DLA PIPER

27 AUGUST 2014

PRIVACY AND M&A TRANSACTIONS: THE DO'S AND DON'TS

PRIVACY UPDATE

Most M&A transactions require parties to exchange at least some personal information, whether it is the seller's employee or customer personal information. Addressing privacy compliance at an early stage of the M&A transaction allows sufficient time for remedial steps, both in terms of the transaction and the target's compliance, to be taken.

While privacy concerns are often overlooked in M&A transactions (at least until after the transaction has completed), since 12 March 2014 the new re-invigorated Australian Privacy Principles (**"APPs"**) together with the very real prospect of fines for breaches of up to $1.7 million means that privacy compliance is now an important issue in M&A transactions (and a potentially costly one if not addressed). That is, compliance both in terms of (i) the transfer and collection of personal information as part of the transaction and (ii) the target with privacy law in conducting its business.

If the transaction involves business operations or related entities in other jurisdictions in the Asia Pacific region you should note that significant legislative advancement on the privacy/data protection front has occurred in this region over the last 2-3 years. Advancements such that it will be necessary to consider the privacy/data protection obligations and impacts in each relevant Asia Pacific jurisdiction. Also, given the EU has been the leader in data privacy protection and is currently considering fines for non-compliance of up to 2% of the annual turnover of organisations, any transaction touching on an entity based in or conducting business in Europe should be especially careful to consider privacy/data protection compliance.

Before we consider the Do's and Don'ts it is important to remember the APPs/Australian privacy law covers the collection, use and disclosure of *"personal information"*, being any information or opinion relating to an identified or identifiable individual. The contact details of an individual business contact at a customer or vendor are personal information, for example.

A subset of personal information is *"sensitive information"* which is personal information that relates to or refers to an individual's health, sexual preference, racial or ethnic origin, political

opinions, religious or philosophical beliefs, trade union membership, criminal conduct and/or genetic/biometric information (to name a few).

The collection/use of personal information requires prior notice of certain mandatory matters and for sensitive information requires the unambiguous prior consent of the relevant individuals. In addition, transfer of personal information outside Australia requires that certain obligations first be met by the transferee and, in most cases, the transferee will continue to be liable for such personal information sent outside of Australia, including for any actions of the recipient offshore that, if conducted onshore by the transferee company, would have been a breach of the APPs.

DO'S RELEVANT FOR ANY COLLECTION, USE AND/OR DISCLOSURE OF PERSONAL INFORMATION (AS WELL AS IN THE M&A CONTEXT)

We recommend that any company obtaining or using personal information (even if provided as part of a due diligence):

- Designate a person or team to be responsible for privacy issues/compliance.
- Limit collection/disclosure of personal information to a minimum.
- Limit internal and external distribution of personal information to a *"need to know"* basis.
- Use only secure methods to share personal information (eg use of the basic version of Dropbox, with limited security and inability to track on forwarding of information, will not be appropriate).
- Be particularly careful with sensitive information including ascertaining the right to use it for the purposes required and to disclose it to a potential purchaser in an M&A transaction, for example -
    - Ensure that the company is aware of when it is required to give notice to and/or obtain consent from those individuals whose personal information is being disclosed/collected.
    - Ensure personal information is deleted or de identified when it has been used for the notified purposes.

At all stages of an M&A transaction, from initial contact or the MOU to the completion/implementation of the transaction, privacy issues need to be addressed by both buyer and seller.

In particular, although often overlooked, the receipt of personal information by a potential buyer from the seller as part of the due diligence process is a *"collection"* of personal information by that potential buyer and therefore must comply with the APPs. The potential buyer, on receipt of such personal information from the seller (or other third party), has its own primary privacy obligations with respect to notice and the holding and use of such information) under the APPs. Also, should a potential buyer not proceed with the transaction, the APPs impose an obligation on that potential buyer to de-identify or destroy such personal information.

FOR SELLERS

Just like in other areas of its business requiring compliance, a seller should ensure that they are in good/compliant privacy shape in order to ensure a smooth transaction. This includes ascertaining that all relevant privacy policies and processes are in place and that:

- Any prior notice/purposes notified to individuals cover the intended disclosure to potential buyers as part of a due diligence.
- Appropriate technical and organisational security measures are in place to prevent unauthorised, unlawful or accidental loss, destruction of or damage to the information.
- If the information is to be disclosed outside Australia, such purposes and disclosures have been notified/consented to in the relevant documentation prior to or at the time of collection.
- For sensitive information, the seller has each individual's consent to disclose that information for the purposes of the due diligence.

Of course, if the Seller's existing privacy policy/notice originally provided on the collection of personal information does not (or cannot be construed to) cover the disclosure of personal information to a potential buyer as part of a due diligence, in most cases it is going to be impractical/not appropriate to provide relevant

notice/gain relevant consents for the due diligence disclosure (especially if the transaction is market sensitive or to be kept secret). Therefore, even if a sale is not currently being contemplated, review your privacy policy to see if disclosure of personal information in a due diligence scenario has been notified as a purpose/potential disclosure in your existing privacy policy/notice. If not, amend your policy now as you never know when this will come in handy.

FOR BUYERS

It is important that buyers not only consider the seller's general compliance with the APPs (or any relevant Asia Pacific privacy laws) in the conduct of the seller's business but also consider its own obligations in respect of receipt (ie collection), use and disclosure of any personal information provided to it by the seller as part of the due diligence process.

As regards the collection of personal information as part of the due diligence process, buyers should consider:

- What obligations they have in respect of notification.
- If sensitive information is collected, what obligations they have with respect to obtaining consent.
- What warranties/guarantees are provided by the seller that it is able to provide such personal or sensitive information to (and for what purposes such can be used by) the potential buyer (and ensure they are included in the non-disclosure agreement and/or sale agreement).
- What obligations (both at law and pursuant to the non-disclosure agreement) apply to the potential buyer if the transaction does not proceed.
- What obligations (both at law and under the sale agreement) apply if the transaction does proceed.

In addition, when considering the compliance health of the seller, the buyer needs to also consider:

- The type of personal information collected, used and disclosed by the seller in its business.
- Whether appropriate notification has been given and/or consents obtained (this includes both the consideration of the relevant privacy policy or statement setting out the purposes for collection as well as the processes: that is, when and how such was delivered/obtained in the collection process);
- Identifying any compliance failures or areas of compliance concern and, if possible, get such remedied before completion.
- Ascertaining what areas of compliance concern need to be warranted/indemnified by the seller.
- Setting up a plan of action for post completion actions to fix any identified privacy compliance concerns.

Specific **Do's** for buyers in an M&A transaction (in addition to the ones mentioned above) include:

DO:

- Put in place appropriate information processing agreements with third party due diligence providers and check notifications to be provided to individuals (and/or consents to be obtained, if relevant).
- Identify personal information to be retained and to be transferred as part of the process.
- Implement appropriate technical and organisational security measures in respect of the transaction processes (eg information provided as part of the due diligence needs to be kept separately and destroyed/returned if the deal does not proceed).
- Assess/audit the target's privacy compliance.
- Confirm the ability of the target to lawfully use the relevant personal information and, if relevant, its ability to disclose/sell such information.
- Identify risks and either fix/reduce them or allocate liability for such in the sale/purchase agreement.

In addition to the ones mentioned above, some of the specific **Don'ts** for buyers in an M&A transaction include:

DON'T:

- Start the transaction process without having considered the privacy implications.
- Assume the target's compliance, you must perform your due diligence on this.
- Wait until the last minute to consider privacy compliance.
- Forget (or choose not) to implement relevant security measures in respect of the transaction process.
- Assume that the seller will provide all necessary information.
- Ignore or underestimate the privacy issues identified and their potential impact.
- Collect, retain or process as part of the due diligence process more information than is absolutely necessary for your legitimate purposes.
- Underestimate or ignore any post acquisition steps (or fail to implement such) required to achieve appropriate privacy compliance.

As with other M&A areas, the privacy issues noted above are not insurmountable. They will be "uncovered" through appropriate consideration and your due diligence and may be dealt with via pre or post transaction remedial action, allocation of risk through the agreement or otherwise. However it is clear that privacy, both in terms of the transaction processes (in particular, the due diligence) as well as the target's business compliance, is now an important consideration in all M&A transactions.

Please do not hesitate to contact any of our dedicated privacy team if you wish to discuss any of the matters raised in this Update or if we can assist you with privacy compliance in respect of any M&A activity or generally.

FURTHER INFORMATION

For further information on any of the topics discussed, do not hesitate to contact:

Alec Christie
Partner
T +61 2 9286 8237
alec.christie@dlapiper.com

Contact your nearest DLA Piper office:

BRISBANE
Level 28, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA
Level 3, 55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE
Level 21, 140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH
Level 31, Central Park
152–158 St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY
Level 22, 1 Martin Place
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 8007
sydney@dlapiper.com

www.dlapiper.com

JAB/TAH/AUM/1207236990.1