LEGAL REVOLUTIONary
Rechtsmagazin der digitalen Wirtschaft

Datenschutzrechtliche Millionengeldbußen bedrohen die M&A Branche

Was ist in der Planung der Due Diligence zu beachten?

Nadine Neumeier (LL.M.) | Rechtsanwältin | Baker McKenzie

18. November 2020

LR 2020, Seiten 290 bis 298 (insgesamt 9 Seiten)

Die EU-Datenschutz-Grundverordnung („DSGVO") findet auch auf M&A-Transaktionen Anwendung. Dies wurde zuletzt eindrucksvoll verdeutlicht, als die Aufsichtsbehörde in Großbritannien (ICO) gegen eine internationale Hotelkette im Juli 2019 eine Geldbuße in Höhe von rund EUR 110 Mio. verhängte, die kürzlich auf EUR 20.450.000 reduziert wurde. Der Grund war eine Cyber-Attacke, die beim Erwerb einer anderen Hotelkette aufgrund eines nicht ordnungsgemäß durchgeführten Due Diligence Prozesses nicht erkannt wurde. 1

Die DSGVO sieht bei Verstößen Geldbußen von bis zu 20 Millionen Euro oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs eines Unternehmens – je nachdem, welcher Betrag höher ist – vor. Doch welche datenschutzrechtlichen Erwägungen stellen sich üblicherweise in einer M&A-Transaktion und was ist zu beachten? Häufig diskutiert wird die Übermittlung von Daten im Rahmen eines Asset Deals - wenig Beachtung geschenkt wird den vorbereitenden Maßnahmen, wie z.B. der Vorbereitung der Due Diligence oder der Offenlegung von personenbezogenen Daten im Datenraum durch die Verkäuferseite. Dieser Beitrag soll ebendiese oft vernachlässigten Aspekte beleuchten. 2

I. Vorbereitung der Due Diligence: Interne Datenbeschaffung

Zunächst lohnt es sich, einen Blick auf die vorbereitenden Maßnahmen der Due Diligence zu werfen. Die interne Datenbeschaffung kann damit einhergehen, dass personenbezogene Daten innerhalb der Unternehmensgruppe an ein Unternehmen der Gruppe übermittelt werden, die den Due Diligence Prozess vorbereitet. Eine solche Übermittlung stellt eine Verarbeitung von personenbezogenen Daten dar und ist damit am Maßstab der Art. 5 ff. DSGVO zu bewerten. Dies gilt sowohl für Übermittlungen innerhalb einer Unternehmensgruppe als auch für Übermittlungen an externe Unternehmen. 3

1. Jede Übermittlung bedarf einer Rechtsgrundlage

Die Übermittlung der personenbezogenen Daten zum Zweck der internen Datenbeschaffung bedarf – auch innerhalb einer Unternehmensgruppe – einer Rechtsgrundlage. Die Praxis zeigt, dass eine (wirksame) Einwilligung in die Offenlegung sowie Übermittlung von personenbezogenen Daten der Beschäftigten, Kunden sowie Partnern zum Zwecke der Transaktion regelmäßig nicht - zumindest nicht in allen Fällen - eingeholt werden kann. Daher kommt es unter anderem auf die Interessensabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO an. 4

a) Berechtigtes Interesse

Sowohl der Verkäufer als auch die Zielgesellschaft (Target) der Transaktion können berechtigte Interessen geltend machen. Dies sind zumeist die berechtigten, beispielsweise wirtschaftlichen, Interessen der Parteien, die M&A Transaktion vorzubereiten. 5

b) Überwiegendes Interesse der betroffenen Person

Es ist davon auszugehen, dass die betroffene Person (z.B. ein Mitarbeiter[1] oder ein Kunde) grundsätzlich ein Interesse an der Geheimhaltung ihrer personenbezogenen Daten hat. Dies hängt jedoch vom Einzelfall ab. Ein geringeres Geheimhaltungsinteresse wird angenommen, wenn es lediglich um berufsbezogene Kontaktdaten eines Kundenansprechpartners geht. Ein größeres Geheimhaltungsinteresse wiederum besteht in Bezug auf Evaluierungsdaten eines Mitarbeiters oder das Kaufverhalten eines Kunden im B2C-Bereich. 6

c) Abwägung und Erforderlichkeit

Es empfiehlt sich, in jedem Unternehmen der Unternehmensgruppe eine Stelle zu identifizieren, die die Daten „einsammelt". Sofern dies nicht möglich ist, sollten zumindest entsprechende Datenübermittlungsverträge zwischen den jeweiligen Verantwortlichen geschlossen werden. Dadurch können die Übermittlungen aus Sicht der technischen und organisatorischen Maßnahmen abgesichert werden, beispielsweise können die Pflicht zur Pseudonymisierung der personenbezogenen Daten sowie die Verschlüsselung der Übermittlung aufgenommen werden. Hierbei ist jedoch zu beachten, dass der Abschluss 7

[1] Aus Gründen der Lesbarkeit wird bei Personenbezeichnungen die männliche Form gewählt, es ist jedoch immer die weibliche Form mitgemeint.

eines Datenübermittlungsvertrags keine Rechtsgrundlage darstellt. Vielmehr kann dies eine Interessensabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO positiv beeinflussen.

d) Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten (z.B. Gesundheitsdaten, Daten zur Gewerkschaftszugehörigkeit oder zu religiösen und weltanschaulichen Überzeugungen) können in diesem Stadium regelmäßig nur in anonymisierter Form übermittelt werden, da die Vorbereitung einer Due Diligence (abgesehen von der Einwilligung, die jedoch jederzeit widerrufen werden kann und daher in diesem Fall nicht praktikabel ist) nicht unter die Ausnahmen des Art. 9 Abs. 2 DSGVO fällt. Die Übermittlung in anonymisierter Form unterfällt nicht der DSGVO. Anonymisierte Daten sind solche Daten, die keinen Personenbezug mehr aufweisen. Hier kommt beispielsweise das Schwärzen der Daten in Betracht. 8

2. Zweckkompatibilität

Das übermittelnde Unternehmen muss feststellen, ob die Verarbeitung zum Zweck der Vorbereitung der Transaktion mit dem Zweck, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist (Art. 6 Abs. 4 DSGVO). Zum Beispiel könnten Kontaktdaten eines Kunden im B2C Bereich für Marketingzwecke erhoben worden sein. Dieser Zweck steht nicht offensichtlich im Einklang mit der Vorbereitung einer Unternehmenstransaktion. Im Rahmen der Zweckkompatibilität sind verschiedene Kriterien zu berücksichtigen. Als Beispiel genannt seien die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen oder das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können. Eine pauschale Aussage kann nicht getroffen werden, da dies stark von den in der jeweiligen Zielgesellschaft enthaltenen personenbezogenen Daten abhängt. 9

3. Informationspflichten gegenüber Mitarbeitern, Kunden und Lieferanten

Sollen nicht geschwärzte Daten innerhalb der Unternehmensgruppe zur Vorbereitung der Due Diligence übermittelt werden, sind die Informationspflichten (Art. 13 Abs. 3 DSGVO) gegenüber den betroffenen Personen (z.B. Mitarbeitern, Kunden und Lieferanten) zu beachten. Diese finden ebenso Anwendung, wenn der Verantwortliche die personenbezogenen Daten nachträglich für einen anderen Zweck weiterverarbeiten will. In diesem Fall sind die betroffenen Personen erneut zu informieren. Dies stellt typischerweise dann ein Problem im Rahmen einer Transaktion dar, wenn die Transaktion noch geheim gehalten werden soll. 10

Es stellt sich die Frage, ob eine Ausnahme des Art. 13 DSGVO greift. In Einzelfällen kann auf Art. 13 Abs. 4 DSGVO zurückgegriffen werden, wenn die betroffenen Personen (z.B. Key Employees und Mitarbeiter) über diesen neuen Zweck der Verarbeitung bereits informiert sind. Zu beachten ist, dass die Ausnahme nur greift, wenn die betroffene Person über die Informationen des Art. 13 Abs. 1 und 2 DSGVO bereits verfügt. Eine analoge Anwendung des Art. 14 Abs. 5 lit. b DSGVO, wonach die Informationspflicht nicht besteht, wenn die Erteilung der Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, ist risikobehaftet. 11

Einige Unternehmen sehen allgemeine Informationen in ihren Datenschutzhinweisen z.B. gegenüber Mitarbeitern und Kunden vor, die bereits den Fall künftiger M&A Transaktionen beinhalten. Es ist jedoch fraglich, ob eine solche „Blanko"-Information den Anforderungen der Transparenz genügen kann. Einige Unternehmen sehen allgemeine Informationen in ihren Datenschutzhinweisen z.B. gegenüber Mitarbeitern und Kunden vor, die bereits den Fall künftiger M&A Transaktionen beinhalten. Dies kann den Anforderungen der Transparenz der DSGVO genügen, wenn die Informationen des Art. 13 Abs. 1 und 2 DSGVO vollständig enthalten sind. Es wird allerdings auch vertreten, dass solche „Blanko"-Informationen nicht den Anforderungen an die Transparenz unter der DSGVO genügen können.[2] Die Diskussion zeigt, dass eine Bewertung im Einzelfall erfolgen sollte und davon abhängt, ob die erforderlichen Informationen vollständig enthalten und transparent dargestellt sind.

Entscheidet sich ein Unternehmen (aus welchen Gründen auch immer) dagegen, die Informationspflichten zu erfüllen und das Risiko eines Verstoßes der DSGVO in Kauf zu nehmen, sollte das Unternehmen die Vorgehensweise und die Gründe umfassend dokumentieren. Hier wird die Zukunft zeigen, inwiefern und in welchem Umfang Aufsichtsbehörden oder Gerichte ein solches Vorgehen sanktionieren. 12

II. Datenraum

In einem nächsten Schritt ist der Datenraumanbieter zu wählen und der Datenraum zu befüllen.

1. Auftragsverarbeitungsverträge

Der Anbieter eines Datenraums wird regelmäßig als Auftragsverarbeiter i.S.d. DSGVO zu qualifizieren sein. Das heißt, der Verkäufer hat einen Auftragsverarbeitungsvertrag im 13

[2] Vgl. *Maschmann*; BB 2019, 628, 634.

Einklang mit Art. 28 DSGVO mit dem Anbieter des Datenraums zu schließen. Üblicherweise wird der Anbieter eines Datenraums einen Standardauftragsverarbeitungsvertrag zur Verfügung stellen. Da der Verhandlungsspielraum in Bezug auf den Standardauftragsverarbeitungsvertrag häufig gering ist, empfiehlt es sich bereits bei der Auswahl des Anbieters den Standardauftragsverarbeitungsvertrag zu prüfen. Insbesondere ist in diesem Zuge auch eine Prüfung bezüglich der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO des Anbieters zu empfehlen.

2. Datenraum außerhalb der EU/EWR

Falls sich der Datenraum außerhalb der Europäischen Union / des Europäischen Wirtschaftsraums (EWR) befindet, bzw. die Daten außerhalb des EWR gespeichert werden sollen, gelten zusätzlich die Anforderungen an internationale Übermittlungen von personenbezogenen Daten (Art. 44 ff. DSGVO). 14

a) Angemessenheitsbeschluss

15

Eine Übermittlung an ein Drittland ist dann unproblematisch, wenn für das Drittland ein Angemessenheitsbeschluss der EU Kommission (wie z.B. für Japan, die Schweiz oder Neuseeland) vorliegt.[3] Neben territorialen Angemessenheitsbeschlüssen können auch sektorspezifische Angemessenheitsbeschlüsse (z.B. Beschluss der EU Kommission bzgl. des EU-U.S. Privacy Shield Abkommens („Privacy Shield")) gefasst werden. Im Fall einer (geplanten) Datenspeicherung in den USA kann jedoch nicht mehr auf das Privacy Shield zurückgegriffen werden, da der Gerichtshof der Europäischen Union („EuGH") am 16. Juli 2020 das Privacy Shield für unwirksam erklärt hat.[4]

b) Geeignete Garantien

Liegt für das jeweilige Drittland kein Angemessenheitsbeschluss vor, müssen (1) „geeignete Garantien" vorgesehen werden und (2) den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (Art. 45 Abs. 1 DSGVO). 16

[3] Vgl. Europäische Kommission, Website, abrufbar unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[4] EuGH, Übermittlung personenbezogener Daten von Facebook Ireland in die USA – Schrems II, NJW 2020, 2613.

Für Anbieter von Datenräumen kommen insbesondere Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern[5] als geeignete Garantien in Betracht. Wenngleich die Kritik am Privacy Shield auch in Bezug auf die Standarddatenschutzklauseln geübt wurde, hat der EuGH im Grundsatz entschieden, dass die Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern wirksam sind.[6] Allerdings können diese nicht mehr bedingungslos verwendet werden. 17

Der EuGH kam zu dem Ergebnis, dass das U.S.-Recht wegen der behördlichen Zugriffsrechte nicht ein der Sache nach gleichwertiges Datenschutzniveau gewährt.[7] Laut dem Europäischen Datenschutzausschuss („EDSA") sind Übermittlungen an einen U.S.-Datenimporteur auf der Grundlage von Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern im Einzelfall an Hand der Umstände der Übermittlung und mit Blick auf mögliche „zusätzlich zu treffende Maßnahmen" zu beurteilen.[8] Leider ist bisher unklar, in welchen (Regel-)Fällen ein Aussetzen der Übermittlung erwartet wird. Insbesondere können die Ausnahmen des Art. 49 DSGVO nicht herangezogen werden, da diese nur in bestimmten Einzelfällen anwendbar sind. 18

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder („DSK") äußerte, dass Standarddatenschutzklauseln bei Datenübermittlungen in die USA ohne zusätzliche Maßnahmen grundsätzlich nicht mehr ausreichend sein sollen.[9] Der EDSA analysierte diese Frage und stellte am 10. November 2020 weitere Leitlinien zur Verfügung .[10] Diese verweisen auf eine Einzelfallprüfung und den Einsatz von vertaglichen, technischen oder organisatorischen zusätzlichen Maßnahmen.[11] Insbesondere deutsche Aufsichtsbehörden kündigen diesbezüglich einen „strengen" Umgang an.[12] 19

[5] Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (K(2010) 593).
[6] EuGH, NJW 2020, 2613.
[7] EuGH, NJW 2020, 2613.
[8] EDSA, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und MaximillianSchrems, S. 3, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_de.pdf.
[9] DSK, Pressemitteilung, 28.07.2020, abrufbar unter https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf.
[10] EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, abrufbar unter https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.
[11] EDSA, Fn. 10, Rn. 46 und 47.
[12] Vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung, 17.07.2020, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf; Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung, 16.07.2020, abrufbar unter https://datenschutz-hamburg.de/pressemitteilungen/2020/07/2020-07-16-eugh-schrems.

Sofern möglich, können (und sollten) daher Datenraumanbieter innerhalb des EWR gewählt werden. 20

III. Offenlegung der Daten gegenüber potentiellen Erwerbern

Sobald der Datenraum befüllt ist, beginnt normalerweise die Due Diligence durch die Erwerberseite. Das heißt, es erfolgt eine Offenlegung der Dokumente gegenüber dem oder den potentiellen Erwerber(n).

1. Rechtsgrundlage

Die Rechtsgrundlage für die Offenlegung von personenbezogenen Daten in einer Due Diligence ist regelmäßig das überwiegende Interesse des Verkäufers und/oder der Zielgesellschaft gegenüber den Interessen der betroffenen Personen, die ihre personenbezogenen Daten Dritten gegenüber nicht offengelegt haben wollen. Die Offenlegung muss erforderlich sein. Als milderes Mittel ist bei einer Due Diligence grundsätzlich an die Anonymisierung der Dokumente zu denken. Dies kann beispielsweise durch Schwärzung erreicht werden, sofern technisch sichergestellt ist, dass die personenbezogenen Daten nicht wiederhergestellt oder anderweitig erkannt werden können. 21

Typischerweise sollten mitarbeiterbezogene Dokumente (z.B. Arbeitsverträge, Leistungsbeurteilungen) immer geschwärzt werden. Ausnahmsweise kann eine andere Beurteilung bezüglich sogenannter Schlüsselmitarbeiter (Key Employees) erfolgen, wenn die Kenntnis der personenbezogenen Daten hier wesentlich zur Kaufentscheidung beitragen würde. Solche Ausnahmen sollten jedoch restriktiv angewandt werden. Alle anderen geschäftsbezogenen Dokumente, z.B. Verträge, sollten - so weit möglich - geschwärzt werden. 22

Alternativ können mitarbeiterbezogene Informationen auch in aggregierter Form zur Verfügung gestellt werden. Das bedeutet, dass die Informationen statistisch aufbereitet werden, ohne Rückschlüsse auf einzelne Mitarbeiter zuzulassen. Dies kann beispielsweise so erfolgen, dass die Anzahl der Mitarbeiter in den einzelnen Bereichen, die Gehaltskorridore, die Altersgruppen, etc., und in Zahlen ausgedrückt werden. Hierbei ist zu beachten, dass auch durch die Kombination verschiedener Informationen ein Rückschluss möglich sein kann. Deshalb sollte die Aufbereitung in aggregierter Form unter Einbeziehung eines Datenschutzexperten erfolgen. 23

2. Offenlegung an potentiellen Erwerber außerhalb des EWR

Sitzt der potentielle Erwerber in einem Land außerhalb des EWR, gelten zusätzlich die vorstehend ausgeführten Anforderungen an internationale Übermittlungen von personenbezogenen Daten (Art. 44 ff. DSGVO).[13] In diesem Fall werden regelmäßig Standarddatenschutzklauseln (Controller to Controller) zum Einsatz kommen. Auch diesbezüglich ist davon auszugehen, dass die Ausführungen des EuGH entsprechend gelten. Damit sind „zusätzlich zu treffende Maßnahmen" zu erwägen. Auch hier können die Ausnahmen des Art. 49 DSGVO nicht herangezogen werden, da diese nur in bestimmten Einzelfällen anwendbar sind. 24

3. Informationspflichten

Auch in diesem Verarbeitungsschritt verlangt die DSGVO eine frühzeitige Information der betroffenen Personen, sofern keine vollständige Anonymisierung der personenbezogenen Daten erfolgt. Dies können Mitarbeiter, Kunden und Lieferanten der Zielgesellschaft sein. Hierbei gelten die vorstehenden Ausführungen.[14] 25

Im Rahmen der Offenlegung der personenbezogenen Daten gegenüber dem potentiellen Erwerber unterliegt auch dieser einer Informationspflicht gegenüber Mitarbeitern, Kunden und Lieferanten der Zielgesellschaft (Art. 14 Abs. 4 DSGVO). Dies betrifft insbesondere die Informationen zum konkreten potentiellen Erwerber, welche personenbezogenen Daten und zu welchem Zweck gegenüber dem potentiellen Erwerber offengelegt werden und woher die personenbezogenen Daten stammen. Wie bereits angesprochen, kommt in diesem Fall eine Ausnahme in Betracht, wonach die Informationspflicht nicht besteht, wenn sich die Erteilung der Informationen als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde (Art. 14 Abs. 5 lit. b DSGVO). Die Rechtsprechung legte in der Vergangenheit strenge Maßstäbe an, was die Unverhältnismäßigkeit bei Transparenzrechten angeht.[15] Aus diesem Grund kann hier nur im Einzelfall die Abwägung zugunsten des potentiellen Erwerbers ausgehen, beziehungsweise ein risikobasierter Ansatz gewählt werden. Beispielsweise kann eine Komplettschwärzung der personenbezogenen Daten in Bezug auf umfangreiche geschäftsbezogene Dokumente im Einzelfall aufgrund der Fülle der Dokumente als unverhältnismäßig angesehen werden, wenngleich dies von einer Aufsichtsbehörde nicht unbedingt so gesehen werden muss. Die Abwägung ist umfassend zu dokumentieren. In Bezug auf Mitarbeiterdaten empfiehlt sich eine eher vorsichtige Bewertung, das heißt die Offenlegung in aggregierter oder geschwärzter Form ist vorzugswürdig. Bei anonymisierten Daten bestehen auch keine Informationspflichten. 26

[13] Siehe vorstehend III.2.
[14] Siehe vorstehend unter I.3.
[15] LG Kiel, Urt. v. 4.4.2008 – 8 O 50/07.

IV. Ausblick

Zusammenfassend lässt sich sagen, dass Fragen des Datenschutzrechts eine immer größere Rolle im Rahmen von M&A Transaktionen spielen – Tendenz steigend. Dies liegt nicht nur an den drohenden Geldbußen, sondern auch daran, dass Bewertungsfragen bezüglich des Kaufpreises einer Zielgesellschaft, sowie Reputationsschäden auf Verkäufer- und Erwerberseite, eine Rolle spielen können. 27

Die wirtschaftlichen Auswirkungen - insbesondere in der Vorbereitungsphase einer Due Diligence - sind für die Parteien einer Transaktion nicht zu vernachlässigen. Es empfiehlt sich daher frühzeitig Datenschutzrechtsexperten in die Planung und Strukturierung einer M&A Transaktion zu involvieren. 28