 2020

Hogan Lovells

Overview

The growing importance of data to mergers and acquisition (M&A) transactions highlights the need to have effective due diligence, transaction structuring, and execution that addresses the growing demands of data protection and cybersecurity regulation in the Asia-Pacific (APAC) region.

This guide provides an overview of the most important ways in which data protection and cybersecurity regulations can impact M&A transactions.

We have structured the guide in the form of a timeline, analyzing each stage of the transaction: pre-signing, signing, signing to closing, and post-closing.

Data protection in M&A: Navigating APAC data protection and cybersecurity regulations

Data protection and cybersecurity regulations have taken on increased importance in the APAC region M&A transactions. Understanding these compliance requirements is critical to securing and maximizing the value of the target's data assets and to assessing the risks accompanying the acquisition. Getting the compliance right can also be important to transaction due diligence and the implementation of transitional service arrangements between the acquirer and the seller.

Value in data

It goes without saying that data is of critical importance to businesses. This is especially clear in the digital economy, where data can be an acquisition target's single most valuable asset. But looking beyond the technology sector, businesses across a wide range of sectors are increasingly leveraging technology to drive competitive advantage. Information about customers and prospects, from contact information through to transaction data and insights derived from digital platforms, can be a key component of the business value of the transaction. The business strategy for acquisition will invariably include the desire to continue to sell to these customers and often the intention to drive synergies by marketing the acquirer's products across the combined business. Ensuring that the target's data can be used in the way that the acquirer expects will depend on the applicable data protection laws. Effective due diligence is key.

… and risk

The flip-side to the enormous potential value in data is the associated compliance risk. Data protection and cybersecurity regulations have grown considerably in APAC in recent years. Most major economies in the region now have data protection authorities, and the trend by regional lawmakers is to seek to emulate the European Union's General Data Protection Regulation (GDPR) with increasing exacting compliance requirements and ever larger fines. Effective transactional due diligence will consider the target's state of compliance. Has it invested sufficiently in data protection and cybersecurity compliance? Are there pending complaints and investigations that could compromise the acquirer's ability to use the data as expected, or result in significant fines and remediation costs?

To mitigate risks, it's key to ask acquirers the right questions.

Key questions for acquirers:

- Are we buying the data we think we are buying?
- Can we use it for the purposes we expect?
- Can we integrate the data with our existing holdings of data?
- Is the target compliant with data protection and cybersecurity regulations?
- If not, what needs to be done? What are the risks for us as an acquirer? Do we need to receive indemnification, adjust the valuation, or require the seller to remediate prior to sale?

Stage I - Pre-signing

1. Populating the data room

The use of virtual data rooms to support due diligence is now commonplace to M&A transactions. Such use often involves transferring and/or disclosing the target's employee data and will require compliance with the data protection laws in the relevant jurisdictions. This inevitably requires a thorough understanding of the target's privacy policy and the jurisdictional data protection law in which the target is based. Consent is often a threshold requirement for disclosure of personal data, but there are jurisdictions where notification is sufficient or consent may be implied. There are also some jurisdictions in which data protection laws have specific exemptions from consent requirements for transactional due diligence.

Whether or not consent is required, most APAC data protection laws include a concept of data minimization, which requires organizations handling personal data to limit processing and disclosure of personal data to the extent necessary for the purpose. It follows that the need to disclose employee personal data should be carefully assessed at each stage of the due diligence process. At the early stages of due diligence, the acquirer will likely seek to understand employee costs and potential redundancy liabilities. Individual employee identities are not generally going to be relevant to this purpose, meaning that aggregate data will likely be sufficient. At later stages in due diligence, it may be important to understand details about specific key employees or senior managers or specific employee-related disputes, but this need should be assessed carefully.

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 business information. It is vital that such agreement includes provisions on personal data security and/or standard data transferring clauses, if there is cross-border transfer of personal data.

Best practices:

- Carefully evaluate the need to disclose personal data at each stage of due diligence and whether aggregate data or redacted data will suffice.
- Consider consent requirements and applicable exemptions under data protection laws.
- Redact/limit personal information (e.g., names and addresses) in the documents available in the data room.
- Provide model employment contracts rather than all contracts.
- Do not disclose sensitive personal information.
- Choose a secure data room provider, complying with data protection laws.
- Ensure that all persons accessing personal data available in the data room are bound by confidentiality.

2. Due diligence

The acquisition target's data holdings can be key to its valuation. Due diligence can also reveal potential liabilities for data protection and cybersecurity violations.

Identifying material risks and liabilities

The APAC region has a complex patchwork of national data protection and cybersecurity laws. Comprehensive data protection laws are now in force in Australia, China, Hong Kong, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Taiwan, and Thailand, with India expected to enact a comprehensive law in the near future. In the wake of GDPR, these laws are being updated and given more teeth, making the compliance challenge greater than it has ever been in the past. Whilst cybersecurity regulation as a separate type of regulation focusing on information technology (IT) security has been slower to come to APAC, China's introduction of a cybersecurity law in 2017 has spearheaded a regional move towards tighter regulation of IT systems and networks.

With the increasing focus on compliance in the region, it is clear that the target's policies and procedures in relation to data protection and cybersecurity should be evaluated as part of due diligence. It is critical to understand that the target has obtained the consents it needs to process, transfer, and disclose its holdings of personal data. The target should be applying appropriate security measures to its processing of personal data and should have appropriate policies in place dealing with areas such as data processing by third parties, data sharing arrangements, and data retention. Particular areas of focus include the target's compliance with direct marketing requirements, which vary across the 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 data to the acquirer for direct marketing purposes. Whatever the transaction structure, the ability of the target to transfer personal data to its new affiliates for marketing purposes will likely be a consideration for the integration of the target with the acquirer's existing businesses.

Data protection and cybersecurity due diligence should also look into incidences of non-compliance, including material complaints, data security breaches, and regulatory queries and enforcement action. Depending on the context, 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 data within and from APAC.

Best practices:

- Use a due diligence questionnaire that adequately considers data protection and cybersecurity issues.
- Ensure that data protection policies and procedures are reviewed by relevant subject matter experts on the due diligence team.
- 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.

Remediation

Due diligence often discloses that the target has under-invested in data protection and cybersecurity compliance. The pace, scope, and sophistication of data breaches and cyberattacks continues to increase, placing businesses' data security practices under heightened scrutiny from consumers, private litigants, and regulators. Such breaches can expose the data of millions of individual consumers, resulting in potentially massive liability. Such breaches trigger both direct (financial) and indirect (brand reputation and diminished customer loyalty) costs.

If the target did not allocate sufficient resources to the protection of its data, the purchaser may be left with the bill. Purchasers often are surprised to learn that significant additional IT spend is necessary post-closing and wish to understand those commitments pre-closing, so as to consider whether the price should be reduced to reflect the necessary remediation or whether the seller should be required to implement improvements prior to closing. It may be that the acquirer intends to migrate the target business to its own IT systems and infrastructure, but this too will entail costs that should be taken into account as part of the overall valuation of the transaction.

Due diligence into necessary remediation efforts is typically undertaken as a collaborative effort between legal and IT professionals.

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 acquirer's integration plans for the target.

Data integration

As data becomes an increasingly valuable and strategic corporate asset, businesses look to combine customer databases to maximize transaction value. Integrating databases will often raise data protection compliance issues. The target's existing data subject consents and other compliance measures may not address the scope of a combined business or align with its legal structure. The purpose of the use of personal data after integration may also increase as the acquirer seeks the benefits of the combination.

The operating efficiencies envisaged for an integrated business may be 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 data protection controls.

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

Best practices:

- Incorporate strategy for data integration into the due diligence plan.
- Assess the strategy against data protection requirements to understand if they can be achieved.

Choosing the deal structure

Asset purchases involve the transfer of specific assets and liabilities. Personal data is not a conventional business asset given that data subjects often have the right to consent to any transfer of personal data. Well-drafted privacy policies will address the possibility of a future merger, acquisition, or restructuring, but this preventive measure is often missed, meaning that a careful review of the requirements of applicable data protection laws will be necessary.

Transactions structured as share transfers may not give rise to this challenge. Some jurisdictions have specific exemptions under data protection laws for corporate transactions, which can also provide relief to this thorny problem.

Best practices:

- Like contracts, personal data cannot always be assigned in a transaction. These restrictions may affect deal structures.
- Consideration may need to be given to obtaining consents from data subjects as part of the interim steps before completion.

Stage II - Signing

Drafting the share purchase agreement: Representations and warranties

The value of and risks relating to data should be confirmed through the negotiation of appropriate representations and warranties in the transaction documents. Those representations vary by industry and risk levels but often include representations regarding:

- Compliance with data protection and cybersecurity laws and contractual requirements.
- Security of information technology assets.
- Detection of network vulnerabilities and data breaches.
- 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 representations should also address any significant due diligence findings and assumptions, and may need to be backed by indemnification where specific risks or incidents of non-compliance are identified through due diligence.

Other contract provisions

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.
- Covenants to address ongoing safeguards of sensitive information.

Best practices:

- Consider treating data protection similarly to environmental risks in the share purchase agreement (SPA), including a potential audit to establish a baseline and remediation steps.
- Data protection may affect SPA representations and warranties on employment, conditions precedent, and covenants between signing and closing.

Ancillary agreements

The transaction may require various ancillary agreements dealing with personal data, including:

- A transitional services agreement dealing with post-closing data integration and services.
- A data sharing agreement to govern data transfers pre-closing.
- Where appropriate, other licensing and data processing agreements for operation of the business post-closing.

Best practices:

- 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.

Stage III - Between signing and closing

Between signing and closing, the purchaser's integration team will be developing plans on how to integrate the employees and information systems of the acquired businesses into purchaser's own organization. Integration planning may require the transfer of significant personal data between target and purchaser prior to the 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:

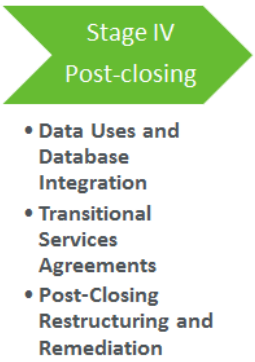
- The target may have to make filings with relevant data protection authorities in connection with the transfer.
- The target must be able to justify that the transfer only involves data that is absolutely necessary for the integration task, and that the recipients of the data are limited to the integration 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 target may consider creating a governance framework to ensure that data protection concerns are reflected during each stage of the process.

Best practices:

- Put in place a data protection framework agreement between the buyer 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 data 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.

Stage IV - Post-closing



Data uses and database integration

Acquiring data assets through an acquisition does not give a buyer unrestricted rights to use the data post-closing. Most data APAC data protection laws restrict transfers of personal data within a group of companies in the same way they restrict transfers between unrelated parties, and any limitations on the purposes for which the target was permitted to use personal data will "flow through" to the acquirer. 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 acquirer plans on using the data for marketing purposes.

Transitional services agreements

After closing, the parties to the transaction may need to continue migration and integration of business operations for a period of time. During this period, the target may continue to conduct a number of data processing operations on behalf of the buyer.

These post-closing data processing operations are generally 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.

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:

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, Tommy Liu, Matthew Bousfield, and Angele Lok.

Contacts

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

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

Matthew Bousfield
Counsel, Singapore
T +65 6302 2565
matthew.bousfield@hoganlovells.com

Angele Lok
Associate, Hong Kong
T +852 2840 5042
angele.lok@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Colorado Springs
Denver
Dubai
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
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com