First and foremost

Matthias Bürge, Andreas Moll and Charlotte Rupf from Prager Dreifuss assess the importance of data protection considerations in M&A due diligence

Companies face a challenge when it comes to different compliance rules, with the legal framework applicable to data protection playing an important role in this process. Data protection awareness in Europe may have substantially increased in the past few years but is nevertheless often an underestimated issue. Special attention should be paid to the topic in M&A transactions.

If companies or their assets are transferred in the context of an M&A, the transfer and processing of data may be at issue in various respects and at several stages of the transaction, be it (i) in connection with its preparation (disclosure of information to potential acquirers), (ii) in the context of its completion (actual data transfer (namely in asset deals)) or (iii) in connection with the subsequent integration of the acquired company in the group of the acquirer (use of the target company's data).

> **There is a significant risk that data disclosed in a data room is too extensive, or accessible to too many or to the wrong people**

This article primarily focuses on the preparatory phase of M&A deals where data protection issues particularly arise in relation to the due diligence process. First it describes the general data protection rules, which have to be considered when setting up a data room. It then briefly shows the potential consequences of a breach of these rules. Finally, it concludes with recommendations how companies can comply with these rules in the due diligence process.

Conflicting interests

The purpose of disclosure and the establishment of a data room is usually the search for potential purchasers or investment partners (the investors). A company discloses financial information, important contracts and other documents to potential investors to provide them with the opportunity to assess contractual risks and the value of the company. It is obvious that, on the one hand, potential investors are interested in information being as comprehensive as possible to decide whether they would like to buy or invest in the target company. The target company, on the other hand, has to abide by data protection rules as well as contractual and statutory confidentiality obligations. As such what information may be disclosed by a company in a due diligence process and at what stage?

Barriers to disclosure of information in due diligence

Confidentiality obligations

When setting up a data room in M&A transactions companies should bear in mind that, in addition to being compliant with data protection rules (see below), they are generally obliged to protect business and industrial secrets as well as further confidential information. Information is considered confidential if it is not publicly known – for example, unpublished financial data, business plans or knowhow not in the public domain. Furthermore, professional secrets and bank secrecy have to be kept and cannot be disclosed in a due diligence process. If a company considers disclosing memoranda provided by third party advisors or consultants (eg a memorandum regarding a new envisaged group structure), the consent of this third party is usually required given that such memoranda regularly contain provisions making their disclosure subject to the author's prior consent.

Swiss data protection rules, on which this article focuses, partly overlap with these general confidentiality barriers. However, they encompass also further data which would otherwise not be protected.

Data protection obligations

The Swiss Federal Act on Data Protection (FADP) aims to protect the privacy and the fundamental rights of persons when their data is processed. It applies to data pertaining not only to natural persons but also – unlike data protection regulations in most other jurisdictions – to legal persons (such as corporations, limited liability companies etc). According to the FADP's article 3 section a, personal data is defined as all information relating to an identified or identifiable person. Hence, in a due diligence process, under Swiss law, personal data is at issue not only when dealing with data of employees and corporate officers but also in the context of processing customer and supplier data. Therefore, a company disclosing its contracts or any other information containing personal data has to be careful not to violate any data protection provisions. Companies should never forget that they do not only have to protect their own data but also data of third parties such as suppliers and customers.

Risk of unjustified data processing

In the context of the preparation of M&A transactions, the risk of unjustified data processing and transfer is substantial. There is a significant risk that data disclosed in a data room is too extensive and/or accessible to too many or to the wrong people. Potential investors may receive more personal information than actually required for the purchase of, or an investment in, a company.

As a fundamental rule, each processing of personal data has to be in line with the principles set out in FADP's articles 4 et seq. That disclosure of company information in a data room and its assessment by the investor have to be qualified as data processing is obvious in view of the legal definition of this term in article 3 section e. Pursuant to this provision, data is processed by any operation with personal data, irrespective of the means applied and the procedure, and in particular by the collection, storage, use, revision, archiving, destruction and namely *disclosure* of data.

In case of a breach of data protection provisions, affected persons may claim damages, request the surrender of profits and seek compensation for personal suffering. They may particularly also request that (i) their data be corrected or destroyed, (ii) data processing be stopped

and (iii) no data be disclosed to third parties. According to the FADP, the claim is related to, and expressly governed by the rules regarding, personality protection according to article 28 et seq. of the Swiss Civil Code. Furthermore, in case of an unlawful disclosure, contractual penalties are often triggered. Finally, the breach of data protection rules may under certain circumstances result in criminal sanctions.

In view of these far-reaching consequences, the parties involved in a due diligence process are well advised to process data only in compliance with the FADP. What does this mean in more practical terms?

General data protection principles

Personal data may only be processed lawfully, in good faith and in a proportionate manner. As a general rule no more information than is absolutely necessary should be disclosed in a data room, and a company managing a data room is well advised to disclose information gradually. The relevant test will always be whether the other party really *needs to know* the information at the current stage.

Furthermore, personal data may only be processed for the purpose indicated at the time of collection – which is evident from the circumstances or provided for by law. The collection of personal data and in particular the purpose of its processing must be evident to the data subject.

The consent of the data subject leads to a lawful or justified processing of data. However, it has to be considered in this context that such consent is valid only if given voluntarily upon the provision of adequate information. Additionally, consent must always be given expressly in case of processing of sensitive personal data or personality profiles (see below).

Cross-border disclosure is only permitted if the privacy of the data subject is adequately protected by the recipient. If there is no statute providing for adequate protection, the parties have to ensure such protection by entering into respective contractual provisions. If no such adequate protection is guaranteed, personal data may in principle only be disclosed abroad with the consent of the data subjects.

Possible justifications

If the above-mentioned data protection principles are breached the processing is unlawful, unless it is justified by (i) the consent of the affected party, (ii) an overriding private or public interest or (iii) statutory law (article 13 para 1 of the FADP).

In case of disclosure of sensitive personal data (including religious, ideological, political or union-related views or activities, health, racial origin, social security measures and administrative or criminal proceedings) or personality profiles (which are defined as a collection of data permitting an assessment of essential characteristics of the personality of a natural person) to third parties, a justification is always required. Additionally, a party receiving sensitive personal data or personality profiles is obliged to inform the data subject of the collection.

Justification based on statutory law or overriding public interest is not necessarily readily apparent or available in the case of disclosure in a due diligence. Therefore, we will focus hereinafter on the justification by consent of the affected party and the overriding private interest.

As mentioned above, an affected person may only give valid consent, if it is based on appropriate information and given voluntarily. Precautionary general consent to data processing included in general terms and conditions to a contract is usually insufficient to meet these two criteria. The provisions in general terms and conditions are often vague, and any approval included in them is considered involuntary, because they are usually not negotiable.

There is usually a broad range and number of documents in a data room. Obtaining the individual consent of each and every single party involved is in most M&A transactions barely or in some cases not at all feasible. First of all, the timeframe is usually very tight. Secondly, the risk of an affected party not responding is rather high and may result in uncertainty regarding the lawfulness of the intended disclosure. Finally, the transaction is usually only known to a very limited circle of persons interested in its strict confidentiality. This circle privy to the transaction could be undermined if a large number of consents of third parties needed to be obtained.

As regards the justification of an overriding private interest, the FADP's article 13 para 2 lists certain examples which may possibly justify the unlawful processing of data. For instance, a person processing data may be considered as having an overriding interest if the personal data is processed by such party in direct connection with the conclusion or the performance of a contract and if the personal data is that of a counterparty. Parties involved in an asset deal or company transfer may, according to the predominant opinion of legal doctrine, invoke this justification reason because the contract's continuing performance by the acquirer is in the interest of all involved parties. However, the company disclosing data has to carefully weigh up its disclosure interest against the privacy interest of the affected data subject. This often leads to substantial uncertainty. Taking appropriate measures to live up to the above-mentioned data protection principles becomes all the more important.

The Commissioner's recommendations

The Swiss Federal Data Protection and Information Commissioner issued guidelines regarding adequate data protection in the context of M&A in 2010, expressly setting out measures to comply with the FADP. With respect to the due diligence process, these guidelines include:

- Personalised data shall not be physically transferred to potential investors or their advisors. These parties shall merely be given the possibility to see information on site or in a data (information) room.
- The selection of potential investors granted access to a data room shall be strictly limited to those persons with an actual interest in the company's acquisition.
- Only a restricted group of persons shall be allowed to access the data room. These persons have to contractually agree to not further use and to destroy the received information in case of a possible failure of the negotiations.
- The disclosed information shall be limited to what is really necessary and shall be reduced to the amount justified in view of the weighing of interests. Furthermore, data should be anonymised or aggregated so no person can be identified.
- The extent of provided personal data shall be appropriate to the stage of the transaction process. The more advanced the process is, the more information may be disclosed. If the conclusion of a transaction contract gets closer and becomes more likely, more data may be disclosed.
- In order to have additional security, non-disclosure agreements (NDAs) with explicit data protection clauses shall be concluded pursuant to which potential investors and their advisors shall be obliged to comply with data protection regulations.
- Specified statutory professional confidentiality provisions need to be unconditionally complied with.

Practical recommendations to mitigate data protection issues

What do the Commissioner's recommendations mean? How can they help avoid or at least mitigate data protection issues?

According to the first recommendation, companies should prohibit the copying, saving and printing of documents from the data room to prevent confidential information spreading. This may be somewhat cumbersome for the potential investor and its advisors but adequately supports data protection.

In case the transaction negotiations fail, the persons granted access to the data room should agree to destroy all received information including their due diligence results. Very often, data room providers prepare data room rules setting out all these obligations and request each user accepts these rules before accessing the information by their first login.

Recommendations four and five provide that never more information than absolutely necessary should be disclosed. Instead of fully holding back documents from the data room, this requirement may also be fulfilled if personal data set out in such documents is anonymised or blackened. Companies may then at later stages of the transfer negotiations, when the deal is more likely to be concluded, disclose less blackened documents, if required. When blackening information, no individual – natural or legal – person may be identified. In the early stages of a deal, contracts with the top management should be blackened in a way that not even the CEO may be identified. A step by step disclosure allows to forgo the disclosure of personalised data from the outset and ensures that rather only general information is disclosed in the initial phase.

> **Cross-border disclosure is only permitted if the privacy of the data subject is adequately protected by the recipient**

With respect to recommendations two and three, data rooms nowadays are predominantly established as online platforms (virtual data rooms). The customary technical security standards to preclude unauthorised persons from gaining access to digital data shall, of course, also apply to such data rooms. Hence, companies have to ensure that the access to the online platform is strictly password protected. To avoid further issues and efforts connected to international data transfers, it seems advisable that the server of the online platform not be located in a jurisdiction whose legislation does – from a Swiss perspective – not guarantee adequate data protection (for instance the USA, India, Japan or China).

Furthermore, the access to the data room should be strictly limited to those persons who really need to assess the documents (need-to-know-principle). The group of persons, to whom access is granted, should be kept as small as possible. Additionally, such persons must have a current and genuine interest in the due diligence.

It goes without saying that every single person granted access to a data room should be expressly obliged to (i) use the information in the data room only for the purpose of due diligence, (ii) not disclose information to any third party (iii) not print or copy documents from the data room and, (iv) take appropriate measures that, when logged in to the data room, no other person may access the relevant computer or other communication device.

Customer, supplier and in particular employee data should – at least in the initial phase of the due diligence – be disclosed only in an abstract way. Therefore, no individual data of employees, for example, but rather only their number, average age and salary or percentage of women and university graduates etc should be disclosed. Last but not least, one may consider to disclose more sensitive information only upon specific request.

Referring to recommendation six, the following can be noted: to keep a possible M&A transaction in the preparatory phase strictly confidential, protect business and industrial secrets as much as possible, and comply with the above data protection principles, it has become standard that target companies sign confidentiality agreements/NDAs at the outset of the transaction process, before starting the due diligence. In general, these agreements contain provisions regarding the storage, return or destruction of information and are secured by a contractual penalty for non-performance. Furthermore, the agreements usually provide that accessed information shall not be forwarded by the recipient to any third party and exclusively used for the evaluation and assessment of the target company. Commonly, the agreed non-disclosure duty and confidentiality obligation, respectively, shall survive both (i) in case a transaction contract between the parties is concluded and (ii) in case the parties discontinue to proceed with the transaction.

Considering that virtual data rooms may regularly be accessed from everywhere in the world, and because in international transactions parties and advisors in various jurisdictions need to assess the disclosed information, disclosure is often considered an international data transfer. Accordingly, if jurisdictions are involved which do not guarantee an adequate data protection level, respective contractual guarantees have to be entered into.

In case information is protected by statutory confidentiality provisions (see the seventh recommendation) or other highly sensitive information needs to be disclosed, it may be considered to use the concept of 'advisors only disclosure', also known as clean team approach. The advisors have to undertake that they will convey to their client no details of the reviewed documentation but only generic information.

Summary and conclusion

The protection of personal data and compliance with the respective legal framework has – at least in EU jurisdictions and Switzerland – become an important and sensitive topic, especially when it comes to M&A and particularly due diligence. As Swiss data protection provisions protect not only data of natural but also legal persons, good M&A practice requires that disclosure of personal data, not only of employees but also of customers and suppliers, is only made lawfully, ie in line with the applicable data protection rules.

Needless to say, that the obligation to protect data does not end with the due diligence but also extends to the completion of the M&A transaction.

Sufficient human resources and time have to be reserved so the transaction and particularly the due diligence process can be diligently planned and structured in a way which is compliant with the relevant rules and which secures the right of personality of all involved data subjects.

Dr. Andreas Moll, M.C.J.
Partner, Prager Dreifuss

T: +41 44 254 55 55
E: andreas.moll@prager-dreifuss.com
W: www.prager-dreifuss.com

About the author

Andreas Moll is a partner in the Corporate & M&A team of Prager Dreifuss. He specialises in mergers and acquisitions, corporate finance, takeovers and private equity both on a domestic and international level. In addition, he regularly acts as general corporate counsel, sometimes also as director, of Swiss entities.

Matthias Bürge LL.M.
Partner, Prager Dreifuss

T: +41 44 254 55 55
E: matthias.buerge@prager-dreifuss.com
W: www.prager-dreifuss.com

About the author

Matthias Bürge is a partner in Prager Dreifuss' Corporate & M&A team. His practice focuses on all types of domestic and international transactions (such as mergers, acquisitions, restructurings and spin-offs). He also advises with respect to acquisition financing, be it on the side of the financing banks or on the borrower's side. Bürge has vast experience in the fields of corporate law, contract law and insolvency law. In these fields, he also represents clients in court or before administrative authorities.

Charlotte Rupf
Associate, Prager Dreifuss

T: +41 44 254 55 55
E: charlotte.rupf@prager-dreifuss.com
W: www.prager-dreifuss.com

About the author

Charlotte Rupf is an associate in the M&A team of Prager Dreifuss. She concentrates on domestic and international transactions (such as mergers, acquisitions, restructurings and spin-offs). She also advises both borrowers and financing banks with respect to financing of such transactions. Furthermore, Rupf works in the area of dispute resolution and advises companies with regard to corporate law matters.

PRAGER DREIFUSS
ATTORNEYS AT LAW