ALTANA
AVOCATS • PARIS

A FRENCH PERSPECTIVE: MITIGATING CYBER RISKS IN M&A DEALS

As in the US, data breaches and cyber threats can jeopardize M&A transactions or have detrimental impact. French and European rules make it specific in various respects.

JULIE CORNELY
M&A DEPARTMENT
ALTANA

SANDRINE CULLAFFROZ-JOVER
IT & DATA PRIVACY DEPARTMENT
ALTANA

The value of the target's data assets in mergers and acquisitions should not be estimated without a comprehensive knowledge of the technical and legal measures set up for its conservation.

Mitigating cyber risks in M&A deals allows buyers to make their acquisition at market value and secure the sustainability of the acquired IT-related assets.

A recent example of critical reputational impact and data protection related liability is the acquisition by TripAdvisor, of Viator, the tour-booking company, for $200 million, in August 2014. Just a month following the acquisition, a data breach led the buyer to notify roughly 1.4 million customers that data and personal details might have been compromised following said data breach (including customers' credit card information, email addresses and encrypted passwords). This could have been anticipated with a thorough technical and legal IT assessment in the scope of the deal.

Companies increasingly rely on data and new technology to conduct their businesses, gather and store substantial know-how, and extensively harvest sensitive data notably from their customers, third party suppliers and human resources.

The potential exposure of such valued information can directly impact M&A transactions when assessing the market value of a target's assets or its brand reputation.

Several industries are more vulnerable to cyber threat than others such as Financial Services, Defense, Telecom, Retail, Energy, and Pharmaceuticals.

When targeting French companies pertaining to these industries, buyers should perform cyber-security due diligence in order not only to assess compliance with European and domestic privacy Laws but also with sector-based regulation applicable to it.

Consequently, upstream verifications have become critical during the due diligence process in the scope of M&A transactions. If appropriate cyber-security due diligence used to be overlooked in M&A deals, the opposite has become the growing trend.

RISK IDENTIFICATION

When performing due diligence including cyber-security related issues, the analysis will need to focus on the IT infrastructure scheme of the target, outsourcing management agreements, internal processes and incident/response plans.

In addition, examination of the operational processes will require particular attention in order to highlight the lines of responsibility and effective control over the data flows within the target IT infrastructure.

The IT assessment should lead to a validation of the legal framework managing such data flows in order to ensure that the three following compliance-criteria are met: Confidentiality – Integrity & Availability.

From a buyer's and investor's perspective, cyber-security due diligence should be conducted to determine:

- the collecting, storage, use or processing means of valued information (including customer or employee-related personal data);
- the classification of the processed data (i.e. in order to determine whether such data is critical for the business);
- the storage location;
- the processing management;
- the applicable personal data policies, declarative requirements, security and disaster recovery plans, and all relevant IT agreements and their day-to-day monitoring;

- the applicable insurance policies and their actual coverage;
- the past and existing, as well as actual and pending, security incidents and data breaches.

From the seller's perspective, focus should be put on the secure disclosure of sensitive personal data to the buyer and its advisors in compliance with the seller's internal privacy policy and applicable domestic privacy Laws.

RISK MANAGEMENT

Depending on the due diligence findings, adjustments or protection may need to be negotiated through particularly:

IT-related documentation: when applicable, IT documentation may need to be upgraded so as to comply with the highest technical standard applicable within both entities as well as integrate the internal policies so as to preserve the value of the IT-related asset.

SPA: when applicable, provide in the SPA for:

- Conditions precedent pursuant to which corrective actions prior to Closing are to be carried out by the seller;
- Upward or downward price adjustment depending on the due diligence findings;
- Specific representations and warranties;
- Standalone indemnity procedure(s).

Insurance Coverage: when applicable, the buyer may have to increase insurance coverage in order to cover identified potential damages and data loss risks.

FOCUS: PRIVACY ISSUES ATTACHED TO VALUABLE IT ASSETS

IT assets will be considered a valuable asset if and only if compliant with applicable Laws. This is particularly true of customer databases.

French regulation is particularly stringent as regards privacy and data security protection and generally, the buyer will need to investigate the full compliance of the disclosed proceedings attached to those assets identified as key in the transaction with the French Data Protection Act *(Act n°78-17 of 6 January 1978 on information technology, data files and civil liberties).*

When performing this compliance analysis, points of attention will defer depending on when it takes place:

- **Pre-closing:** the buyer should pay particular attention to the declarative requirements fulfilled by the target prior to the acquisition of its customer database particularly since the French Supreme Court ruled on 25 June 2013 that the sale of a customer database can be purely and simply invalidated for failure by the former applicant (i.e. data controller) to comply with Data Protection Act declarative requirements (Act n°78-17 of 6 January 1978 on information technology, data files and civil liberties).
- **Post-closing:** the buyer will in most cases be tempted to combine its own customer database with the target's for marketing purposes. In such event, the combination of both customer databases will be deemed creating of a new processing for which the prior approval of the data subject (i.e. each individual whose data is collected) is mandatory regardless of the fact that purchaser and target belong to one and the same group post closing (CNIL, ruling n°01-040, June 28th, 2001).

In cross-border M&A deals, the buyer should, in the early stages of the due diligence, identify all legal restrictions prior to transferring any personal data across E.U. borders more particularly since the E.U.-U.S. Safe Harbor Framework has been recently invalidated by the European Court of Justice *(ECJ, October 6th, 2015, Maximillian Schrems case, C-362/14).*

Consequently, an analytic review of the target's IT agreements to red flag all references to Safe Harbor Framework should allow the buyer to anticipate the implementation of suitable alternatives, such as Binding Corporate Rules (BCR) or European standard contractual clauses.

ALTANA

Altana is a full-service business law firm with 60 lawyers, offering tailor-made legal assistance in complex cross-border and domestic transactions and litigation.

Our M&A team has a very strong international focus and several of our attorneys are admitted both to the Paris Bar and to the NY Bar. We advise on public and private mergers, acquisitions, divestiture, joint venture and carve out transactions, as well as group reorganizations. We work seamlessly with the other departments of the firm, including our IT & Data Privacy department.

KEY RECOMMENDATIONS

SELLER BE AWARE OF:

- Fulfilling of appropriate and mandatory declarative requirements for processing of personal data
- Ensuring compliance of in-house privacy policies with applicable privacy Law
- Setting up appropriate secured processes to preserve valued information
- Securing the disclosure of any sensitive personal data

BUYER BEWARE OF:

- Identifying and classifying target's valued IT-related assets
- Reviewing target's data storage, security, and recovery means
- Reviewing target's IT-related contractual documentation
- Adjusting the data security process in place within the target company
- Anticipating coverage of identified risk through the IT-documentation, the SPA and/or insurance coverage