Contacts

Dr. Benjamin Fehr, LLM
Attorney-at-Law
Partner, Leader Corporate Law/M&A
+41 58 792 43 83
benjamin.fehr@ch.pwc.com

Susanne Hofmann
ICT & Privacy Lawyer
Director, Leader of Legal Compliance
+41 58 792 17 12
susanne.hofmann@ch.pwc.com

Laura Fertitta
Attorney-at-Law
Corporate Law/M&A
+41 58 792 46 35
laura.fertitta@ch.pwc.com

Dr. Idir Laurent Khiar
ICT & Privacy Lawyer
Legal Compliance
+41 58 792 17 51
idir.laurent.khiar@ch.pwc.com

pwc

Data privacy law: a critical factor for M&A transactions

As of November 2018

Today, corporate decision makers are well advised to consider data privacy as early as possible. Finally, taking a broad view is paramount as some data privacy laws claim extraterritorial reach, such as the EU's GDPR, leading to a complex overlap of national and regional data privacy laws.

The views and opinions expressed are those of the authors.

A steady flow of news on loss and abuse of personal data has put data privacy high on the agenda of lawmakers. The EU's General Data Protection Regulation (GDPR) is representative for that global trend. Its high fines evidence a much stricter stance on data privacy at the moment.

In no way does this only concern social media companies. These stricter requirements on data privacy have also clear implications for the M&A business. Today, data protection poses substantial risks and may critically affect the success of M&A transactions. Further digitalisation of businesses and industries and the increasing importance of intangible assets of a target company is likely to increase its role and significance.

Corporate decision makers and lawyers must be able to anticipate and understand the growing role of data privacy in M&A as it affects transactions along its three distinctive phases.

Target list: value & strategy

Compliance risks & costs: A non- or semi-compliant target will ultimately drive post-merger costs up. Besides triggering the risk of heavy fines and reputational damages, compliance costs for implementing data protection gaps or remediation measures can be substantial, depending on the size and complexity of the target. Understanding the level of compliance with applicable data protection regulation or agreeing on a cost sharing are becoming important valuation steps.

Personal processing & asset valuation: Personal data such as data of employees, suppliers or clients may form part of a target's inherent value and may be the fundamental driver behind a transaction. Understanding the rules set by privacy laws for processing personal data is becoming a precondition for any successful business strategy. Unaddressed compliance questions can restrict the use of personal data. In a best case, they are hidden costs likely to be borne in the post transaction phase. In the worst case, they are true show stoppers.

Databases & competition regulation: Competition authorities show a growing interest in data driven industries. M&A transactions involving large databases (e.g. in telecommunications, marketing or retail business) may come under increased scrutiny with potential obligations or commitments that may substantially limit the anticipated combined use of databases.

Due Diligence: data room & transfers

Data room setup & risks: From an M&A perspective a disclosure of data between involved par-ties is mandatory to conduct a due diligence on the target, prepare the closing and finally mitigate the risks of a transaction. Privacy law also applies to data rooms. The provider of a data room is considered by law as acting as a data processor. However, the parties on whose behalf the provider acts are ultimately responsible for the provider's actions and, thus, the data room's compliance with privacy law. Neglecting this exposes the parties not only to the risk of heavy fines in the event of a data breach but also to substantial reputational damage. A proper data processing agreement (e.g. access restrictions, encryptions, anonymisation or blackening of data) and assurances to meet tough communication deadlines to authorities and potentially to concerned persons in the event of a data breach have become indispensable.

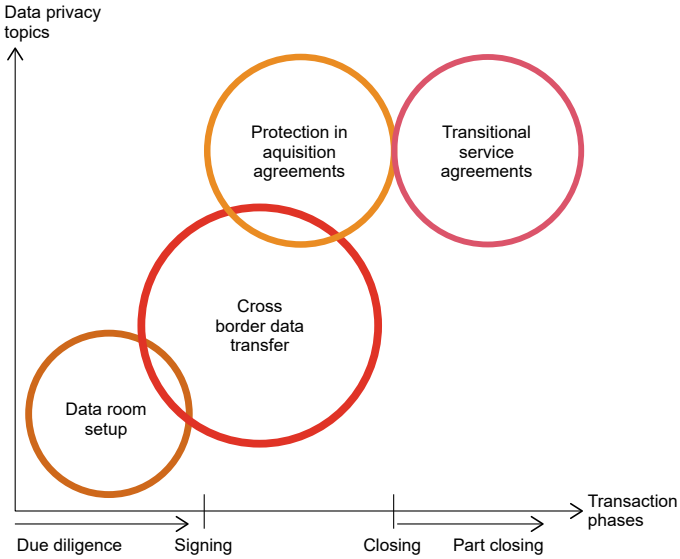
Cross border data transfer: Any transfer of personal data outside of the EU/EEA or Switzerland is prohibited without safeguards providing for an adequate level of data protection. Remote access by parties located in third countries also qualifies as transfer of personal data. Data transfer agreements with standard contractual clauses belong to the most used safeguards. In many instances, transfers of data to the United States may be based on self-certification within the Privacy Shield Framework. Data transfers absent of safeguards are likely to trigger major fines.

Structuring of the M&A transaction: Adequate level of data protection depends also on the structuring of the M&A trans-action. In the case of a share deal, the shares of the target will be transferred to the buyer. In general, data remains within target. The target continues to process its data and – at least in the first instance – no data will be transferred to third parties. However, this might change if the buyer integrates the target company in a group structure or intents to process personal data for other (commercial) reasons. In case of an asset deal, the assets and liabilities of the target will be transferred to the buyer, not the shares. In this case (personal) data may be transferred to third parties and the buyer must insure adequate data protection measures.

Post-acquisition integration: managing risks

Acquisition agreements: Representation and warranties, indemnities as well as purchase price adjustments are the contractual tools to address risks related to non-compliance with privacy law. In that regard, any information on data protection compliance obtained prior to or during the due diligence phase will prove highly valuable.

Transitional services agreements: Under certain circum-stances, transitional services agreements may also contain data protection-related parts. A data processing agreement may be necessary where a seller continues to process personal data on behalf of a buyer. Separation of specific intra-group process-ing activities from a parent company into separate companies (carve-outs) is possible. However, the legal responsibilities with regard to ensuring data protection compliance may ultimately remain with the buyer.



Conclusions

To sum up, corporate decision makers should consider the impact of data privacy law and compliance on:

- A target's risk and value;
- The anticipated or planned use of databases;
- The setup of data rooms and data transfers to third countries;
- The structuring of the M&A transaction; and
- The structuring of post-acquisition integration.

Today, corporate decision makers are well advised to consider data privacy as early as possible. Finally, taking a broad view is paramount as some data privacy laws claim extraterritorial reach, such as the EU's GDPR, leading to a complex overlap of national and regional data privacy laws.