GDPR IN M&A TRANSACTIONS

The impact of the General Data Protection Regulation (commonly referred to as the "**GDPR**") on companies has likely not gone unnoticed. However, it is less well known that the scope of the GDPR goes beyond, for example, obtaining consent for sending direct marketing, and also has implications for M&A transactions.

This should come as no surprise. The GDPR lays down rules for any "processing" of "**personal data**". Both terms are broadly defined. All data relating to B2C customers are, of course, personal data. But the same applies to all information concerning employees and contact persons at suppliers and B2B customers – that too qualifies as personal data. "**Processing**" simply means any use of personal data: from collection to deletion and from simple transfer to access.

The transfer of and access to personal data of employees, (contact persons at) customers, and suppliers in the context of **M&A transactions** – between seller, potential buyers, and their advisors (especially during the due diligence phase) – must therefore comply with all GDPR rules.

The entry into force of the GDPR has had another, equally important consequence. In M&A practice, there is increasing attention to the processing of personal data within the target and the extent to which the **target** itself complies with the GDPR ("**GDPR compliance**"). Since the GDPR, non-compliance with data protection rules can have significant negative consequences – in this context, particularly for the buyer.

THE IMPORTANCE OF GDPR IN M&A-TRANSACTIONS

The GDPR provides for effective enforcement of violations. Breaches of the GDPR can be sanctioned with fines (up to EUR 20 million or 4% of global annual turnover), but also with a prohibition on further use of personal data. These are increasingly significant risks for the buyer. Compliance with the GDPR by the target is therefore a key element in the **risk assessment** of the transaction and in determining the target's **value**.

If the target has invested time and resources in GDPR compliance, this will undoubtedly be rewarded with an increase in its value in the event of a transaction. The buyer gains the certainty that they can **continue using the acquired personal data (e.g., customer lists) in the future** and will not need to make major GDPR-related investments. A GDPR-compliant target will be easier to value and will be perceived as a trustworthy and professional contracting party by potential buyers.

On the other hand, a business that has not taken the necessary GDPR measures presents a significant risk for the buyer (e.g., administrative sanctions, prohibition on data use). Understandably, non-compliance by the target is also relevant for valuation purposes, as the buyer will want to build in a safety margin for, among other things, **fines and measures it must take with a view to GDPR compliance**. The buyer will be less willing to pay full price for such a risk-laden acquisition than for a "ready-to-use," compliant one.

Finally, the **choice between a share deal or an asset deal** also significantly affects the GDPR-related risks. Unlike a share deal, where only the shareholder changes, an asset deal involves transferring the ownership of the personal data (as part of the assets) to the buyer, who becomes the new "controller" under the GDPR. Such a transfer brings with it specific obligations under

the GDPR – obligations that do not apply to the same extent in a share deal. In other words, GDPR will generally have a greater impact in the context of an asset deal.

A SAFE DUE DILIGENCE

Inform

In most cases, it will not be necessary to obtain consent from individuals whose data are transferred in the context of an M&A transaction. The Belgian Data Protection Authority recognizes that such transferring will often be legitimate on the basis of the (documented) legitimate interests of the parties involved. That said, individuals must always be informed about how and why their personal data are used. This applies equally in M&A contexts. Companies must therefore ensure that the transfer of personal data in the context of M&A transactions is systematically included in their privacy notices for employees, customers, and suppliers.

Minimize

The seller may only share personal data that are necessary and relevant for the potential buyer(s) in the context of the due diligence process. The scope and level of detail must be aligned with the phase of the transaction process. The Belgian Data Protection Authority recommends providing only general and aggregated (i.e. anonymized) data in the initial phase, especially when there are several potential buyers. As candidates drop out, the seller may gradually disclose more information. Concretely, this means that sellers should provide model agreements (e.g., employment or customer contracts), possibly accompanied by a list of common clauses, instead of individually signed contracts.

Organize

Using a professional data room is not only common practice in M&A transactions, it is also strongly recommended under the GDPR. A data room significantly reduces the risk of data breaches. Since the data room facilitates the transfer of commercially sensitive information and personal data between seller and potential buyer(s), it is crucial that the service provider's data room and privacy practices meet all applicable data protection standards. Common safeguards include encryption, limited access (on a need-to-know basis), access controls, restricted download and print functions, etc.

In addition, the seller must not forget to conclude a data processing agreement with the data room provider. We also recommend that sellers conclude appropriate confidentiality agreements – from a GDPR perspective – with potential buyers and their advisors. These agreements should, among other things, define who has access to the personal data and what happens to them after the due diligence process ends.

Implement

The seller should implement the necessary procedures – for example, for handling data breaches – and ensure that all parties with access to the data room are aware of these procedures (e.g., by including them in the data processing or confidentiality agreements).

In short, it is important to start preparing the data room early and to rely on expert support when doing so.

HOW TO VERIFY GDPR COMPLIANCE?

Know Your Target

It is not always easy for the buyer to determine whether the target complies with the GDPR. A good first step is to understand the purposes for which the target processes personal data. This requires the buyer to take the target's sector into account. For example, in the automotive sector, it is important for buyers to know that a chassis number qualifies as personal data. If the target is a franchisee, familiarity with the GDPR rules applicable in a franchise context is key.

Key Questions

A good understanding of the target enables the buyer to ask focused questions. A useful starting point is requesting the record of processing activities. This record is a good indicator of the company's maturity with regard to data protection. The buyer should also inquire about the legal grounds for processing, purposes of use, implementation of data subject rights procedures, data storage locations, data processing and joint controllership agreements, security measures, appointment of a Data Protection Officer, etc.

Data Protection as a Cultural Value

Finally, the buyer should verify whether the GDPR measures implemented by the target were more than a one-time effort (e.g., in preparation for the due diligence process). It is essential to assess whether the procedures and measures are actually applied in practice and whether incidents have occurred in the past (e.g., a data breach, an investigation by the DPA). The buyer should look for signs that data protection is part of the company culture.

Seller Tip

Targets can expect more in-depth investigations by buyers going forward. A proper self-assessment is therefore crucial – especially in asset deals. This enables the seller to identify and remedy potential risks in advance or assess their impact on price, warranties, and indemnities.

CLOSING THE DEAL

Liability for GDPR non-compliance will likely transfer to the buyer after completion; at the very least, the buyer will experience indirect negative consequences. It is therefore inevitable that the GDPR will increasingly shape the content of transaction agreements.

While many still rely on general warranties (e.g., the target complies with applicable law) to cover GDPR-related risks, it is recommended to include a more specific warranty. This should state that the target not only complies with applicable law but also with its own privacy policies and notices, has implemented adequate procedures and security measures, and is not aware of any data breaches or related complaints.

Often, due diligence will uncover specific risks (e.g., a complaint or existing data breach). In such cases, the buyer is likely to insist on specific indemnities in the acquisition agreement so that liability remains with the seller.

If due diligence reveals that the target is not yet GDPR-compliant on critical points, the parties may also agree on a remediation plan and assign responsibilities accordingly. They may, if needed, formalize this as a closing condition.

Finally, the seller may also have an interest in agreeing with the buyer on responsibilities for further use of the personal data after transfer. Indeed, it is not excluded that the seller could (also) be held liable for processing activities by the buyer that are incompatible with the original purpose for which the data were collected.

USE OF CUSTOMER DATA AFTER THE ACQUISITION

Preparation

As explained above, it is important to verify during due diligence whether the target lawfully processes its customer data – especially when the database is a key asset in the deal. The Belgian DPA requires that customers be informed about the possibility that their data may be transferred to a third party in case of a change in the controller – such as in an asset deal. This possibility should be mentioned in the privacy notice. If not, the seller should still actively inform the customers before the transfer (see below under "Transparency").

Transparency

In the case of an asset deal, the data transfer itself must also be communicated to the affected customers – preferably by the transferring company. This communication should include the identity of the new controller, the legal ground for the transfer, and the right to object.

In addition, it is recommended that the acquiring company informs customers after the transfer – especially if any elements of the processing will change. This includes the company's identity, the purposes and activities for which the data will be used, the categories of personal data, (new) recipients, and the rights of data subjects.

Direct Marketing

When a customer database is transferred in the context of a transaction, no new consent is typically required for direct marketing. This is different from buying data from a data broker. In principle, the new controller may rely on the legal ground used by the original controller, provided it is valid and the data are used for the same purposes. Contacting the same customers about the same products or services is generally permissible, but using the data for other purposes – e.g., promoting different products or services of the buyer – may require new consent.

- Even if a sale or merger is not yet on the horizon, include the potential transfer of personal data in your privacy notices for employees, customers, and suppliers.

- Before transferring personal data in the context of due diligence, consult a privacy expert. They can help document the legal ground (e.g., legitimate interest) and define necessary measures: confidentiality agreements, anonymization, data minimization, access control, etc.

- As a seller/target, prepare for GDPR-related questions from prospective buyers. As a buyer, do not focus solely on the GDPR's formalities but also verify whether the target has embedded a data protection culture. This requires a good understanding of its processing activities.

- Both parties should ensure that GDPR risks are properly addressed in the transaction documents. What used to be standard practice before the GDPR will often no longer suffice.

- In some cases, affected customers must be informed before and/or after the transfer of their personal data. If the buyer wishes to use the data for direct marketing, no new consent is typically required – provided the purpose and nature of the processing remain unchanged.

Questions? Do not hesitate to contact us.

anouk.focquet@faros.eu