PRIVACY CONSIDERATIONS IN MERGER AND ACQUISITION TRANSACTIONS:

GLOBAL PERSPECTIVES

macpherson kelley.

TIMELEX

RocaJunyent

Tozzini Freire. ADVOGADOS

VM VANEGAS MORALES Consultores

Tanner De Witt solicitors

ORION

Readership Points

M&A Transactions necessarily involve enormous effort focussed on the deal's 'commercial' aspects (eg, merger / competition clearance, negotiating pricing, obtaining finance, etc). Sometimes, privacy and data protection matters can be overlooked, or given only cursory consideration. Privacy compliance can have significant impacts on the successful completion of the M&A Transaction and the ongoing operation of the acquired business.

Inhouse counsel participating in or advising on merger and acquisition transactions should read this article to learn practical insights about:

- common "red flags" concerning privacy- and data protection matters that should be identified and resolved early in the due diligence phase;
- common contractual representations and warranties that should be sought in transactions, and claims that are commonly made for reliance on those representations and warranties;
- a useful, structured approach for acquirers and target businesses, to progressively share personal information in a manner to minimise privacy and data protection breaches; and
- critical integration and compliance steps to be completed post-acquisition.

Key Takeaways

- In the excitement of progressing the 'commercial' aspects of a proposed M&A Transaction, both the Target and the Acquirer must not forget (or leave too late) considerations relating to personal data privacy and protection.
- Failure to identify and resolve privacy and data protection "red flags" during the due diligence phase can delay or prohibit the timely completion of the M&A Transaction. Failure to properly consider and draft appropriate contractual representations and warranties can also invoke (or limit) subsequent claims and indemnities. In some instances, data breaches can also impact the very success of the M&A Transaction, including leaving the Acquirer exposed to legal liability and trading restrictions post-acquisition.
- Due diligence "red flags" don't have to be a deal-breaker, as practical steps can often be implemented to minimise risk.
- Importantly, from a privacy and data protection perspective, the deal is not done when completion occurs - - privacy compliance must continue to be a focus for post-acquisition integration and the ongoing operation of the acquired business.

Introduction

Merger and acquisition transactions **(M&A Transactions)** can be exciting events for businesses. For the potential investor / acquirer **(Acquirer)**, it can represent a new business stream, and/or an income opportunity. For the potential divestor / seller **(Target)**, it can mean a much-needed injection of valuable assets or cash for ongoing operational purposes, or the successful realisation of an exit or succession strategy.

Often in M&A Transactions, the bulk of the respective parties' efforts, focus and resources are directed towards the 'commercial' aspects of the deal, eg, negotiating the price, obtaining finance, retaining key vendor contracts, and working towards a very tight completion deadline.

But in this process, the underlying – and no less important – privacy and data protection considerations for the Target, the Acquirer and their respective stakeholders can sometimes be overlooked.

When advising on M&A Transactions, inhouse and external legal counsel are well-advised to take into account a range of factors to ensure that privacy and data protection is fully integrated into the entire deal-making process – from the due diligence phase, to completion, to post-completion integration and the ongoing operation of the business.

For the benefit of inhouse legal counsel and other personnel who may be involved in managing M&A Transactions, this article explores the following:

01

Common "red flags" for inhouse legal counsel and other professionals to identify and resolve in the M&A Transaction due diligence process;

02

The common privacy and data protection representations and warranties (R&Ws) that should be sought from and about the Target proposed to be acquired in M&A Transactions;

03

Considerations for when a Target wishes to share the personal data it holds with its potential Acquirers;

04

Examples of claims that M&A and privacy legal professionals commonly see being made about privacy and data protection R&Ws;

05

Common privacy integration tasks to be monitored and/or completed in the post-acquisition / transitional phase (including a Hong Kong case study of how things can go wrong); and

06

Real life tips and practical guidance on privacy and data protection matters, for inhouse legal counsel working in the M&A space.

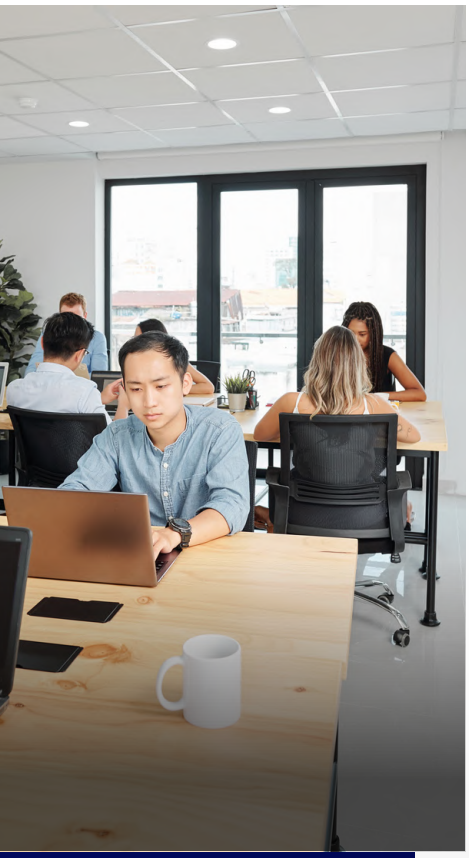
Common "Red Flags" – M&A Transaction Due Diligence Process

When entering into an M&A Transaction, the Acquirer typically conducts due diligence on the Target, to ensure that it is making a good investment and is not taking on unforeseen liabilities. In this process, an Acquirer will typically conduct due diligence on matters covering the Target's general corporate status, ownership of real and chattel assets, workforce composition, ownership of intellectual property, securities given, litigation and investigation history, and other matters of materiality.

The fines, claims and other adverse consequences arising from a Target's non-compliance with data protection laws or involvement in a data breach can be substantial. As such, an Acquirer considering an M&A Transaction should ensure that it conducts a specific due diligence review of the Target's (a) privacy and data protection regulatory history and compliance status, and (b) representations and warranties.The privacy due diligence should be aimed at ensuring that the Acquirer has a clear understanding of the privacy risks associated with the Target, and can take appropriate steps to mitigate those identified risks at the appropriate stage of the M&A Transaction.

As the Acquirer works through the privacy and data protection sections of the due diligence, they should pay particular attention to "red flags" — facts or circumstances related to the Target's data protection practices that could result in civil, criminal or reputational risk for the Acquirer after the M&A Transaction closes.

Below are some of the most important privacy-related red flags that Acquirers should watch out for when considering an M&A Transaction:



No privacy sections in the due diligence questionnaire.

Whilst some due diligence questionnaires can have limited scopes and/or specified materiality thresholds, Acquirers should ask immediate questions of the Target if the Target appears to have omitted or ignored answering the privacy and data protection sections of the due diligence questionnaire.

Insufficient or no privacy policy / data protection policy.

Because the collection and use of personal data are ubiquitous, it should raise eyebrows if a Target discloses that it does not have any privacy policy / data protection policy in place.Similarly, if the provided privacy policy / data protection policy is only brief, it will typically indicate that some of the mandated content is missing (and therefore, this element of proper privacy and data protection compliance is already compromised).

At the very least, a Target's privacy and data protection policies and procedures should comply with the privacy and data protection laws in the jurisdiction where the Target primarily conducts business. If the Target collects personal data from overseas or sends personal data

overseas to affiliates or third parties for processing or other purposes, it should also verify whether its privacy policy / data protection policy needs to comply with the data protection laws of such other jurisdictions.

Because there is no "one-size-fits-all" approach to privacy policies and data protection policies, a Target's processes and documentation should be fit for purpose – ie, it must be appropriate to the specific type and amount of personal data the Target processes, and how the Target uses the data. For example, if the Target deals with a great volume of sensitive personal data (eg, financial or medical information), it should have proper security measures in place to protect the data from unauthorised access, use, modification or disclosure. There should also be processes in place to regularly review and update the privacy policy / data protection policy and its underlying processes to keep them current and relevant.

Accordingly, the mere existence of a privacy policy / data protection policy may not be sufficient, and an Acquirer should dig deeper to ensure that the Target's policy is suitable for its operations.

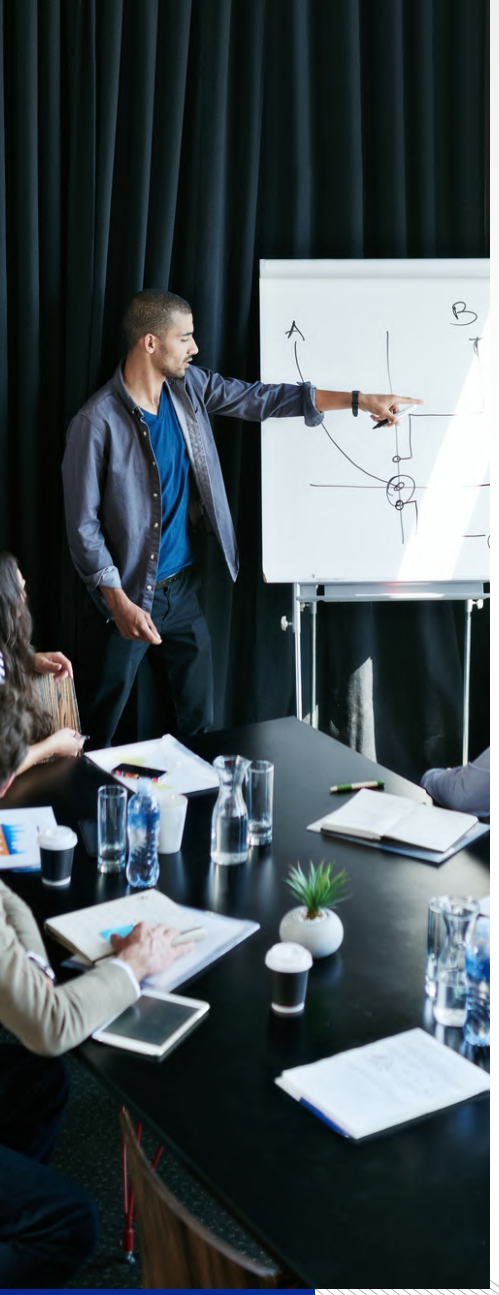
No privacy officer / data protection officer.

Although not all privacy and data protection laws strictly require the appointment of a dedicated privacy officer or data protection officer (**DPO**), the lack of a DPO is a red flag because it can reflect the Target's lack of commitment to data protection regulatory compliance. A DPO is not only responsible for ensuring the Target's compliance with data protection laws and its own data protection policies and procedures, but also plays a central role in preparing for and managing data breach incidents.Accordingly, a Target without a DPO could more likely be in breach of data protection laws, or have an unstructured approach to handling data breaches, or have an unawareness of its current privacy and data protection shortcomings.

Insufficient or no data protection and cybersecurity training for leadership and/or employees.

The existence of a robust privacy and data protection plan "on paper" could be futile if the Target's leaders and employees are not properly trained on its implementation, or are unaware about how to properly deal with cybersecurity risks.

A lack of proper and periodic refresher training increases the Target's risk of mishandling personal data, whether through human error or otherwise, or of falling victim to cybersecurity threats.



No personal data inventory.

An Acquirer should be wary if the Target does not have a personal data inventory – ie, it is not fully aware about the types and amounts of personal data it processes, or why or how it uses or discloses personal data, or where it stores personal data, etc. This is because the Target will not be able to accord suitable protection to personal data in its possession or control, which is a major regulatory risk.

Commercially speaking, because the Target may not be aware that it possesses or controls certain personal data, it may also lose (or have lost) income or opportunities for not using that data to its fullest (and lawful) potential.

Of course, there is also a danger of retaining too much personal data or retaining personal data for too long, which comes with its own risks and costs. Among others, unnecessarily retained data could be accessed by unauthorised persons internally or externally (ie, a security risk), could be made the subject of a disclosure request in legal proceedings (ie, a legal risk) and could increase storage and management expenses (ie, an operational cost).

Past data breach incidents.

The existence of a past data breach incident may not be an issue in and of itself, particularly if the breach was relatively minor (eg, the breach affected only a few people and did not involve sensitive data), or if the breach was well-managed (eg, the cause of the breach was immediately remedied, and its adverse impacts were effectively mitigated).

However, a past data breach incident may be a red flag if the cause of the incident has not been remedied – because it could reflect the Target's disregard for the importance of protecting personal data – or if data breaches, even minor, reoccur – because it could evidence a systemic problem or failing in the way the Target manages and protects personal data. In addition, past data breach incidents may have eroded the Target's goodwill and reputation among its customers, thereby affecting the Target's bottom line in the long run.

Managing "Red Flags"

It is important for an Acquirer to be aware of privacy red flags in an M&A Transaction, as a breach of data protection laws or involvement in a data breach incident may have serious adverse effects to the Acquirer or the Target.

Not all red flags are deal breakers. Acquirers who wish to proceed with an M&A Transaction despite the presence of privacy red flags should take adequate steps to mitigate their impacts – financial or otherwise – to the Acquirer and to the Target. Such mitigating measures could include:

- I·seeking suitable R&Ws in the transaction documentation;
- seeking a commensurate indemnity from the Target;
- negotiating a lower purchase price;
- withholding retention monies;
- requiring the Target to remedy any privacy-related infirmities as a condition to closing; and/or
- developing a comprehensive post-completion privacy program for the Target.

Other practical processes that can assist the due diligence include as follows:

- Organise policies and procedures according to the target subject (employees, customers and/or suppliers).
- Consider the performance / effectiveness of the policies and procedures throughout the data's life cycle.
- Ensure the Target's databases of personal data have been collected in accordance with the relevant privacy and data protection laws (eg, transparency and legitimacy requirements). To this end, testing the customer journey is usually a good practice in digital / online Target businesses.
- Depending on the volume of data subjects and/or requests, test the effectiveness of the Target's processes for managing data security breaches and responding to exercised rights as part of the due diligence process.
- Check that the records of data processing activities have the required minimum content (and not only as a data processor, but also as a data controller).Check the dates of last monitoring by the person in charge of maintaining the Target's records. Ask in the due diligence questionnaire "how" the records are kept up to date.
- Inquire about the different versions of risk documents and whether there is an implementation plan and/or monitoring program which will assist in assessing their effectiveness (especially if there is no possibility of auditing them technically or on site).

Common Representations And Warranties about Privacy and Data Protection in M&A Transactions

As outlined above, the risk of non-compliance with privacy and data protection laws may result in severe negative consequences, particularly for the Acquirer and the ongoing operation of the business. Therefore, M&A Transaction agreements must provide for strong representations and warranties **(R&Ws)** to be given by the Target to the Acquirer.

R&Ws are commonly used to frame the liability of the parties in the M&A Transaction. They are key to assure the truthfulness of facts declared by the Target, and the compliance of actions and behaviours to be compelled by the Target.

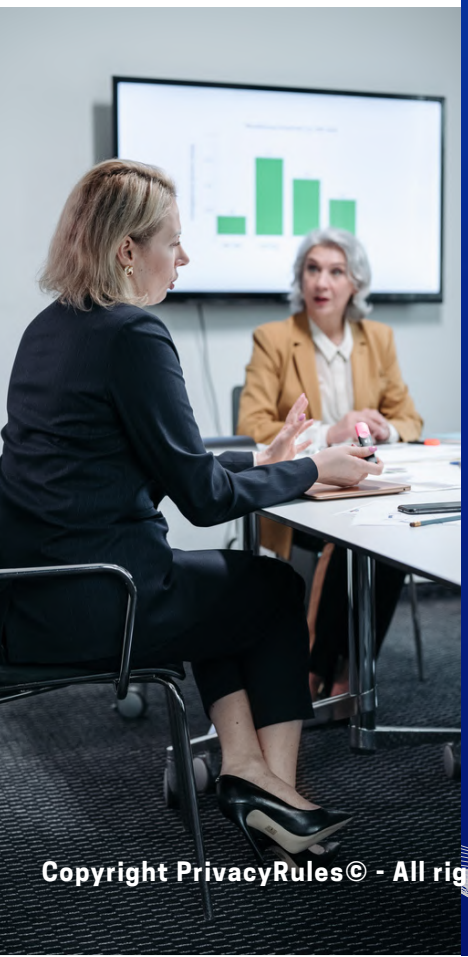
R&Ws can be used by an Acquirer to cushion potential privacy and data protection breaches committed by a Target. In order to properly draft the R&Ws provisions of the agreements, the following should be identified early in the due diligence phase:

- the data processing activities conducted by the Target;
- the privacy-related environment in which the Target conducts its business; and
- an evaluation of the associated risks and liabilities.

The most common risks can be found in:

- Contingencies involving privacy and data protection matters (eg, information security incidents, violation of data subjects' rights, law suits, administrative proceedings, etc.);
- "Blind spots" due to insufficient knowledge of the Target's data flows and relevant processing; and
- Data protection compliance that actually exists only "on paper", and not as a living and evolving element of the Target's internal practices.

Assessing the potential financial impact of a privacy risk can be challenging, as there are a number of factors that are difficult to predict with certainty. However, there are several strategies that can be used to estimate the potential impact of a privacy breach on the M&A Transaction:



Historical precedents:

One approach is to look at historical precedents for similar privacy breaches, and estimate the potential cost based on the severity of the breach and the regulatory response. For example, if a company similar to the Target Company has been fined one million dollars for a similar breach, this can be used as a benchmark for estimating the potential financial impact of a breach by the Target Company.

Cost-benefit analysis:

Another approach is to conduct a cost-benefit analysis that compares the potential financial impact of a privacy breach against the expected benefits of the M&A Transaction. This can help the Buyer to determine whether the potential risks and liabilities associated with the Target Company's privacy practices are outweighed by the potential benefits of the acquisition.

External support:

When privacy risks in the due diligence have been identified as very high, a good strategy to save the deal is to assess the ability to mitigate against those risks after the purchase. If risks are easily solvable in the short term, it may be in the Buyer's interest to continue with the deal and hire a privacy professional to remediate them. This is both a commercial and an awareness-raising strategy that is highly effective for the privacy professional.

Recommended base standards for R&Ws

In general, a sophisticated set of R&Ws should cover at least the standards as set out in Table 1:
Table 1. R&W Standards

Standard	Comment
Compliance	(a) Compliance with the applicable laws related to privacy, data protection and information security in the relevant jurisdiction/s; (b) Compliance with the Target's own policies, representations to clients, employees and suppliers under policies, codes of conduct and/or agreements and applicable industry standards; and (c) Compliance with notices, statements, consents and other communications provided to data subjects regarding the processing of their personal data.
Adoption of measures	(a) To ensure continued compliance with the compliance matters listed above; (b) To guarantee information security, including loss, damage or unauthorised access, use, modification or other misuse of any personally identifiable data processed by the target company; and (c) To guarantee that suppliers and other data processors follow a certain level of data protection compliance
Hold harmless	(a) Provisions regarding past, pending or threatened claims, actions, disputes or complaints regarding the processing of personal data filed by individuals, administrative authorities or any third parties.

R&Ws can indeed offer a certain level of comfort to Acquirers, but they cannot be treated as a universal cure. Even if compensation is paid to the Acquirer by the Target due to the favourably drafted R&Ws, they may not be sufficient to allow for the recovery of public relations and customer relationship damage that is often associated with privacy and data protection failures (and for which the adverse effects may be substantial).

Other practical matters that impact on R&Ws are as follows:

- Execute a contract (a data sharing agreement) between the Target and Acquirer. In addition to the arrangement on how and when data will be exchanged, this contract could stipulate that the prospective Acquirer:
    - undertakes to comply with applicable legislation regarding the processing of personal data;
    - undertakes to keep the data confidential and to use it only in connection with the proposed M&A Transaction;
    - commits to delete the data if the M&A transaction is not successfully concluded;
    - commits to inform data subjects about receiving their personal data in accordance with applicable legislation;
    - commits not to transmit the data internationally (barring very specific and exceptional circumstances - and then coupled with an adequate international data transfer mechanism); and

- undertakes to handle any data subject requests forwarded to it by the Target after the M&A Transaction has taken place.

The data sharing agreement could also stipulate that the Target:

- undertakes to forward to the Acquirer any data subject request it receives; and
- undertakes to delete any copies of the data after the transaction.

- Use the correct terminology and refer to the correct privacy and data protection legislation in all relevant M&A Transaction documents (eg, Business or Asset Sale / Purchase Agreement, Data Sharing Agreements, etc).
- Review any privacy related litigation or regulatory actions that the Target has been involved in, as well as any pending investigations or enforcement actions. This will help to identify any potential liabilities or reputational risks to the Acquirer associated with the Target's privacy practices.
- Identify the Target's risk management system and sample contracts according to the type of recipient. This can be used to make an approximation of the level of compliance of the contracts and the level of compliance with the Target's duty to inform.
- Ensure that any privacy risks associated with the M&A Transaction are properly disclosed in the deal documents, including any R&Ws made or to be made by the Target . This will help to protect the Acquirer from potential legal liabilities and reputational damage.

Considerations for sharing / disclosing personal data

The sharing / disclosure of personal data and databases does become an increasingly important aspect of an M&A Transaction as the Acquirer's due diligence progresses. For both Targets and Acquirers, there can be several challenges either inhibiting or allowing this process to occur.

Some of the main challenges of sharing personal data in M&A Transactions, include as follows:

Contractual requirements for confidentiality

Some of the Target's contracts with customers, vendors and other stakeholders (material or otherwise) may contain clauses as to confidentiality and non-disclosure, which may contractually prohibit the Target from sharing both (a) the fact and existence of the arrangement, and/or (b) its contractual content. This can impact the Acquirer's ability to assess the Target's contractual obligations, and the associated risks.

Legitimate Basis for processing:

In many jurisdictions, there are also strict requirements to only disclose personal data when there is an actual need to do so (ie, principles of necessity and data minimisation).

Sharing data "too early":

It is often important that personal data is not shared too early in the M&A Transaction. It can sometimes be common for the Target's documents, data and other to be provided or made available to the Acquirer "in bulk" (eg, into the M&A Transaction data room), before due consideration has

been given to the contractual and regulatory requirements applying to such records. Unintended and/or unnecessary disclosures can therefore occur.

Regulatory expectations:

In some jurisdictions, the privacy regulators and authorities may also impose statutory requirements or expectations for individuals **(data subjects)** to be informed of the impending M&A Transaction, or even in some situations, to give their consent. This becomes a prohibitive consideration when shielding knowledge of the proposed M&A Transaction from the marketplace is paramount. Informing data subjects is an obligation of almost every data controller, even though this is probably not done systematically in practice.

Considering the impact of the M&A Transaction on data subjects

An M&A Transaction can have tangible impacts on data subjects – from the dissemination of their personal information to other entities, to changes to data flows, to dealing with new 'owners'.

To minimise the impact of an M&A Transaction on data subjects, the Target and Acquirer should consider the following:

- obtain consent from data subjects for the transfer of their personal data to the Buyer (depending on the requirements of the applicable legislation), or implementing measures to ensure that data subjects are transparently informed about the transfer of their data and their privacy rights;
- report the impact of the deal on the privacy rights of employees, customers, and other stakeholders, and have the Target work with the Acquirer to develop strategies to mitigate any potential negative impacts. In general, it is important to ensure that data subjects are informed of the transaction and any potential impact on their personal data in a clear and transparent manner.

Beyond those cases where the law specifically provides for an obligation to inform about the transaction for one of the parties, whenever the Target has an existing relationship with the data subjects, it may be appropriate for the Target to take the lead in informing them about the M&A Transaction.

If the Target is unable to inform the data subjects or if it is more appropriate for the Acquirer to take the lead, then the Acquirer should take steps to ensure that data subjects are informed about the M&A Transaction and any impact on their personal data. In either case, the communication can be made directly or through other methods, such as a website notice or email notification, but it shall always be clear and concise and include sufficient information about how the data subjects' personal data will be processed as a result of the successful close of the M&A Transaction.

Managing data sharing challenges

When attempting to overcome data sharing and disclosure challenges to allow the M&A Transaction to progress, the intentional and phased "step by step approach" as set out in Table 2 below can be suitable. In this regard, personal data is gradually disclosed by the Acquirer to the Target, on as "as needed" and "need to know" basis, as the various milestones of the M&A Transaction are achieved.

Table 2: Step by step approach

Step #	Description	Type of personal data	Recipient
1	Initial offer (Target shares general data with prospective Acquirers so that they can determine whether or not they might be interested in the M&A Transaction (or such part of it))	Summary and anonymized data The prospective Acquirer knows: • The name of the Target; • The activities of the Target; • The nature of data for sale (eg, customer database, driver database, etc); and • The number of records in the database (e.g, number of customers on file if each customer is one record). The prospective Acquirer **does not** know: • The concrete data from the records; or • The name of the columns from the database (eg, name, first name, email address).	Large number of potential prospective Acquirers
2	Serious interest (Target shares an anonymized sample of the database)	Restricted and anonymized data In addition to everything from Step (1) above, the prospective Acquirer knows: • A limited and anonymized portion of the database (eg, a 10% sample of the records); • The name of the columns from the database (eg, name, first name, email address); and • Technical data related to the database (e.g. file format). The prospective Acquirer **does not** know the concrete data from the records.	Limited number of interested prospective Acquirers
3	Information to Stakeholders	Personally identifying data Upon confirmation of the prospective Acquirer's interest the Target should communicate (as appropriate and relevant): • its privacy statement to the affected data subjects; • its intention to pass on the personal data to the prospective Acquirer; • the necessary technical and organisational measures contextual to the M&A Transaction;	Limited number of interested prospective Acquirers

- the opt-out or opt-in mechanism available to the data subjects*; and
- the procedure for data subjects to follow to oppose the transfer or to give consent*.

After the expiration of the stated period, the Target should delete or withhold the personal data of the data subjects who have opted-out or have not opted-in within the stated period.

4	Transaction is quasi-fixed (Target may share the data from the database. However the Target should share the data as much as possible in pseudonymised form)	Complete and pseudonymized data The Target and the Acquirer enter into a contract (eg, data sharing agreement), specifying the uses and disclosures to which the personal data can be put.	Prospective Acquirer with whom the M&A Transaction will take place

* Whether the Target should use an opt-out or opt-in mechanism, depends on the type of transaction and the national legislation applicable to the parties.For example, it could be that the prospective Acquirer offers the same services as the Target and that the Acquirer will continue to perform the already existing contract between the customer and the Target. In such case, it could be sufficient for the Target to use an opt-out instead of an opt-in mechanism.

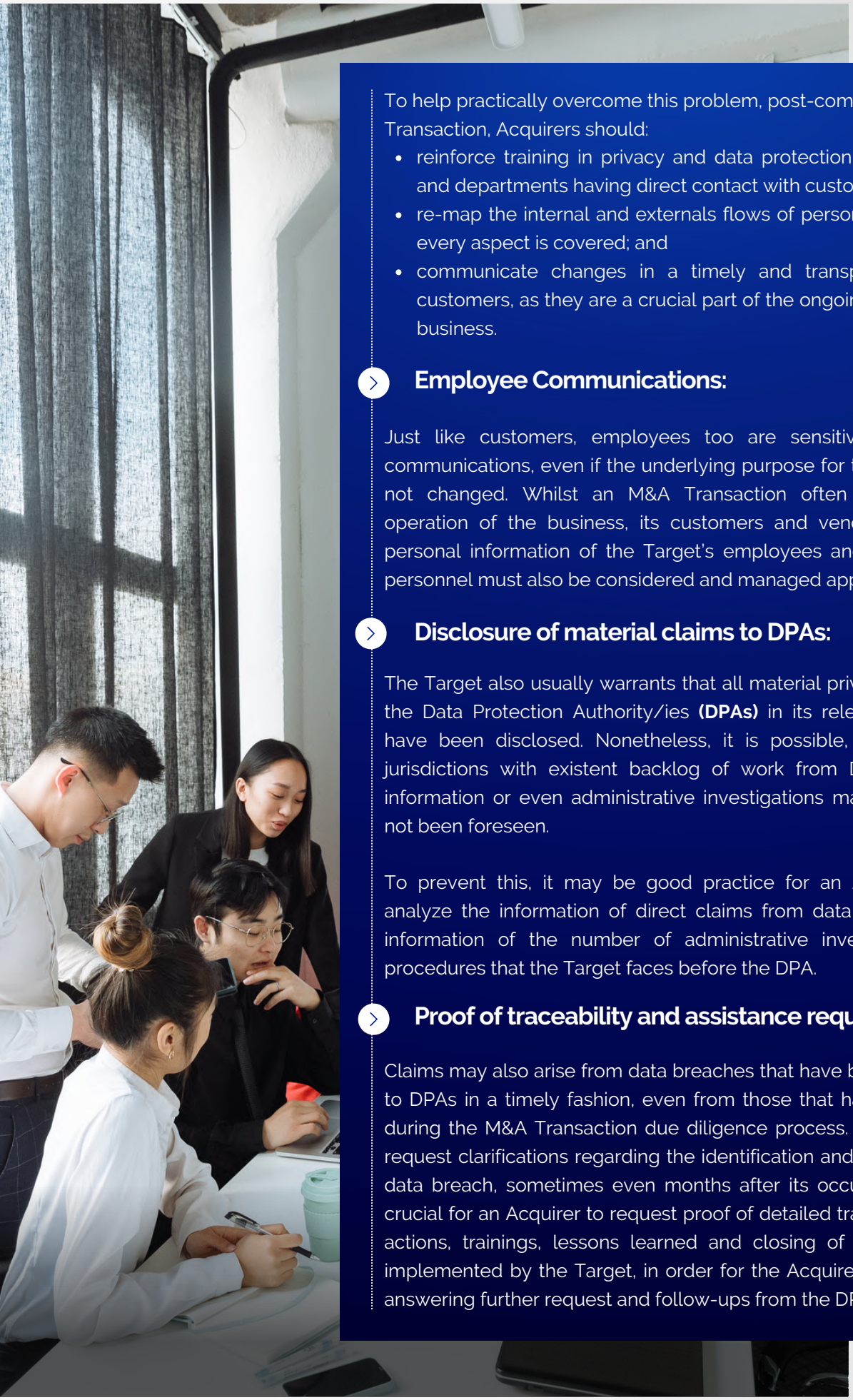
Examples Of Common Claims – R&Ws

During the transition phase of a successfully settled M&A Transaction, there might be privacy and data protection claims that stress the warranties given pre-completion by the parties.

Common examples of R&W claims occur in the following scenarios:

Adequacy of Consent:

A Target usually warrants having obtained appropriate consent from its customers (data subjects) for the processing of their data (often including for marketing purposes). In M&A Transactions involving business-to-consumer activities, the Acquirer commonly wants to adopt a different approach for communicating with customers (eg, utilizing more aggressive marketing campaigns (resulting in higher frequency of publicity messages), or utilizing new technologies (such as bots, AI and others) for customer service channels). Customers are sensitive to changes in communications, even if the underlying purposes of processing do not change. Thus, the amount of disconformity and claims may rise, giving the Acquirer the perception of an elevated risk compared to the one measured before the M&A Transaction.



To help practically overcome this problem, post-completion of the M&A Transaction, Acquirers should:

- reinforce training in privacy and data protection for the personnel and departments having direct contact with customers;
- re-map the internal and externals flows of personal data, to ensure every aspect is covered; and
- communicate changes in a timely and transparent manner to customers, as they are a crucial part of the ongoing acquired Target business.

Employee Communications:

Just like customers, employees too are sensitive to changes in communications, even if the underlying purpose for the processing has not changed. Whilst an M&A Transaction often focusses on the operation of the business, its customers and vendor contracts, the personal information of the Target's employees and other workforce personnel must also be considered and managed appropriately.

Disclosure of material claims to DPAs:

The Target also usually warrants that all material privacy claims before the Data Protection Authority/ies **(DPAs)** in its relevant jurisdiction/s have been disclosed. Nonetheless, it is possible, at least in some jurisdictions with existent backlog of work from DPAs, requests of information or even administrative investigations may arise, that have not been foreseen.

To prevent this, it may be good practice for an Acquirer to jointly analyze the information of direct claims from data subjects with the information of the number of administrative investigations and/or procedures that the Target faces before the DPA.

Proof of traceability and assistance required:

Claims may also arise from data breaches that have been duly reported to DPAs in a timely fashion, even from those that have been mapped during the M&A Transaction due diligence process. DPAs are likely to request clarifications regarding the identification and management of a data breach, sometimes even months after its occurrence. Thus, it is crucial for an Acquirer to request proof of detailed traceability of all the actions, trainings, lessons learned and closing of a data breach as implemented by the Target, in order for the Acquirer to be capable of answering further request and follow-ups from the DPA.

Finalisation of material claims:

A common warranty included from an Acquirer is to culminate any required proceedings before the DPA/s during the M&A Transaction transition period (such as before the data base registry). Although this may seem as a merely formal obligation, it may be crucial for a Target to assure its prompt compliance, as a Target will likely continue to hold potential liability over all data bases, data breaches and claims as long as it is not notified to the applicable DPA/s and affected data subjects.

Privacy integration matters: post-acquisition

Once the M&A Transaction has been formally completed, it is important for the Acquirer to develop and implement a comprehensive privacy integration plan to ensure that the Target's privacy practices are fully and appropriately integrated into the Acquirer's existing privacy program. This may include developing a privacy policy for the combined entity, conducting privacy training for employees, and ensuring that all data processing activities are compliant with applicable privacy laws.

Some of the most challenging tasks involved in this process include as set out in Table 3 below.
Table 3:Integration challenges

Challenge	Comment
Alignment between privacy programs	One of the most challenging tasks in privacy integration is ensuring that the Target's privacy program aligns with the Acquirer's pre-existing privacy program. This can involve identifying any gaps or inconsistencies between the two programs and developing a plan to address them.
Mapping personal data flows	The Acquirer must understand the personal data flows within the Target and ensure that they are integrated into the Acquirer's privacy program. This can be challenging when dealing with large volumes of data or complex data processing activities.
Developing new policies and procedures	The Acquirer may need to develop new privacy policies and procedures to address any gaps identified during the due diligence process or as part of the integration plan. This can be time-consuming and require input from a range of stakeholders, including legal, compliance, and IT teams.
Communicating changes to stakeholders	Any changes to privacy policies and procedures must be communicated to relevant stakeholders, including employees, customers, and vendors, etc. This can be challenging, particularly when dealing with large or geographically dispersed stakeholder groups.
Ensuring ongoing compliance	Once the privacy integration plan has been implemented, it is important to ensure ongoing compliance with applicable privacy laws and regulations. This may involve regular audits, periodic refresher training programs, and the appointment of a dedicated DPO, etc.Policies and procedures need to be understandable to the target subject and updated to and reflective of current laws.

When it comes to integrating the Target's privacy program into the Acquirer's pre-existing privacy program, there is no "one-size-fits-all approach". Ultimately, the goal of the privacy integration plan should be to ensure that the privacy program is optimized – so, whether to replace key personnel roles such as the DPO, or create coordinated teams, or to utilise other approaches, will depend on the specifics of the M&A Transaction and the ongoing privacy and data protection compliance needs of the Acquirer.

A specific case study example of how such implementation can go wrong, is set out in Annexure A.

Conclusion

The careful consideration of privacy and data protection matters are critical to the overall success of an M&A Transaction, and the Acquirer's future operation of the Target business. Whilst other commercial aspects of the deal will compete for attention, privacy compliance throughout the process is fundamental, is not just a tickbox, and cannot be relegated to just a post-completion fix.

Early engagement with all stakeholders, and the involvement of both external privacy professionals and your internal business teams (management, sales, customer service and human resources is vital.

ANNEX A
HONG KONG CASE STUDY: DATA SHARING AFTER AN M&A TRANSACTION

An investigation by Hong Kong's Office of the Privacy Commissioner for Personal Data **(PCPD)** into the healthcare conglomerate EC Healthcare serves as a lesson on how an Acquirer should deal with personal data it has acquired in an M&A Transaction.

EC Healthcare is a Hong Kong-listed company which owns various businesses and brands. Its business has developed through organic growth and acquisitions. Its current branded business lines include Primecare Paediatric Wellness Centre **(Primecare)**, Dr Reborn, New York Medical Group **(NYMG)** and re:HEALTH, each conducting business through separate companies.

The PCPD found that EC Healthcare breached its obligations under the Personal Data (Privacy) Ordinance **(PDPO)** when sharing the personal data of customers between its various businesses where some of the personal data was obtained in an acquisition.

The complaints

The investigation originated with two separate complaints lodged by citizens in 2021.

The first complaint concerned the personal data of the complainant's daughter and her grandmother. In June 2018, the daughter visited Primecare, and provided the personal data of herself and the phone number of her grandmother to Primecare. Fast-forward to 2020, the grandmother, who had been using the services provided by Dr Reborn, noticed that a text message from Dr Reborn included the daughter's name. The grandmother was informed by a staff that her personal data had been transferred to Dr Reborn. Having learnt about the incident from the grandmother in 2021, the mother of the daughter lodged a complaint with the PCPD.

The second complaint concerned the personal data of a different complainant. In 2016, the complainant received treatment from NYMG, and provided his personal data to NYMG. Then, in July 2021, the complainant contacted re:HEALTH to follow up with a complaint lodged by his family member against re:HEALTH. He provided the staff of re:HEALTH with his phone number and surname, and found out that re:HEALTH had access to his full name and the date of his last visit to NYMG. He then lodged a complaint with the PCPD.

The PCPD remarked that both complaints involved "personal data" defined under the PDPO, as the staff member of Dr Reborn and re:HEALTH was able to directly or indirectly identify the customer concerned by imputing the telephone number of a customer into the system.

The PCPD's findings

It was found that different businesses of EC Healthcare had access to information provided by customers to other businesses of EC Healthcare. This was due to the use of an integrated internal customer database system (Customer Database). The Customer Database was used by 28 of the 39 brands under EC Healthcare.

Primecare and NYMG, two of the subject companies under the complaints, were acquired by EC Healthcare after they collected the personal data of the concerned data subjects in the two complaints. The personal data of these two businesses were subsequently transferred and stored in the Customer Database, and were then shared among and accessible by the 28 brands of EC Healthcare after the acquisition.

Neither Primecare nor NYMG informed the concerned data subjects prior to the acquisition that their personal data would be stored in the Customer Database of EC Healthcare, and that their personal data would be accessible by the staff of other brands under EC Healthcare.

The PCPD found that EC Healthcare has contravened Data Protection Principle 3 of the PDPO. This data protection principle requires that express and voluntary consent of the data subject is required before personal data can be used for any new purpose other than the purpose for which the data was to be used at the time of the collection of the data, or a purpose directly related to that purpose.

Enforcement

As a result of the contravention, the PCPD served an enforcement notice on EC Healthcare and directed it to take various remedial actions, including to:

01

cease and prohibit the sharing of customers' personal data among different brands unless such sharing was notified to the customer upon collection of personal data or has been expressly consented to by the customer;

02

ensure that future integration of personal data obtained from clients in the Customer Database and future sharing among group companies under EC Healthcare is lawful;

03

formulate written policies and guidelines to instruct staff on the permissible use of and access to customers' personal data in the Customer Database; and

04

provide training to staff.

Non-compliance with an enforcement notice issued by the PCPD is a criminal offence and may attract fines up to HKD 100,000 (approximately USD 12,800) and imprisonment for two years.

Key points

The investigation into EC Healthcare by the PCPD offers a real-life example of the consequences of the failure to consider the legal implications of the transfer, disclosure and use of personal data after an M&A Transaction.

It is important to address potential data privacy issues proactively before they arise. Before undertaking an M&A Transaction, both the Target and the proposed Acquirer should:

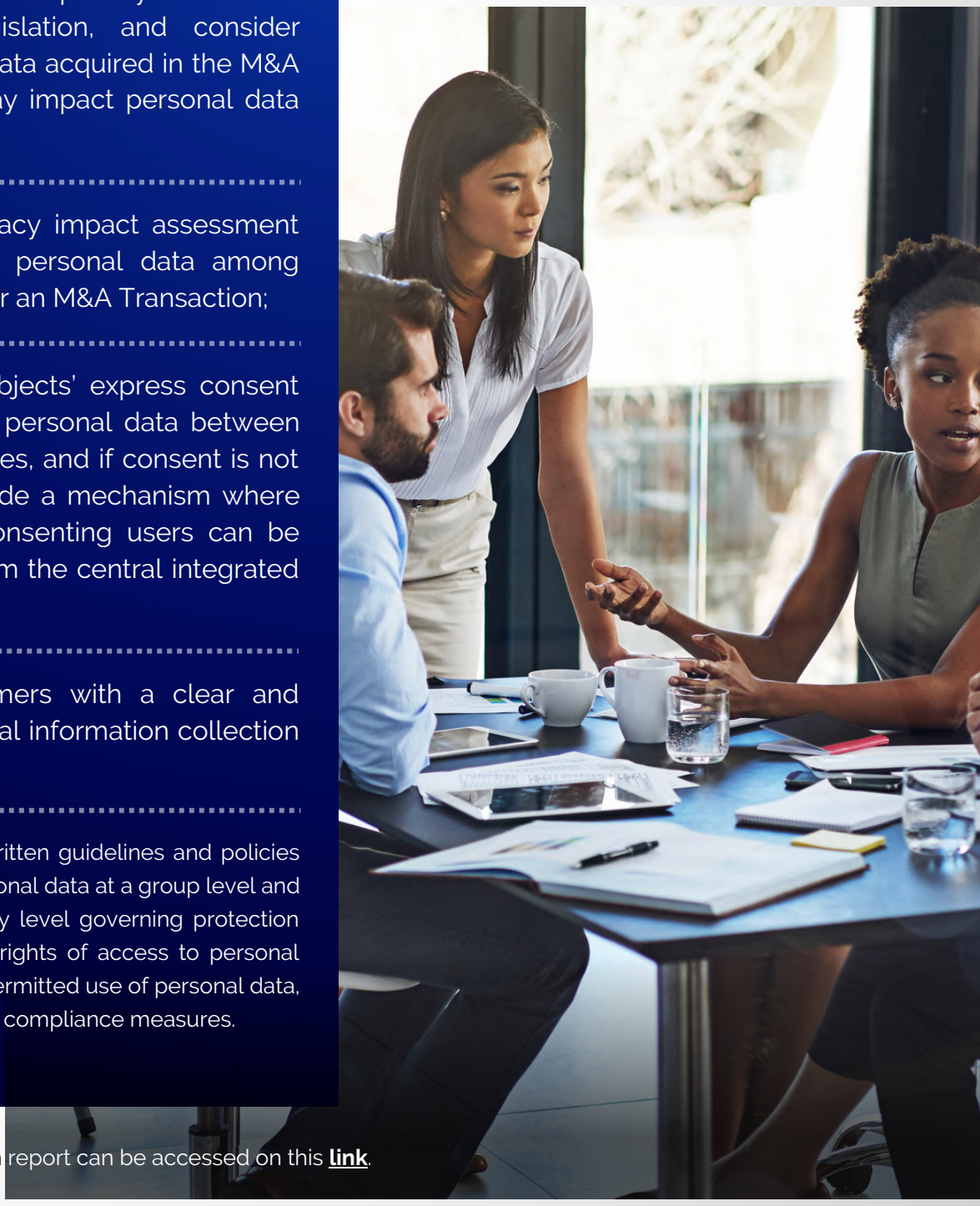
01 consider requirements for the disclosure and transfer of personal data under applicable privacy and data protection legislation, and consider how merging data acquired in the M&A Transaction may impact personal data privacy;

02 conduct a privacy impact assessment before sharing personal data among companies after an M&A Transaction;

03 obtain data subjects' express consent before sharing personal data between group companies, and if consent is not obtained, provide a mechanism where data of non-consenting users can be segregated from the central integrated system;

04 provide customers with a clear and concise personal information collection statement; and

05 formulate clear written guidelines and policies on the use of personal data at a group level and an operating entity level governing protection of personal data, rights of access to personal data, lawful and permitted use of personal data, and other relevant compliance measures.



The full investigation report can be accessed on this **link**.

AUSTRALIA : MACPHERSON KELLEY	**KELLY DICKSON** KELLY.DICKSON@MK.COM.AU	macpherson kelley.
BELGIUM : TIMELEX	**GEERT SOMERS** GEERT.SOMERS@TIMELEX.EU	TIMELEX
BRAZIL : TOZZINIFREIRE ADVOGADOS	**LUIZA SATO** SATO@TOZZINIFREIRE.COM.BR	Tozzini Freire. ADVOGADOS
COLOMBIA : VANEGAS MORALES CONSULTORES	**STELLA SOFÍA VANEGAS** SVANEGAS@VANEGASMORALES.COM **ANGELA NOGUERA** ANOGUERA@VANEGASMORALES.COM	VM VANEGAS MORALES Consultores
HONG KONG: TANNER DE WITT	**PÁDRAIG WALSH** PADRAIGWALSH@TANNERDEWITT.COM **CHRISTIE CHEUNG** CHRISTYCHEUNG@TANNERDEWITT.COM	Tanner De Witt solicitors
SINGAPORE : ORIONW LLC	**WINNIE CHANG** WINNIE.CHANG@ORIONW.COM	ORIONW
SPAIN : ROCAJUNYENT	**BEATRIZ RODRIGUEZ GOMEZ** B.RODRIGUEZ@ROCAJUNYENT.COM	RocaJunyent

This article has been prepared by members of the **PrivacyRules alliance**, a global network of legal, cyber and communications experts around the world.

CONTACT US

PrivacyRules

American Headquarters:
PrivacyRules, Ltd.
151 West 4th Street
Suite 200
Cincinnati, OH 45202, USA

European Office:
Via dei Della Robbia 112,
50132, Firenze
Italy (IT)

Email
info@privacyrules.com

www.privacyrules.com