Data protection in M&A transactions:

A how-to-guide
Data protection in M&A transactions: A how-to guide

The timeline for M&A transactions:

- Populating the data room
- Due diligence
- Drafting the SPA
- Other contract provisions
- Works council consultation
- Ancillary agreements
- Pre-closing integration
- Phase II antitrust requests
- Data uses / database integration
- Provision of transitional services
- Post-closing restructuring / remediation
Personal data is an important aspect of most M&A transactions as almost every company stores information about its employees and customers. For some deals, data is critical.

This how-to guide takes you through the steps of a typical M&A transaction, highlighting how personal data issues can affect deal processes, and how those issues are typically dealt with.

We have structured the guide in the form of a timeline, analyzing each stage of the transaction: pre-signing, signing, signing to closing, and post-closing.

**Stage I – Pre-Signing**

**Populating the data room**

Putting employee or customer data in the data room creates a number of privacy and data protection issues outside the United States, especially in the EU, Asia and other jurisdictions with comprehensive data protection regimes.

In the EU, wherever possible, the information disclosed in the data room should not identify individual employees, but instead be replaced with de-identified, pseudonymized or aggregated information. If this is not possible, the seller may consider reducing the amount of information shared to that which is strictly necessary, but in that case the individuals concerned must be informed of the processing and the purposes of such processing, which may not be possible due to deal confidentiality. Some EU member states are more restrictive regarding the provision of employee data in a data room. In Germany for example, only information about key employees which are critical to the transaction may be provided in the data room.

In addition, “sensitive information” – e.g., information which reveals an employee’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life – should be avoided altogether.

In Switzerland and Austria, not only data relating to individuals but also data relating to companies may also be covered by data protection laws.

Other jurisdictions impose stricter requirements. For example, in some circumstances, transferring personal information outside of Russia or China requires prior consent from the individual to whom that data relates.

A data processing agreement must be entered into with the entity hosting the data room. The data processing agreement must include provisions on data security.

Customer data may also include personal information. If so, personal data should be minimized, or – subject to the national privacy laws – even be redacted.

**Best practices**

- Redact/limit personal information (e.g. names and addresses) in the documents available in the data room.
- Provide model employment contracts rather than all contracts.
- Do not disclose sensitive personal information.
- Analytics tables without names could also be provided, such as table with the average presence in the company and average salary per function.
- Choose a secure data room provider complying with data protection laws.
- Ensure that all persons accessing personal data available in the data room are bound by confidentiality.

**Due diligence**

Data can be central to the valuation of the target. Due diligence can also reveal potential liabilities for data protection violations.

**Identifying material liabilities**

Countries throughout the world have enacted privacy and data protection laws, and new laws are being passed each year. Compliance with those obligations is increasingly
Data protection during pre-signing phase

complex and regulators are increasing civil penalties and, in some cases, making non-compliance criminal. In the United States, for example, recent amendments to the Health Insurance Portability and Accountability Act (HIPAA) allow HHS to impose penalties of up to $1.5m annually per type of violation. The Federal Trade Commission in the United States is entering into an increasing number of consent decrees with companies and imposing record fines for non-compliance. The White House and U.S. Congress will continue to push the private sector to greater action – and other governments, such as those in the EU member states, are not far behind. The proposed European General Data Protection Regulation intends to impose sanctions of up to 5% of a group turnover.

Any potential compliance liabilities can be identified through appropriate due diligence and a buyer can be advised on how to modify the seller’s practices, operations or business post-closing to comply with applicable privacy laws.

The Asia-Pacific region has seen an explosion of new data protection regulation in recent years, with comprehensive “European-style” laws now in force in Australia, Hong Kong, India, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea and Taiwan (and on a sector-by-sector basis in China). The compliance challenge in the region is one that has historically often been overlooked. As a consequence of an increasing frequency of high profile cases of unauthorized use of personal data, regulators are becoming increasingly aggressive in a number of jurisdictions. Fines of up to the equivalent of US$1m are now possible in some jurisdictions and some jurisdictions, such as South Korea, have introduced revenue-based fines.

Best practices

- Create a data protection “heat map” to identify areas of highest compliance risk for the target.
- When evaluating potential liabilities linked to data privacy compliance, keep in mind that there is a global trend to increase sanctions worldwide.

Cyber Security

As of January 1, 2015, 84 percent of the total value of Fortune 500 companies consisted of intangible assets1. Corporate risk has correspondingly shifted to the virtual world. The threats are complex, varied, and rapidly evolving: cyberattacks can compromise sensitive and confidential data such as personal information, corporate secrets, intellectual property, and credit information. Smaller organizations – which have fewer security resources than their larger counterparts – are frequent targets2. The costs can be staggering3. In addition to financial costs, organizations may suffer damage to their reputation, loss of clients, and even disruptions in their business operations.

Operating under the time pressures of a deal, buyers often overlook cybersecurity risks. This mistake can be costly, as a Seller’s cybersecurity capabilities can affect the value of the target or even the viability of a transaction itself. Moreover, acquired companies are often targeted as attack pathways to corporate parents, meaning that cybersecurity vulnerabilities within an acquired company may threaten the assets of the corporate parent after acquisition.

---

3 PwC estimated the average cost per data breach to large organizations at $4.8 million in 2014.
Data protection in M&A transactions: A how-to guide

Valuation
Possession of data does not always create the right to use data. Laws and data providers commonly impose restrictions on recipients’ data use. A German data protection authority has recently stated in relation to an asset deal that email addresses and telephone numbers of the seller’s customers may not be used by the buyer for marketing purposes, unless the customers have declared their consent to receive marketing emails or call from the buyer. After contracts terminate, recipients are typically obligated to return or destroy the data they have received. The restrictions on the use of the data may significantly undercut the value of the target’s data and/or impede a buyer’s intended use of the data after closing. A deal value may thus be affected by such restrictions.

IT Expenses
The pace, scope, and sophistication of data breaches and cyberattacks continues to increase, placing businesses’ data security practices under heightened scrutiny from consumers, private litigants, and regulators. Such breaches can expose the data of millions of individual consumers, resulting in potentially massive liability. Such breaches trigger both direct (financial) and indirect (brand reputation, diminished customer loyalty) costs. Companies must allocate substantial resources to guard against potential liabilities incurred from security incidents involving the improper use or disclosure of data.

Data Integration
As data becomes an increasingly valuable and strategic corporate asset, businesses look to combine customer databases to maximize transaction value. Integrating databases can raise privacy and data protection compliance issues. The target’s existing data subject consents and other compliance measures may not address the scope of a combined business or align with its legal structure. The operating efficiencies envisaged for an integrated business may be challenged by cross-border data transfer controls that prevent or restrict consolidation of data center and other operations. Apart from the regulatory compliance issues, the costs of integrating databases may be substantial and create transaction risk.

Best practices
- Consider a separate cyber security audit as part of due diligence.

- If the target’s value is linked to the personal data it holds, stop and think whether the data really can be used for new purposes.

- Check capex forecasts to make sure adequate IT investments are budgeted for cyber security.

- Create simulations on how the data systems of the buyer will be integrated into the group.

- Check these simulations with data privacy counsel to make sure they are realistic.

- If the target’s value is linked to the personal data it holds, stop and think whether the data really can be used for new purposes.

- Check capex forecasts to make sure adequate IT investments are budgeted for cyber security.

- Create simulations on how the data systems of the buyer will be integrated into the group.

- Check these simulations with data privacy counsel to make sure they are realistic.

Choosing deal structure
Asset purchases involve the sale of specific assets, and some of those assets may consist of data. The purchase and sale of data, however, raises a number of legal issues that require attention. For example, in the United States, the sale of data outside of the transfer of an operating business implicates a number of U.S. laws, including laws applicable to health data and financial data, and the seller’s specific privacy policy representations, the breach of which may be deemed deceptive under section 5 of the Federal Trade Commission Act. Similar restrictions exist in the EU. In Germany, the transfer of personal data to the buyer by way of an asset deal at least requires providing the customers with the opportunity to opt-out before the

---


5 By some estimates the average total cost of a data breach was $3.5 million in 2014, a 15% increase over the cost of breaches in 2013.
Data protection at signing

The sale of a database can in some cases be considered null and void if the database does not comply with applicable legislation.

**Best practices**

- Like contracts, personal data cannot always be assigned in a transaction. This may affect how the deal is structured.
- Where the deal is structured as an asset deal, beware of potential arguments that the sale is null and void, due to data protection violations.

**Stage II – Signing**

**Drafting the SPA**

**Other Contract Provisions**

**Works Council Consultation**

**Ancillary Agreements**

**Drafting the SPA: Reps and Warranties**

The value of and risks relating to data should be confirmed through the negotiation of appropriate representations and warranties in the transaction documents. Those representations vary by industry and risk levels but often include representations regarding:

- compliance with privacy and data security laws and contractual requirements;
- security of information technology assets;
- detection of network vulnerabilities and data breaches;
- disclosure of data related claims and compliance investigations;
- disclosure of arrangements under which data is shared with or by third parties; and

---

Data protection at signing

- security assessments and remediation of any gaps. These representations should also address any significant due diligence findings and assumptions, and be backed by indemnification.

Other Contract Provisions
Depending on the results of the due diligence, a number of other provisions may be considered. These include:

- special indemnities for data-related liabilities;
- closing conditions to address implementation of missing IT safeguards or compliance gaps;
- covenants to address ongoing safeguards of sensitive information.

Best practices
- Consider treating data protection similarly to environmental risks in the SPA, including a potential audit to establish a baseline and remediation steps.
- Data protection may affect SPA reps and warranties on employment (including works council consultation), conditions precedent, and covenants between signing and closing.

Works council consultation
In some countries, works council consultation is required before the SPA is signed. Works councils are increasingly sophisticated on data protection issues. Works council consultation may therefore need to include a data protection aspect if the transaction will affect how employee personal data is handled. The works council may also act as watch dogs to ensure that the buyer and seller comply with personal data rules.

Best practices
- Assume that the works councils will be vigilant on data protection compliance in connection with the deal.

Ancillary agreements
The transaction may require various ancillary agreements dealing with personal data, including:

- A transitional services agreement dealing with post-closing data integration and services;
- A data sharing agreement to govern data transfers pre-closing;
Data protection between signing and closing

- Where appropriate, other licensing and data processing agreements for operation of the business post-closing.

**Best practices**
- Drafters of the SPA should think through data transfers, sharing and use, to ensure that they are covered by appropriate ancillary agreements.

**Stage III – Between Signing and Closing**

### Pre-closing integration

Between signing and closing, the buyer’s integration team will be developing plans on how to integrate the employees and information systems of the acquired businesses into buyer’s own organization. Integration planning may require the transfer of significant personal data between seller and buyer prior to the closing. The scope of information that may be transferred prior to closing is strictly limited by antitrust rules. Sharing any information that may affect the competitive behavior of the two entities prior to closing can be heavily sanctioned under “gun jumping” rules. However, subject to those antitrust rules, it is possible to organize the exchange of some information with the integration teams of the buyer in order to help the buyer prepare for the day when it will operate the businesses.

Transferring employee data to the buyer prior to closing raises particular data protection issues:

Before closing, the buyer’s group is a third party vis-à-vis the seller. Therefore:

- The seller will generally have to consult the relevant works councils of the transferred entities before transferring any employee data.
- The seller may have to make filings with relevant data protection authorities in connection with the transfer.
- The seller must be able to justify that the transfer only involves data that is absolutely necessary for the integration task, and that the recipients of the data are limited to the integration teams within the buyer’s organization.
- The buyer should agree to return or destroy the data in the event the closing does not occur for any reason, and should naturally be bound by a confidentiality obligation and an obligation not to use the data for any purpose other than for integration planning.

For complex integration projects involving large amounts of data, buyer and seller may consider creating a governance framework to ensure that data protection concerns are reflected during each stage of the process. Under the principle of accountability, seller must be able to document that data protection principles were conscientiously applied throughout the process, and that safeguards have been implemented to ensure that the whole process is reversible if the closing does not occur.

### Phase II antitrust requests

During the period between signing and closing, antitrust authorities may request additional information. If the parties’ businesses involve the collection and aggregation of significant amounts of customer data (e.g., user data from the parties’ online properties), a Phase II investigation may include an analysis of whether the combination of those data sets creates a competitively significant barrier to entry that could harm competition. Parties to transactions involving combination of large sets of user data should be prepared to address potential arguments that the deal will foreclose or undermine smaller competitors.

Responding to Phase II requests may require the analysis of employee e-mails, which requires appropriate data protection safeguards.
Data protection post-closing

Best practices

- Put in place a data protection framework agreement between the buyer and the seller to govern and secure the transfers of data pre-closing;
- Limit disclosure of data to integration teams;
- If Phase II antitrust requests require analysis of employee e-mails, make sure employees are informed and other data protection safeguards are implemented.

Stage IV – Post-Closing

Data Uses / Database Integration

Transitional Services Agreement

Post-Closing Restructuring / Remediation

Data Uses and Database Integration

Acquiring data assets through an acquisition does not automatically give a buyer rights to use the data post-closing. For example, in the United States, regulators have made clear that buyers must continue to honor the privacy promises made by the seller prior to closing. As a result, a buyer is responsible for honoring any public privacy policies of the seller and the buyer cannot make more expanded use of the information under the buyer’s privacy policy without first obtaining opt in consent from each individual who had provided the data.

Transitional Services Agreement

After closing, the parties to the transaction will generally have to continue migration and integration efforts, a process that can last up to two years. During this period, the seller may continue to conduct a number of data processing operations on behalf of the buyer.
Data protection post-closing

These post-closing data processing operations are generally part of a broader set of technical and operational services covered by a “transitional services agreement” (TSA). From a data protection standpoint, the TSA will be considered a processing agreement between the buyer, as data controller, and the seller, as data processor.

As with any data processing agreement, cross-border data transfers, particularly in the context of EU business processing data outside the EU, but now also in the case of many Asia-Pacific jurisdictions processing data cross-border, will have to be analyzed and surrounded by safeguards. In some cases, the transitional services may involve processing of personal data by the buyer as data processor on behalf of the seller. This might be the case, for example, if the buyer must handle consumer complaints relating to product sales that remain the responsibility of the seller. In that case, the respective roles of data controller and data processor are reversed, and the TSA must reflect this by putting appropriate obligations on each party. In either case, the TSA will need to describe what happens to the personal data once the TSA comes to an end. In theory, the data processor is supposed to destroy the data or return the data to the data controller.

Post-Closing Restructuring and Remediation

One of the most challenging post-closing tasks will be to integrate the acquired businesses into the buyer’s data protection governance arrangements. The process will be similar to rolling-out the buyer’s global compliance program into the new acquired businesses.

Best practices

- Specific training measures would have to be introduced into the new businesses, data protection officers will have to be named, and compliance gaps identified and corrected.

Conclusion

For almost any deal, Buyer’s deal team should ask the following questions:

- Can we centralize all the target’s data at our existing data centers?
- Have we given instructions not to upload personal employee data to the data room?
- Should we conduct a data protection and/or cyber security audit to create a baseline of potential risks and estimate remediation costs?
- Are we taking data protection into account in our works council consultations?
- What data-specific ancillary agreements will we need?
www.hoganlovells.com

Hogan Lovells has offices in:

- Alicante
- Amsterdam
- Baltimore
- Beijing
- Brussels
- Budapest*
- Caracas
- Colorado Springs
- Denver
- Dubai
- Dusseldorf
- Frankfurt
- Hamburg
- Ho Chi Minh City
- Hong Kong
- Houston
- Johannesburg
- London
- Los Angeles
- Luxembourg
- Madrid
- Mexico City
- Milan
- Minneapolis
- Monterrey
- Moscow
- Munich
- New York
- Northern Virginia
- Paris
- Perth
- Philadelphia
- Rio de Janeiro
- Riyadh*
- Rome
- San Francisco
- São Paulo
- Shanghai
- Silicon Valley
- Singapore
- Sydney
- Tokyo
- Ulaanbaatar
- Warsaw
- Washington, DC
- Zagreb*

*Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses. The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com. Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising.

Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2015. All rights reserved. 10358_EUn_1215

* Associated offices