The next step after the deal is signed

How to disclose personal data in the course of an asset deal

By Philip Schmidt, LL.B. (Corporate), and Christian Leuthner

More than a year has passed since the General Data Protection Regulation (GDPR) set the framework for the processing of personal data within the European Union (EU). The GDPR obliges controllers ("controller": the natural or legal person, public authority, agency or other body, which, alone or jointly with others, determines the purposes and means of the processing of personal data) and processors ("processor": a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller) to comply with a variety of obligations whenever personal data ("personal data": any information relating to an identified or identifiable natural person, a.k.a. "data subject") is involved. (An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.) The processing of personal data as governed by the GDPR includes the disclosure and/or transfer of personal data in connection with M&A transactions and related processes.

Considering this fact, conducting company acquisitions by means of asset deals may involve considerable difficulties. Share deals, however, are a different story. In the case of a share deal, the company shares are sold and transferred such that the target's ownership structure changes. This, however, does not generally lead to a change in the controller according to article 4 number 7 of the GDPR, as the target's customer data remains with the target. Since no data is transferred and no other action is taken with respect to the data involved (including personal data), generally a share deal does not lead to any issues related to personal data.

In the case of an asset deal, on the other hand, individual assets are sold and transferred. If a business is acquired by means of an asset deal, the personal data of customers is likely to be one of the assets transferred to the buyer. In a digitalized and globalized world, the reach of marketing activities and customer networks is crucial for company success, thus customer data is a core asset. As a result, if an asset deal is conducted, personal data is often disclosed and transferred to a new owner (or controller under the GDPR).

The GDPR extends its reach to M&A transactions.

Non-compliance with and violation of data protection rules under the GDPR may be sanctioned with high fines. Not only does this lead to financial difficulties, but it can also result in severe damage to a company's reputation. In order to avoid such an impact, parties to a transaction should deliberately ensure compliance with data protection law. →

The association of German data protection authorities *(Datenschutzkonferenz* or *DSK)* recently published guidance on personal data processing in the course of an asset deal. The resolution provides a brief overview of the requirements and difficulties connected with the disclosure of personal data in an asset deal from a data protection law perspective. It also offers some practical guidance as to how to ensure compliance with data protection law in the course of such a transaction (see the relevant subsection below for details).

Admissibility of data transmission

Under the GDPR, the processing of personal data is prohibited unless explicitly permitted by law. Processing of personal data pursuant to article 4 number 2 of the GDPR includes any operation or set of operations performed on personal data or sets of personal data, such as collection and use of personal data, but also disclosure of personal data from one controller to another.

Legal grounds for permitted processing of personal data are set out in article 6 of the GDPR. These are, inter alia, the necessity of disclosure in order to perform contractual obligations, a legitimate interest of the controller in certain cases and consent.

Performance of a contract

The processing of personal data is permitted if it is unavoidable for the performance of a contract to which the data subject is a party or if it is required in order to enter into an agreement (article 6 paragraph 1 sentence 1 letter b of the GDPR). However, it is often unclear whether disclosure of personal data is indeed mandatory for the performance a contract. This often applies to employee data where employees will in the future be employed with the buyer as a result of the transaction (please note that there is a special German provision on employee data; legal justification is article 88 of the GDPR, section 26 paragraphs 1 and 3 of the Federal Data Protection Act *(Bundesdatenschutzgesetz)* and section 613a of the German Civil Code *(Bürgerliches Gesetzbuch)*). In any case, processing must be limited to the extent necessary to perform the contract. Therefore, the only personal data that may be disclosed is data that is absolutely required for the performance of a contract. Nevertheless, the fulfillment of a contractual obligation does not entitle a seller to disclose his or her complete set of stored personal data. Generally, only names and addresses of customers are required, not e-mail addresses or order histories. Consequently, performance of a contract pursuant to article 6 paragraph 1 sentence 1 letter b of the GDPR is not a sufficient legal basis for the disclosure and transfer of data that is particularly relevant for the success of a business and thus of great interest to a buyer, such as customers' order histories.

Legitimate interest of the controller

Another legal ground for data processing is a legitimate interest on the part of the seller or buyer ("legitimate interests pursued by the controller or third party"), unless the individual concerned has a predominant interest in the data not being processed (see article 6 paragraph 1 sentence 1 letter f of the GDPR). The legitimate interest of the seller or buyer may be interpreted broadly and includes economic interests.

The legitimate interests of the seller or buyer must be balanced against the legitimate interests of the individual concerned in the particular case at hand. The purpose for which the customers' personal data is disclosed can be an indicator of the outcome of a consideration. There are cases where personal data is "only" disclosed as an annex to an asset. For example, if a production site is purchased and existing customers are delivered, the interest in providing/obtaining certain information to ensure uninterrupted delivery to the business's customers is substantial. As the customers likely have a parallel interest in being provided with seamless continuity of delivery services, usually the data subjects will have no overriding interest in the relevant data not being disclosed. If a CRM database is the asset to be acquired for marketing purposes, there is a legitimate interest of the seller (fulfilment of the purchase agreement) as well as of the buyer (direct marketing of products and increased global reach) in the disclosure of personal data. Recital 70 of the GDPR states that direct marketing can be a legitimate interest. However, customers may have an overriding interest in not being subjected to marketing. Pursuant to article 21 of the GDPR, data subjects must be given the opportunity to object to such disclosure.

Consent

Controllers may also rely on data subjects' consent to the disclosure pursuant to article 6 paragraph 1 sentence 1 letter a of the GDPR. However, consent requirements are rather hefty, as consent must be freely given, specific, informed and unambiguously indicated by a statement of clear affirmation. In addition, con- →

sent may be withdrawn at any time. As a result, other justifications for the disclosure of personal data should be utilized if available. Under specific circumstances, however, a customer's consent is inevitably required (for example, in cases where the personal data concerned falls under certain special categories as delineated in article 9 of the GDPR).

Resolution published by the German data protection authorities

On May 24, 2019, the *DSK* published a resolution on the disclosure of personal data in an asset deal in order to create some degree of legal certainty for parties to such a transaction. The *DSK* created case groups based on the seller's and buyer's legitimate interests in light of article 6 paragraph 1 sentence 1 letter f of the GDPR (please note that the data protection authorities of Berlin and Saxony did not agree to the second case group). The resolution does not consider any other legal basis for disclosure.

Customers' personal data regarding existing contractual relationships

Under German law, transfer of a contract requires the consent of any other parties to the contract. The *DSK* argues that the agreement of the customer in this context includes – "as a minus" – consent to disclosure of the data. This way, the interests of the data subject are sufficiently considered.

Existing customers without current contracts whose last contractual relationship is older than three years

Under German civil law, the general limitation period is three years, starting at the end of the year in which a claim arises. The three-year period is often used as a last resort to keep personal data (not including data that must be kept due to statutory retention periods).

According to the *DSK*, personal data from existing customers with whom the last active contractual relationship ended more than three years ago may be disclosed, but only used when the use is related to statutory retention periods (in particular for tax-related purposes). In any other case, the data subject's interest in the data not being used outweighs any other parties' interests.

A conceivable alternative is that the personal data of the customers concerned is not disclosed to the buyer but remains with the seller. If an insolvency administrator is involved, he or she will try to find a service provider (to be financed with the assets) who will retain the data for a certain period.

Personal data of customers in cases of advanced contract initiation; existing customers without current contracts and whose last contractual relationship is less than three years old

In cases where the last contractual relationship is not older than three years (again taking into account the general limitation period under German law) and in cases where a contractual relationship with a prospective customer has been initiated in an advanced stage, the personal data of such customers may be disclosed if the data subjects have sufficient time (the *DSK* suggests six weeks) to object to their data being disclosed to the buyer. This is known as the opt-out model. The *DSK* considers this procedure to be cost saving for companies, as it takes the interests of the customers into account to a sufficient extent without generating excessive effort or risk on the part of the company. According to the *DSK*, many customers would be surprised if asked to give their express consent and would likely refuse to grant it, which would be contrary to the parties' interests. The option to object should be simple and presented in a consumer-friendly manner for example an option to tick a box in an online procedure.

The *DSK* emphasizes that banking data (IBAN) cannot be disclosed using the opt-out model. The explicit consent of customers is generally required for disclosure of banking data. This, however, does not include payment history.

Customers' personal data in cases of open claims

Claims against customers may be transferred unless prohibited by law (section 398 and following of the German Civil Code. See section 399, the 2nd alternative German Civil Code and section 354a of the German Commercial Code [*HGB*]). In this context, data may be disclosed by the former creditor to the new creditor. The data subjects' interests, however, outweigh other interests if the transfer is excluded by agreement.

Customers' personal data belonging to a special category pursuant to article 9 paragraph 1 of the GDPR

Article 9 paragraph 1 of the GDPR prohibits the processing of special categories of personal data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or →

trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person). Such data may only be processed by means of informed consent in accordance with article 9 paragraph 2 letter a and article 7 of the GDPR. This, however, only applies to customer data. Employee data may be disclosed to exercise rights under employment law (article 9 paragraph 2 letter b and paragraph 4, section 88 of the GDPR; section 26 paragraph 3 of the Federal Data Protection Act and section 613a of the German Civil Code).

Conclusion

The GDPR extends its reach to M&A transactions. We welcome the resolution by the *DSK* as an official statement on the disclosure of personal data in the course of an asset deal. Although the statement is non-binding, it provides transaction parties with objective guidelines regarding how to comply with data protection law. Given the fact that transaction parties and authorities are increasingly focusing on data protection law, more comprehensive guidance on data protection during a transaction is needed, as well as direction in dealing with employee data and data disclosure during a due diligence process (which the resolution does not cover at all). Note here the planned £99 million fine announced by the UK Information Commissioner's Office against a global hotel group due to a security incident that was not identified during due diligence.

The resolution also fails to assess which categories of personal data fall within the scope of the individual case groups. Due to this lack of information, an individual assessment of the permitted disclosure of customer data during an asset deal is always required.

Practical recommendations: what transaction parties need to consider

As non compliance with data protection law may lead to high fines as well as reputational damage, and since the effort of data implementation is great when a target does not comply with data protection law, buyers and sellers are strongly advised to take data protection law into account at all stages of a transaction. This leads to the following recommendations:

- **Find a legal justification for the disclosure of personal data.** Personal data may not be disclosed without a legal justification. Both seller and buyer need to assess whether the disclosure of personal data in connection with the transaction falls within the scope of one of the above-stated case groups. If it does not, other legal justifications need to be considered.
- **Adhere to the principles of data minimization and purpose limitation.** Personal data should only be processed to the extent required for the specific purpose for which it was collected – and solely for that purpose. If the buyer does not continue to pursue the same purpose, consent is likely required.
- **Implement adequate technological and organizational measures.** Controllers and processors must implement an adequate level of data protection to ensure adequate data security (for example, encryption or pseudonymization of data, "pseudonymization" meaning the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and is subject to technological and organizational measures to ensure the personal data is not attributed to an identified or identifiable natural person). This also includes the security supplied by service providers.
- **Inform data subjects.** The controller (seller/buyer) must provide data subjects with comprehensive information regarding the intended processing procedures (articles 13 and 14 of the GDPR). If information was directly obtained from the data subject, this information regarding processing procedures must be provided when the initial processing occurs. In any other case, data subjects must be informed as soon as possible, at the latest within one month. <–

Dr. Philip Schmidt, LL.B. (Corporate)
Rechtsanwalt Reed Smith LLP
Frankfurt am Main

pschmidt@reedsmith.com

Christian Leuthner
Rechtsanwalt Reed Smith LLP
Frankfurt am Main

cleuthner@reedsmith.com

www.reedsmith.com