M&A TRANSACTIONS AND THE NEW BRAZILIAN DATA PROTECTION LAW

M&A transactions involving entities processing personal data subject to the new Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados or "LGPD"*) will change when this legislation comes into force in August 2020. The LGPD will impact all those involved in the deal, the conduction of the due diligence, the structure of the deal, and the negotiation of the transaction documents.

When the target company processes personal data subject to LGPD, the seller, as a data controller, must put in place procedures to ensure that the transaction does not violate the LGDP. The seller must define the documents/information that are key for all those involved in the deal to evaluate the target businesses, and specific personal data may not be made available if it does not bring value to the transaction. Information that is not to be made available can simply be redacted from documents or summarized so as not to allow access to personal data. Providing for the anonymization and pseudonymization of personal data are additional alternatives to reduce the exposure to breaches of the legislation.

For personal data to be made available, definition of the legal basis for data processing is necessary to avoid breaches whether by the seller and/or by those that have access to such data. Procedures for the international transfer of data must be considered carefully if personal data is to be transferred abroad in the context of the evaluation of a cross-border transaction.

Those involved in the deal, whether the potential purchasers, the VDR service providers or the intermediaries must make sure that their access to personal data is lawful, since they will also become data controllers and will be subject to liabilities in the event of breach of law.

One of the alternatives for such third-parties is to make an initial verification as to whether the seller has put in place the necessary procedures for the lawful transfer of personal data. Other alternative is to negotiate contractual representations from the seller to the effect that adequate data protection measures were put in place before the actual access to data. Third-parties will also be required to have their own governance to comply with the LGPD (or another data protection law in case of cross-border deal), since their breach can lead to joint and several liability with the seller.

The LGPD will also affect due diligence proceedings. Failure by the target company to establish effective data protection governance can give rise to contingencies and the target company

may be subject to civil liability and administrative sanctions. The following are examples of diligence relevant check list:

(i) if the target company put in place a set of rules to protect personal data and has a legal basis for processing each set of personal data;
(ii) if such rules are enforceable (e.g., if there are opportunities for whistleblowers);
(iii) if there was any data breach incident;
(iv) if the target company appointed a data protection officer;
(v) if the contracts entered into by the target company have data protection provisions; and
(vi) if the target company employed software to ensure data protection.

Thus, diligence will encompass not only legal matters, but also information technology aspects. Provision of information must encounter the balance between data protection and the right of potential purchasers to obtain enough information to evaluate the transaction.

The LGPD may affect the structure of the deal whether it is an equity deal or an asset deal. In the context of an equity deal, equity interest in the target company will be transferred and no transfer of data is likely to occur, i.e., data will remain at target company's level. After the closing, when data processing changes the data protection practices of the target company or if any corporate restructuring is put in place, new verification of the legal basis for the data processing must be carried out.

In the case of an asset deal, when the transfer of assets/liabilities from the seller to purchaser encompasses personal data, the parties must verify the legal basis for such transfer. If the deal requires consent from a large number of data subjects, the parties should consider structuring it as an equity deal lest the transaction be jeopardized.

M&A transaction's documentation will be impacted by the LGPD as well. Purchase agreements will likely have representations and warranties in relation to the compliance with data protection laws to which the target company is subject. Warranties and indemnification provisions may also be laid down to deal with potential breaches of data protection laws by the target company whether prior or after closing of the transaction. Depending on the exposure of the target company to data protection liabilities, purchase price adjustments and other covenants may be set out.

Other ancillary agreements to be entered into in the context of an M&A transaction must also contemplate data protection provisions, particularly in cases where one of the parties will render services to the other after closing (e.g., technical services agreements).

The outbreak of data protection laws around the world (Brazil included) demonstrates the intent of governments to protect individuals' privacy, but they are not designed to pose unreasonable burden on investments and transactions.

Dealmakers will need to devise strategies that do not undermine the privacy of individuals. Although some transaction costs will likely increase, ensuring compliance with the legislation in all phases of the M&A will facilitate the negotiation and a favorable outcome of the transaction, reducing risks and securing privacy protection to the data subjects.

Author:
Daniel Tardelli Pessoa
dpessoa@levysalomao.com.br