MV COMPLIANCE

PRIVACY IN M&A

MACEDO VITORINO

ABOUT US

MACEDO VITORINO WAS ESTABLISHED IN 1996, FOCUSING ITS ACTIVITY ON ADVISING DOMESTIC AND FOREIGN CLIENTS IN SPECIFIC ACTIVITY SECTORS, INCLUDING BANKING, TELECOMMUNICATIONS, ENERGY AND REAL ESTATE AND INFRASTRUCTURE.

Since the incorporation of the firm, we have been involved in several high-profile transactions in all of the firm's fields of practice, including banking and finance, capital markets, real estate, M&A, complex disputes and corporate restructurings.

We have strong relationships with many of the leading international firms in Europe, the United States and Asia, which enable us to effectively handle any cross border legal matters.

We are mentioned by The European Legal 500 in most of its practice areas, including Banking and Finance, Capital Markets, Project Finance, Corporate and M&A, Tax, Telecoms and Litigation. Our firm is also mentioned by IFLR 1000 in Project Finance, Corporate Finance and Mergers and Acquisitions and by Chambers and Partners in Banking and Finance, Corporate and M&A, TMT, Dispute Resolution and Restructuring and Insolvency.

The multidisciplinary and integrated character of our corporate and commercial group allows us to efficiently solve the legal issues of our clients, in particular:

- Commercial contracts, distribution agreements and franchising
- Competition and European law
- Copyright, intellectual property, IT, patents, and trademarks
- Corporate and acquisition finance
- Dispute resolution, litigation, mediation and arbitration
- Employment
- Foreign investment, mergers & acquisitions and privatisations
- Real estate acquisition and disposal
- Tax

If you want to find out more about MACEDO VITORINO please visit our website at WWW.MACEDOVITORINO.COM

CONTENTS

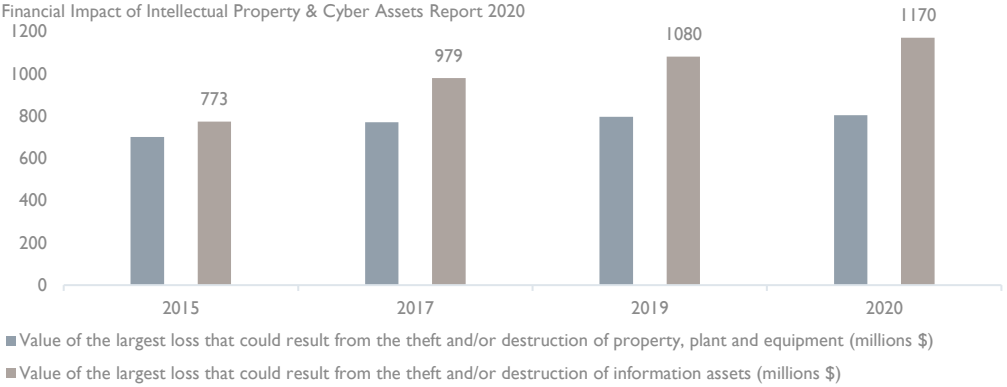
INTRODUCTION

Data is everywhere. Information assets are highly valued by companies. Nowadays, businesses depend more frequently on information technologies and data than a few years ago, mainly before the entry into force and application of the European General Data Protection Regulation (GDPR).[1]

In M&A transactions, data is the key for the evaluation of the target company and the risks associated with the deal. Transactions rely on cybersecurity to protect sensitive and confidential information. However, as insurance coverage over information assets is still not widely sought for, risks are greater for companies that may be more vulnerable during M&A transactions.

But if not the risk of an information breach, or the risk of mispricing the transaction, then the risk of being held legally liable for such breach, including personal data violation, must be of alarming to businesses during M&A transactions.

Source: Ponemon Institute/AON
Financial Impact of Intellectual Property & Cyber Assets Report 2020



Within the context of a transaction, there are two key points regarding data protection compliance to be considered: whether personal data can be transferred from the target to the acquiror; and whether the parties comply with privacy laws.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

In general, asset deals may be more exposed to data protection compliance risks than share deals or corporate reorganizations, since, in these latest two cases, there is no change in the position of the parties to contracts with employees, customers, and suppliers; that is, there is no transfer of the data controller position, which, even though a shareholders' change, will remain the same entity. However, there are still significant compliance risks associated with share deals. The differences stages of a M&A transaction require different measures to ensure proper data protection compliance.

In this paper, we aim at providing you with the main points of interest that should concern the parties to a transaction, and to outline potential solutions to minimize or eliminate compliance risks.

1. PRE-SIGNING

The typical M&A transaction kicks off with a due diligence on the acquiror, the target, or both. The due diligence is essentially an analytical review of data disclosed by the relevant party to a transaction. And the disclosure of data poses a significant compliance risk for those attributed the duty off keeping it safe.

Usually, access to data in a due diligence is assured via a data room, from which the reviewing party will obtain the contents that are object of the due diligence, including personal data, e.g., information on employees, customers. For this purpose, it may be advisable that data rooms disable save and print options, which is already common practice in many transactions.

Even before the transaction agreement is done, the parties are already obliged to comply with applicable data protection rules, as the pieces of information reviewed during a due diligence will most likely include personal data. And because data rooms usually host personal data, the parties to a transaction must execute data processing agreements with data room providers.

Personal data includes any information relating to an identified or identifiable natural person, as defined by the GDPR.

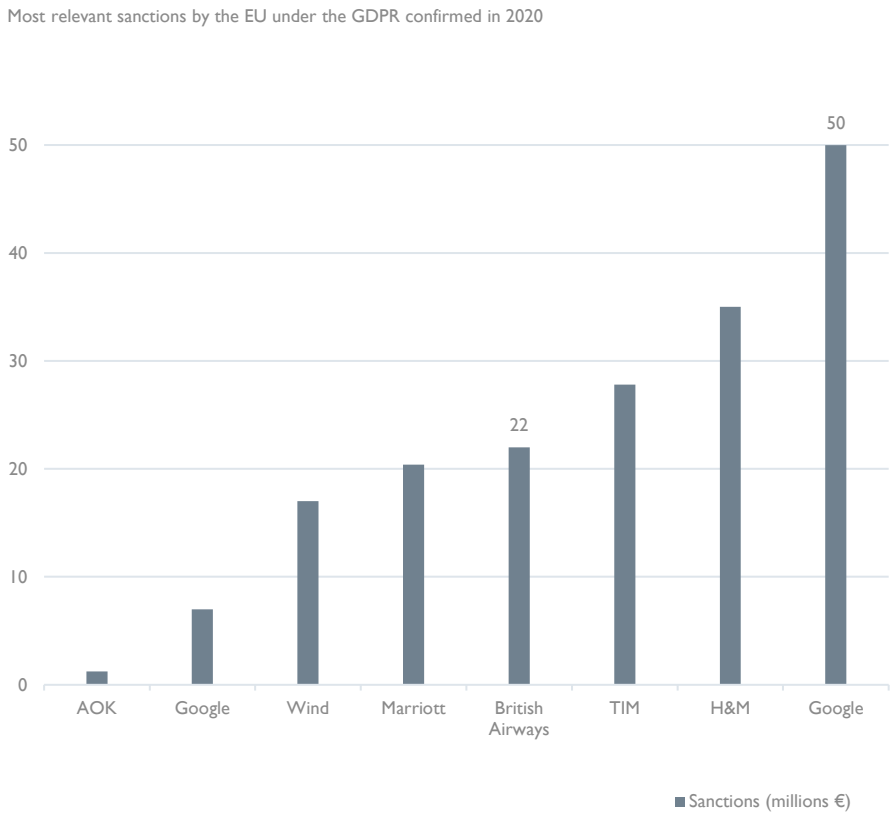
Deal structure and industry-specific due diligence is of great relevance, too. On one hand, personal data cannot always be transferred in asset deals, and, on the other, for businesses which are data-intensive, handling great amounts of personal data, it is advisable to conduct further compliance due diligence focusing on data protection.

When extra care is advisable, because e.g., the target company handles sensitive data, there are at least three main areas of play:

- The transferability of data and, when applicable, the consent of data subjects on data transfer;
- Whether the original purposes of the data processing (and for which, for example, data subjects gave their consent) are compatible with the acquiror's business and data processing purposes in connection with the M&A transaction; and
- The security standards in place at both target and acquiror to keep data safe.

To this date, the highest fines applied by the Data Protection Authority in Portugal amounts to €400,000, fine which was applied to a hospital for the unduly access to health details of patients by health professionals and the inadequacy of security standards. Recently, the Municipality of Lisbon, was also charged for 225 breaches to the GDPR for unduly sharing sensitive personal data of activists

with third parties. The Municipality may be fined to a maximum amount of €20,000,000 under the GDPR. In other European Union (EU) countries, the scenario is different as to the number of breaches and fines amounts, as shown below.



Either for valuation or risk assessment, the acquiror should hence understand what the target's liabilities on privacy matters are, as the acquiror may take on the target's liabilities at completion.

What you should watch for:

- Access to the data room should be restricted and information disclosed in the data room should be the necessary (data minimization principle). The employees or customers should not be identified or identifiable. For this purpose, and so that the information keeps meaningful value to the due diligence, the disclosing party can anonymize/pseudonymize information;

- Alternatively, employees or customers should be informed that their information will be processed for the purpose of a due diligence and the disclosing party should obtain their consent. Not only this is impractical in large transactions, but also the parties should consider the fact that consent is only an appropriate lawful basis for data processing if it is genuine, which is not likely in an employment context, and thus the parties should rely on a different lawful basis for transferring data of employees;

- The information disclosed should be limited to that that is strictly necessary to perform the due diligence. For this purpose, e.g., employment agreements can be sampled, or the information can be aggregated, or only key information can be disclosed, or the disclosure of sensitive data should be avoided;

- The valuation of the target company should take into consideration that there may be restrictions to the use of personal data by the acquiror post-closing;

- Whenever the target is processing data on behalf of a third party, data sharing agreements will likely include change of control or change of ownership clauses, which should be accounted for by the acquiror;

- Both deal structure and the industry of the target are relevant for the purpose of assessing price, exposure to risk and steps required for a compliant M&A transaction.

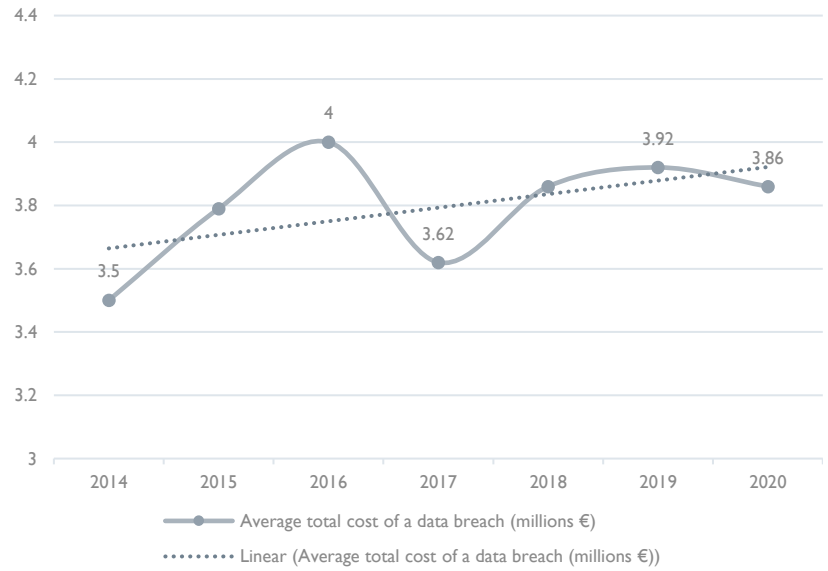
2. SIGNING

If it were not for the comprehensive set of privacy rules, the assumption would be that the target company owned (and could freely exploit) the personal data it acquired over the years. But that is not the case.

Once the due diligence is complete, the transaction documents should safeguard the party's position in view of any potential data breaches or infringement of data protection rules.

There are plentiful ways to ensure one's position during negotiations and at signing: contract negotiations should entail an adequate level of protection against the findings resulting from the due diligence, whether this is reflected on the price or in contractual provisions; the share and purchase agreement should include representations and warranties that are tailored for data protection compliance and/or transferring the risk of violation; the counterparty should be able to warrant that it is compliant with privacy laws and has put in place adequate security standards, etc.

Source: IBM Security
Cost of a Data Breach Report 2020



The target should warrant the acquiror, e.g., that there are not any pending proceedings related with data security breaches, that it has adequate security standards in place, or that it is compliant with the applicable privacy laws. Indemnification clauses and limitations of liability are also relevant in view of any potential breaches and/or liability resulting from the target's business up until the completion date.

Insomuch as some transactions may be of greater complexity as regards data, data sharing and data integration, it may be cost-effective and legally advisable to include ancillary services agreements for the specific purpose of ensuring data protection compliance in the transaction documents.

There should be extra care in international M&A transactions due to potential international data transfers.

If data is transferred to a country outside of the EU-EEA, an assessment of the level of adequacy of the jurisdiction, to which the data will be transferred, has to be carried out. Alternatively, mechanisms such as standard contractual clauses, binding corporate rules, approved codes of conduct, approved certifications or a combination thereof have to be included in the transaction documents.

At signing, if the target processes or controls data, the acquiror should have obtained a comprehensive catalogue of data and respective consents, Records of Processing Activities (RoPAs), Data Protection Impact Assessments (DPIAs), if applicable, and Legitimate Interests Assessments (LIAs).

What you should watch for:

- Data breaches and infringements of privacy laws are costly. Whenever appropriate, privacy-related risks should be accounted for with remediation and indemnification clauses;
- If deemed adequate, it may be advisable that the parties agree to conditions precedent and covenants in respect to data processing;
- Non-disclosure agreements (NDAs) should include data protection clauses and contractual penalties in case of failure to keep information confidential. We should note that NDAs executed by the parties for the purpose of ensuring confidentiality during the transaction process will most likely expire at signing of the asset purchase agreement (APA) or share purchase agreement (SPA), so it may be relevant to execute a new NDA at signing or include a non-disclosure provision in the purchase agreement;
- If the target does not warrant that it is legally authorised to share the data with the acquiror, the acquiror risks exposure to liability for unauthorised processing of data;
- Insurance on cyber risks is valuable and may even be a solution to a deadlock where the target is reluctant to be exposed to such a relevant liability.

3. PRE AND POST-CLOSING

The day the share and purchase agreement are executed by the parties does not always match the closing of the transaction. The period between signing and the closing date could, in fact, take months. During this period, the transaction parties may also exchange information.

The parties should take into consideration that while the transaction is not closed, the acquiror is a third party and sharing information can result in responsibility before the competition authorities.

Some deals require a level of confidentiality that is sometimes conflicting with the interests of privacy laws. The timing for transfer of liability is key, then. When possible, and to avoid unnecessary exposure to compliance risks, the acquiror can be provided with statistical information instead of actual data, even if it is pseudonymized.

After the deal is closed, it is likely that the acquiror might have to face limitations on the use of data.

The acquiror should mind that the consent provided to the target by data subjects sometime in the past may both enable and limit the data processing by the acquiror. And even in a share deal, where the controller of data does not change, privacy policies will need to be updated, should the purpose or use of personal data change after completion.

What you should watch for:

- Data sharing before the closing date should be limited to that strictly necessary for data integration purposes, and those handling data should be limited to the minimum;
- Should the transaction not occur, the parties must be able to adequately eliminate and dispose of any data obtained during negotiations and before closing date;
- Consent is not transferable in the context of an M&A transaction unless the data subject was informed of such a possibility when providing his consent, so this should be considered by the acquiror;
- Data sharing before the closing date should be limited to that strictly necessary for data integration purposes, and those handling data should be limited to the minimum;
- Where the purpose or use of data does change after completion, the acquiror will need to obtain the consent of the data subjects for their data to be processed under the revised privacy policies.

4. HOW DOES THE GDPR IMPACT M&A?

In the context of an M&A transaction, personal data of many sorts is handled and/or transferred from target to acquiror. This will include employees' information, applicants' CVs, IP addresses, suppliers' information, etc..

The right to data privacy is not an absolute right. It is relative to its function in society.[2] Throughout the transaction process, it is crucial that the parties weigh their legitimate interests against the fundamental rights and freedoms of data subjects.

The assessment of an adequate balance between the right to protection of individual data and freedom of enterprise adds a layer of complexity to M&A that is novel to the market.

During negotiations, the acquiror is a third party as it is neither the data subject, nor the controller, processor, or an entity who, under the direct authority of the controller or processor, are authorized to process personal data. This puts the parties in a very delicate position as to what information can be shared at a stage where trust and disclosure is key to the success of the transaction.

On one side, the logistics are seriously impacted as parties must go on tiptoe through each stage of negotiations and even after executing the agreement, bearing in mind that sharing information means exposure to a compliance risk.

On the other, data privacy influences both valuation and deal structure. As we explored, the price may be adjusted by exposure to compliance risks, and the structure of the deal must be compatible with the transfer of data from the target to the acquiror.

On the third, where transactions are negotiated behind closed doors, the current data protection framework, compliance obligations, and recent history of sanctions motivated by infringements during

[2] In this sense, please see Judgement of the Court of Justice of the European Union, of November 9, 2010, *Volker und Markus Schecke and Hartmut Eifert versus Land Hessen,* cases C-92/09 e C-93/09.

negotiations, suggest that even though the door is closed, it is not locked, and personal data protection concerns may not be neglected.

MACEDO▪VITORINO

MACEDOVITORINO.COM