Data protection and insolvency – an overview for practitioners

By Thilo Märtin, Attorney-at-Law in Germany, Sven Sperling, Attorney-at-Law in Germany, and Susi Barbara Kropp-Kuhn, Qualified Judicial Executive

Introduction

The EU General Data Protection Regulation (GDPR), which took effect on 25 May 2018, has without doubt focused minds on the subject of data protection. The range of fines that can now be imposed – up to 20 million euro or 4% of a company's total annual turnover – is one reason, perhaps the main reason, for this new awareness.

The fact that data protection law also similar to the GDPR existed previously, has apparently escaped the notice of most companies. The two-year period between the Regulation's entry into force and its application does not appear to have been long enough to allow for preparations. Official guidelines were also a long time coming, probably also contributing to the poor implementation.

In the event of insolvency, a company's failure to implement data protection law is a matter for the insolvency administrator, who becomes the controller of the company's data. The insolvency administrator has the responsibility for complying with data protection law when he or she takes possession of the insolvency estate.

If optimum realisation of the insolvency estate is to be achieved, a company's customer data records cannot be left out. But the question of whether personal data can be used in relation to corporate transactions and restructuring measures requires the weighing of a number of complex data protection considerations. There is no doubt that the new requirements and increased fines have increased liability risks for insolvency administrators.

This article gives an overview of the key data protection issues affecting insolvency administrators. It focuses only on the questions faced by (preliminary) insolvency administrators in connection with data protection compliance within debtor undertakings. That administrators also have data protection requirements to apply within their own organisation goes without saying, however we do not discuss this issue here.

I. Data protection during insolvency – general

Article 2 of the GDPR provides that the regulation applies only to the processing of personal data. Processing means virtually any operation involving personal data (including transfer to another party and even simple disclosure).

Under Article 4(1) GDPR, personal data means any information relating to an identified or identifiable natural person (such as names, email addresses, telephone numbers, payment data, purchase histories, operational data and machine data collected automatically, interests, hobbies, age or IP addresses).

Data protection law does not cover all data – only data which relates to a person. Therefore, data concerning legal entities is not personal data. With regards to customer data, only the name of the customer contact is relevant in data protection terms, unless the customer is a natural person. Note that information concerning sole traders, as natural persons, does count as personal data, as the Regulation protects all natural persons and does not require a person to be a consumer.

Compliance with data protection obligations is the responsibility of the 'controller' as defined in Article 4(7) GDPR. The controller is the natural or legal person which determines the purposes and means of the processing of personal data.

The (preliminary) insolvency administrator as controller

On transfer of the right of management and disposal (section 80 of the German Insolvency Code (*Insolvenzordnung*, InsO), decision-making authority over the debtor's assets, and thus also its data, passes to the administrator.

From this point on, the insolvency administrator can and must decide on the purposes and means of processing of data. However, he or she can determine these purposes and means only after taking charge of the insolvency estate (section 148 InsO). To act as controller before this time, without actual influence over the data, would be inequitable.[1]

All data, as economically realisable interests, is initially subject to attachment to the debtor's insolvency estate in accordance with section 35 (1) InsO. The administrator can access it directly from where it is stored (e.g. the debtor's server). If data is stored in a cloud system, contractual claims against the service provider, as preferential claims, permit de facto access.[2] Whether the access is direct or, if a processor is used, indirect, is irrelevant; what counts is de facto control.

Thus, once the insolvency administrator has taken possession of the debtor's assets, he or she is considered to be the controller according to the GDPR definition.

A 'strong' preliminary insolvency administrator (one to whom the power of management and disposal has passed) is also considered to be a controller under certain conditions. A 'weak' preliminary insolvency administrator will only in exceptional cases be considered the data controller, as the individual duties conferred on him or her in accordance with section 22 (2) InsO generally relate to securing the insolvency estate and do not grant him or her any extensive powers.[3]

For the sake of completeness, we point out here that the supervisor in insolvency proceedings conducted by the debtor in self-administration does not become the controller in accordance with the GDPR, as in this case the debtor retains the power of management and disposal.

Processing on behalf of a controller

Data is not considered part of the insolvency estate, with corresponding effects in terms of liability, if the debtor processes it on behalf of a third party (Processor, Article 28 GDPR). Data accessed by the debtor in connection with processing activities carried out on behalf of another controller does not become part of the insolvency estate. In doctrinal terms, the most convincing view is that the claim to return (transfer) and erasure of data laid down in the mandatory processing agreements (Article 28 GDPR) should be classed as a right to segregation.[4] From the perspective of the party commissioning the processing, processing contracts should be drafted to allow them to continue to have the broadest control possible over the data. Given the strict terms of data processing contracts, the realisation of data of a contract processor for other purposes in the course of restructuring, is generally out of the question (see below).

[1] *Thole*, Der (vorläufige) Insolvenzverwalter als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO, ZIP 2018, 1001, 1003.
[2] *Berberich/Kanschik*, Daten in der Insolvenz, NZI 2017, 1, 2.
[3] *Thole*, Der (vorläufige) Insolvenzverwalter als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO, ZIP 2018, 1001, 1011.
[4] *Berberich/Kanschik*, Daten in der Insolvenz, NZI 2017, 1.

Insolvency administrator and debtor as joint controllers

One new feature of the General Data Protection Regulation is the construct of the 'joint controller'. Where two or more controllers jointly determine the purposes and means of processing, they are joint controllers within the meaning of Article 26 GDPR.

To be joint controllers, both parties concerned must also be controllers in accordance with Article 4(7) GDPR independently of each other. In accordance with Article 4(7) GDPR, decisions regarding purposes and means may be made alone or jointly. The possibility that a debtor and its insolvency administrator may together be joint controllers cannot be immediately ruled out.

As described above, to be a controller for the purposes of the GDPR, a party must have both legal and actual influence over the processing of data. An insolvency debtor ceases to satisfy the legal criteria required to be identified as data controller at the latest when the power to manage and dispose of the debtor's assets passes to the insolvency administrator in accordance with section 80 InsO. The power of management and disposal is conferred on the insolvency administrator exclusively and removed from the debtor entirely. In practical terms, the activity of the insolvency administrator only produces a commingling of spheres of influence.[5] Mere cooperation is not sufficient to make the parties joint controllers.[6]

Consequently, from the time the order commencing proceedings is issued, the insolvency administrator controls the processing of data to such an extent that responsibility in terms of data protection is clearly transferred to him or her alone. There is thus no joint control by the insolvency administrator and the debtor.

This issue is more difficult to assess in the period prior to this, however. During preliminary insolvency proceedings, the administrator's accountability in data protection terms depends on the de facto influence he or she has over the relevant data processing operations. The weaker the position of the insolvency administrator and the less influence he or she has over handling of data as a result, the less likely he or she is to be viewed as a data controller (Article 4(7) GDPR).

Regarding preliminary proceedings, the question of whether the debtor and insolvency administrator are joint processors, even in relation to individual data processing operations only, should be carefully examined. If they jointly determine means and purposes, an arrangement in accordance with Article 26 GDPR specifying who is responsible for compliance with the obligations under the GDPR is required. Regardless of this arrangement, data subjects can continue to exercise their rights against both parties.

The requirements regarding the precise form of such arrangement are currently unclear, as bodies such as the European Data Protection Board (EDPB) have not yet commented.

Case: possession of only part of the estate

The status as controller has both a legal and a factual component. So, what happens if the insolvency administrator does not take possession of some parts of the insolvency estate?

In accordance with previous rulings of the Federal Court of Justice (*Bundesgerichtshof*, BGH),[7] the insolvency administrator's obligation to assume possession of the insolvency estate under 148 InsO does

[5] ZIP 2018, 1001, 1004.

[6] *Paal/Pauly/Martini*, 2nd ed. 2018, GDPR Article 26 paragraphs 19-21.

[7] BGH, judgment of 19 June 2008 - IX ZR 84/07.

not necessarily cover all of the debtor's assets. If taking possession would involve disproportionate effort, the insolvency administrator does not intend to realise certain assets, and satisfaction of the creditors is therefore not jeopardised, the insolvency administrator may choose not to assume possession.

This means that it is possible for the insolvency administrator not to be regarded as the data controller, thus limiting his or her liability. If items are taken into possession merely in order to determine whether they belong to the insolvency estate and assess whether they can be realised, the administrator does not automatically have full responsibility for them. However, obligations to preserve the items and ensure that they are safe for others cannot be evaded.

If, when examining whether an item can be realised, the insolvency administrator finds that data is being processed in breach of data protection principles, his or her duty to mitigate damage means he or she must cease processing. Reasonable technical and organisational measures must also be observed when assessing whether assets can be realised.

If the debtor's business operation is released from the insolvency estate, the insolvency administrator is no longer responsible for the processing of data in the debtor undertaking.

In practice, however, it can be assumed that if the debtor's business is operated by the insolvency administrator once proceedings have commenced, he or she is the data controller within the meaning of the GDPR. As such, he or she has two competing obligations: to continue to operate the debtor's business in accordance with section 158 InsO on the one hand, and to comply with data protection law on the other. Companies entering insolvency have usually been in distress for a long time, and in small and medium-sized companies in particular it is often the case that implementation of the GDPR has not been given top priority. Frequently even the most basic measures such as data protection notices and legal notices on the company's website are absent; and technical and organisational measures have certainly not been adequately described and implemented. In such cases, the insolvency administrator, working closely with the creditors and the court, must examine whether available financial and organisational resources permit GDPR compliance measures to be taken in the short term, or whether, in case of doubt, operations must cease.

General obligations

We do not discuss the general obligations of the controller under the GDPR, such as the duty to maintain records of processing activities (Article 30 GDPR), compliance with data subject rights (Articles 12 to 23 GDPR), rules relating to processors (Article 28 GDPR), appointment of a data protection officer (Articles 37 to 39 GDPR) and compliance with the necessary technical and organisational measures (Article 32 GDPR).

II. Realisation of personal data in insolvency

Without doubt, personal data, especially customer data, is of significant economic value for companies and will become increasingly valuable in the future. Advertising targeting particular groups of customers or potential customers, or focussing on particular products is a source of new marketing opportunities.

Customer data forms part of an insolvent debtor's assets, meaning that it is an attractive target for realisation. The question for the insolvency administrator is whether that data can be realised legally.

If the data concerns natural persons, it can only be realised in compliance with data protection law. It must be remembered that personal data cannot simply be sold in the same way as merchandise. This is particularly important in relation to special categories of personal data in accordance with Article 9 GDPR, such as health data. With a few exceptions specified in Article 9(2) GDPR, this data can only be processed with consent.

Consideration of the restructuring scenario

To determine whether data can legally be realised, the specific restructuring scenario needs to be examined closely. The question of whether the data is transferred to a new legal entity and is thus processed within the meaning of data protection law is particularly important.

Share deals and corporate transformations

Share deals involving the transfer of the shares in the debtor company are not problematic. If the share deal involves disposal of some of the company's shares or the entire undertaking, there is no transfer of data to a third party for the purposes of data protection law and thus no processing of data. The data remains within the undertaking and the controller of that data does not change in data protection terms.

Any resultant membership of a group of undertakings does not, in the absence of an intra-group privilege, release the company from the requirement to have a legitimate basis for transmission of data within the group. However, the existence of an intra-group customer data management function may constitute a legitimate interest in processing (see below).

In the case of corporate transformations, the acquiring or newly established legal entity assumes the legal position of controller due to the partial universal succession provided for in section 20 (1) No. 1 of the German Transformation Act (*Umwandlungsgesetz*, UmwG). As a rule, there is no transfer and thus processing of personal data here either.[8]

Although the controller does change if there is a share deal or transformation and insolvency proceedings are terminated alongside this (the insolvency administrator is replaced by the organs of the company), a mere change of controller does not produce any specific obligations towards data subjects such as a renewed obligation to provide information.

Asset deals

In the vast majority of cases, however, realisation takes the form of an asset deal, which involves the sale of specific assets of the insolvent undertaking. Transfer of data to the acquirer, as a third party, constitutes transfer and thus processing for which a legal basis is required.

Legal bases for the processing of personal data

Under data protection law, processing of personal data is prohibited without authorisation. Processing is permitted only if one of the conditions set out in Article 6 GDPR is satisfied (or another legal basis for the processing applies).

In particular, processing of data is permitted if the data subject has consented to the processing (Article 6(1)(a) GDPR), processing is necessary for the performance of a contract with the data subject (Article 6(1)(b) GDPR) or processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (Article 6(1)(f) GDPR).

Consent as legal basis for processing

Transfer of data is permitted if the data subject has given consent. Under Article 7 GDPR consent must be actively given ('opt-in'), freely given, specific, informed and unambiguous; 'bundled' consent to use of data is not sufficient.

The prohibition set out in Article 7(4) GDPR must also be observed. Consent is invalid if performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

[8] *Berberich/Kanschik*, Daten in der Insolvenz, NZI 2017, 1, 8.

If consent has not been given, the insolvency administrator can obtain it before the sale. As well as involving significant administrative effort, the success of this course of action also depends on the response of the data subjects. A satisfactory response has previously been obtained in relation to the sale of a pharmacy. In other sectors, the response can be expected to be more cautious.

Performance of a contract with the data subject

Another possible legal basis for the processing of customer data is the performance of a contract. For this to apply, the acquiring entity must also take over the ongoing contracts in place between the customer and the insolvency debtor. The acquirer can then use the data to perform the contract as the insolvency debtor did previously. In data protection terms, transfer of data in connection with the sale of rights and obligations arising from the contracts is merely an intermediate step.

The provisions of civil law regarding the transfer of contracts must be complied with here, and they ultimately require data subjects to give their consent to the transfer of the contracts. If consent is obtained by means of standard business terms, section 309 No. 10 of the German Civil Code (*Bürgerliches Gesetzbuch*, BGB) provides that consent is only effective if the acquiring party is identified by name in the standard business terms.[9] This can be done by amending the company's standard business terms to explicitly identify the party acquiring the contract and presenting this to the data subject as an amendment to the standard business terms. If and to the extent that the data subject is granted an adequate period to object to the amendment (usually three weeks) and insofar as transfer of the contract to the acquirer is effective under civil law, this method can also be used to transfer customers and customer data.[10] In the case of the simple sale of accounts receivable, section 402 BGB permits the transfer of data in conjunction with Article 6(1)(b) GDPR.[11]

By contrast, the transfer of employee data to the acquirer of a business is permitted under section 613a BGB provided that the employment contracts are transferred to the acquirer.

Processing on the basis of a legitimate interest

If customer data is sold, the processor of that data is the insolvency administrator rather than the debtor. The debtor is only a third party here.

Controller's legitimate interest

The insolvency administrator's legitimate interest in transfer of data arises from his/her duty under section 159 InsO to realise the debtor's assets as favourably as possible. This involves considering every option for realisation to enable optimal satisfaction of creditors. Parts of an undertaking sold without their customer data would be significantly less attractive, making optimal realisation unlikely. The preservation of jobs during restructuring of an undertaking can also be taken into account when weighing interests.[12]

Legitimate interests of third parties

Alongside the processor's interests, the interests of a third party can also be a legitimate basis for processing. Possible third parties are creditors, the debtor, and the debtor's employees.

[9] Alternatively, section 309 No. 10 BGB provides for a right of the partner to free itself from the contract.

[10] The option of giving advance notice of the transfer and enabling data subjects to object is also supported by the Bavarian Data Protection Authority for the Private Sector (*Bayerisches Landesamt für Datenschutzaufsicht*, BayLDA), see press release of 30 July 2015.

[11] Zeitschrift für Bank- und Kapitalmarktrecht, *Frisse et al*., BKR 2018, 177 (183).

[12] *Beyer/Beyer*, Verkauf von Kundendaten in der Insolvenz – Verstoß gegen datenschutzrechtliche Bestimmungen? (NZI 2016, 241)

Here the creditors' interest is the same as the insolvency administrator's: optimal realisation of the debtor's assets. The debtor can also have an interest in optimal realisation – if surplus assets are returned to the debtor after satisfaction, for example.

Interests of data subjects

The interests of the controller and third parties must be weighed against the rights of data subjects, i.e. customers, and most particularly their right to self-determination regarding information (Article 2 (1) GG).

The fundamental right to self-determination in relation to information ensures that people can determine who knows what about them and what this knowledge is used for. This fundamental right does not apply without limitation. The data subject's interest in maintaining confidentiality, which in principle always applies, will not always weigh more heavily than a particular interest in use of the information. The balance will vary depending on the individual case, and in particular on which specific data are affected, and whether these data concern the data subject's private life or can be attributed to the business sphere.

Weighing of interests

To determine which is the overriding interest, all circumstances of the case must be evaluated. If only non-sensitive customer data are affected – such as names and email addresses – and if the insolvency administrator can show that his or her legitimate interest is founded on continuation of the business and the objective of optimal creditor satisfaction, it can be reasonably assumed that the insolvency administrator or insolvency creditors have an overriding interest.

It must also be borne in mind that customer data has usually been provided to the company knowingly and it can therefore be assumed that the customer has a general interest in the goods and services offered.

If a part of an undertaking is transferred in its entirety, and if employment contracts are transferred along with it by way of a transfer of the undertaking in accordance with section 613a BGB, it should also be considered when weighing interests that the data will be handled by the same individuals.

A decision to prohibit the transfer of customer data would reduce the prospects for realisation of the assets involved in the insolvency, which would be contrary to wishes of the legislator that optimal creditor satisfaction should be achieved (section 159 et seq. InsO).

It is clear that the interests of the parties are different when it comes to insolvency, and that precisely as a result of that difference a balancing of those interests may come out in favour of realisation.

If a legal entity is acquired by way of a share deal and is subsequently incorporated into a group of undertakings, it should be noted that recital 48 of the GDPR explicitly refers to the transmission of client data within the group for administrative purposes as a legitimate interest. As a result, the requirements for the transmission of data are simplified once the debtor undertaking is incorporated into the group.

In the view of the Bavarian Data Protection Authority for the Private Sector (BayLDA) regarding the previous legal position (press release of 30 July 2015), a 'right-of-objection' procedure was conceivable,[13] as long as data subjects were granted a sufficiently long period in which to exercise their right of objection beforehand. If the data subject does not exercise this right of objection, it can be assumed when weighing the various interests that there is no overriding interest precluding the sale. The BayLDA also takes the view that where the only data transmitted comprises names and postal addresses, this can be done even without applying the 'right-of-objection' solution.

[13] See fn 9 above.

For all the advantages that this solution brings in practice, it should not be relied on blindly. Note that a time-limited right of objection can merely be taken into account in the weighing of interests, and does not justify the transmission per se.

Regarding subsequent use of customer data, it must also be remembered that provisions of competition law also apply alongside data protection law. The *Deutsche Datenschutzkonferenz*[14] (a forum for German data protection supervisory authorities) regards section 7 of the German Act against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb*, UWG) as key[15] for the weighing of data protection interests, although recital 47 of the GDPR expressly refers to direct advertising as a justified interest. As a consequence, the Deutsche Datenschutzkonferenz says, an entity acquiring data by way of an asset deal must obtain (renewed) customer consent for electronic or telephone advertising. One could easily take a different view – but that would risk a run-in with the data protection authorities.

Due diligence

Because the disclosure of personal data to interested parties for due diligence purposes constitutes processing of that data, a legal basis is required for that too. Processing will be based on a legitimate interest of the seller or the acquirer. The key factor here is how much data needs to be necessarily disclosed. The phrase 'as much as necessary, as little as possible' is a good guide.

Alongside customer data, employee data is also of relevance here. The value of an undertaking can be influenced quite considerably by its employees, i.e. their qualifications and costs. Interested parties will want to look at this data in as much detail as possible. To comply with the principle of data minimisation under Article 5(1)(c) GDPR, this data should only be supplied in statistical, pseudonymised or anonymised form.

Consequences of unlawful sale

Under Article 58(2) GDPR, the supervisory authorities can take various corrective measures and can in particular prohibit processing and require the erasure of data.

The supervisory authorities may impose fines in accordance with Article 83 GDPR in addition to or in place of measures under Article 58(2) GDPR.

If data is processed without a legitimate basis, for instance because there is no overriding legitimate interest in the sale of customer data, this constitutes an infringement of the basic principles for processing in accordance with Article 83(5)(a) GDPR. Infringements of Article 83(5) GDPR attract fines at the higher level and may be up to EUR 20,000,000 or 4% of a company's worldwide annual turnover.

The fines may be imposed on the controller or on a processor working for the controller as a natural or legal person, and consequently on the insolvency administrator personally (if he or she is the controller) and on the debtor (for processing carried out before proceedings commence or after they end). Fines which are put into effect after proceedings have commenced and rank as preferential liabilities may give rise to liability on the part of the administrator under sections 60 and 61 InsO, and thus parallel liability for the administrator and the insolvency estate.

In 2015, under the old regime, the BayLDA imposed a five-figure fine on a buyer and seller for the unlawful transfer of email addresses held by an online shop. What kind of sanctions will be imposed under the new framework remains to be seen.

[14] Kurzpapier Nr. 3 – Verarbeitung personenbezogener Daten für Werbung, 29 June 2017.

[15] What further changes will result from the proposed e-privacy regulation (repealing Directive 2002/58/EC) or the 'digital content' directive (COM(2015) 634 final) remains to be seen.

III. Summary

For insolvency administrators wishing to realise personal data, detailed examination of data protection law is indispensable. This is due not only to the fines that can now be imposed, but also to the increased economic importance of personal data.

While share deals and corporate transformations are not problematic in regards to the transfer of customer data, asset deals raise significant questions for the practitioner and administrators. Various interests must be weighed carefully.

In the absence of relevant court rulings, the only guidance available at present is that produced by the data protection authorities. The 'right-of-objection' solution proposed by the BayLDA should always be considered.

Sven Sperling is an attorney-at-law in Germany and a prospective specialist in employment law at MKM + Partner Rechtsanwälte PartmbB in Nuremberg. He advises numerous undertakings and corporate groups in all industries on data protection law and acts as an external data protection officer.
Email: *sperling@mkm-partner.de*

Thilo Märtin is an attorney-at-law in Germany and a founding partner of MKM + Partner Rechtsanwälte PartmbB. His main areas of focus are data protection, IT law and intellectual property. He advises clients from Germany and abroad on all areas of European and German data protection law.
Email: *maertin@mkm-partner.de*

Susi Barbara Kropp-Kuhn, qualified judicial executive, is responsible for quality management within Schultze & Braun Rechtsanwaltsgesellschaft für Insolvenzverwaltung mbH. She is also the data protection manager for Schultze & Braun's insolvency administration unit. She has worked as an expert witness and insolvency administrator since 2008.
Email: *SKroppKuhn@schultze-braun.de*