PSP
MÜNCHEN

White Paper

M&A und Datenschutz

Kann das gutgehen?

Autor: Dr. Axel-Michael Wagner

Version 2.0
[Juli 2019]

ZUSAMMENFASSUNG

Das White Paper widmet sich der Frage, welche Daten, die im Rahmen von Unternehmenstransaktionen (M&A) eine Rolle spielen, von der DSGVO betroffen sein könnten, und erklärt, welchen datenschutzrechtlichen Vorgaben bei M&A-Projekten Beachtung geschenkt werden sollte. Dabei geht es inhaltlich um zwei Aspekte. Zum einen behandelt das White Paper personenbezogene Daten bei M&A-Projekten, die im Rahmen der Unternehmenstransaktion selbst verarbeitet werden. Zum anderen wird aufgezeigt, welche datenschutzbezogenen Risiken in Bezug auf die Zielgesellschaft bestehen und mit welchen Gestaltungsmöglichkeiten der Käufer diese Risiken reduzieren kann.

Inhalt

Einleitung

Die pragmatische Antwort auf die Frage, welche Daten, die in einem M&A-Prozess eine Rolle spielen, dem Datenschutzrecht unterliegen können, lautet: Potenziell alle. Aber keine Sorge: Das ist nichts Neues. Es hat nur in der M&A-Praxis bislang kaum jemanden interessiert. Wenn im Rahmen von M&A-Transaktionen bisher an „Datenschutz" (oder doch eher nur an die Verhinderung von Abwerbeversuchen?) gedacht wurde, dann am ehesten noch in Verbindung mit einer Due Diligence-Prüfung bei der Anonymisierung oder Schwärzung der Mitarbeiterliste des Zielunternehmens. Die EU-Datenschutzgrundverordnung (DSGVO) mit ihren drakonischen Strafandrohungen zeigt aber, dass es sich lohnt, einen genaueren Blick darauf zu werfen, womit man sich datenschutzrechtlich im Zuge einer M&A-Transaktion beschäftigen sollte. Die Zeiten der grauen Theorie sind vorbei. Die englische Datenaufsichtsbehörde ICO belegte die Hotelkette Marriott im Juli 2019 mit einem Bußgeld in Höhe von knapp 100 Mio. Pfund, weil diese beim Erwerb der Hotelkette „Starwood" eine unzulängliche Datenschutz Due-Diligence-Prüfung durchgeführt hatte und dadurch 339 Millionen Datensätze über Hotelgäste abhandenkommen konnten. Und die deutsche Datenschutzkonferenz hat in einem Beschluss vom 24. Mai 2019 das Thema Asset Deal genauer unter die Lupe genommen und hier „aus dem Nichts heraus" einige Regeln aufgestellt.

An der Schnittstelle zwischen DSGVO und M&A geht es inhaltlich im Wesentlichen um zwei Aspekte. Der erste Aspekt betrifft die Frage, welche personenbezogenen Daten im Rahmen eines typischen M&A-Projekts generiert werden und wie sie „zirkulieren". Dies schließt die Fragestellung ein, in welcher datenschutzrechtlichen Funktion welche Beteiligten tätig werden und welche datenschutzrechtliche Grundlage für ihre Verarbeitungstätigkeiten jeweils besteht. Schließlich geht es in diesem Bereich darum, wie Daten geschützt werden müssen, damit sie DSGVO-konform verarbeitet werden.

Der zweite Aspekt hingegen betrifft die Frage, welche datenschutzbezogenen Risiken sich der Käufer durch den Erwerb „aufhalsen" kann und wie hiermit im Unternehmenskaufvertrag umgegangen werden kann.

Der M&A-Prozess

M&A im Sinne dieses White Papers geht vom Grundfall eines „100%-Kaufes“ – Share Deal oder Asset Deal – aus. Andere Transaktionsstrukturen wie Transaktionen unter Beteiligung des Managements, Minderheits- und atypische Beteiligungen sowie umwandlungsrechtliche Maßnahmen werden hier überwiegend ausgeklammert. Die datenschutzrechtlichen Probleme verändern sich dadurch aber nur in Randbereichen.

Der M&A-Prozess gliedert sich grob – bis zum Closing – in:

- eine Vorverhandlungsphase, die typischerweise mit einem Letter of Intent endet,
- eine Due Diligence- und Verhandlungsphase, die typischerweise mit einem Vertragsabschluss (Signing) endet, und
- eine Interims-Phase zwischen Signing und Closing, die typischerweise mit dem Vollzug (Closing) endet.

Die Phase nach dem Closing umfasst sowohl die „Post-Merger-Integration“-Phase, die üblicherweise zwischen Käufer und Zielgesellschaft stattfindet, sowie etwaige Streitigkeiten über unternehmensbezogene Garantien etc. („Post-Closing-Disputes“). Diese weiteren Elemente werden hier ausgeklammert.

Ebenso werden hier wettbewerbs- und kartellrechtliche Aspekte nicht behandelt, die im Einzelfall z. B. eine Schwärzung von (auch Unternehmens-)Namen notwendig machen können.

Welche personenbezogenen Daten werden verarbeitet?

Aus datenschutzrechtlicher Sicht geht es zunächst einmal um die Frage, welche Daten (bzw. Datenkategorien) welcher Betroffenen im Zuge einer M&A-Transaktion irgendwie „verarbeitet" werden. Dabei spielt es keine Rolle, ob die Daten öffentlich zugänglich sind oder nicht. Nachfolgend wird unterstellt, dass es sich bei Verkäufer, Käufer und Beratungshaus nicht um natürliche Personen, sondern um Organisationen (insbesondere Gesellschaften) handelt, die jeweils durch Repräsentanten (Mitarbeiter) handeln. Die verarbeiteten Datenkategorien und Betroffenen sind im Wesentlichen Folgende:

- **Beschäftigtendaten der Mitarbeiter des Verkäufers**, **des Käufers und der Beratungshäuser**, die an der Transaktion teilnehmen. Bisweilen gibt es sogar eine förmliche „All Party's List" mit Kontaktdaten sämtlicher Beteiligter. In erster Linie sind dies die unternehmensbezogenen Kontaktdaten, möglicherweise aber auch deren Lebensläufe/Qualifikationen/(Unternehmens-)Präsentationen sowie private Telefonnummern. Hierzu zählen auch sämtliche Arbeitsergebnisse mit Personenbezug, also namentlich gekennzeichnete (bzw. auf einen bestimmten Autor zurückverfolgbare) Berichte, Bewertungen, Notizen, Korrespondenz etc.. Aber auch Bewegungsdaten innerhalb eines Datenraums (angesehene Dokumente, Verweildauer, gestellte Fragen etc.) sind personenbezogene Datenspuren, welche die Beschäftigten „hinterlassen".

- **Beschäftigtendaten der Mitarbeiter der Zielgesellschaft**, die im Rahmen der **Due Diligence-Prüfung** als **Ansprechpartner** fungieren (z. B. Leiter Rechnungswesen, Umweltbeauftragter, Leiter der Patentabteilung etc.) sowie ggf. von deren Beratungshäusern, die im Zuge der Due Diligence-Prüfung Auskünfte erteilen (Jahresabschlussprüfer, Rechtsanwalt etc.). In erster Linie sind dies die unternehmensbezogenen Kontaktdaten dieser Beschäftigten, aber auch Arbeitsergebnisse mit Personenbezug.

- **Beschäftigtendaten der Mitarbeiter** (einschließlich der Geschäftsführung) **der Zielgesellschaft** als „**Prüfungsobjekte**" der **Due Diligence-Prüfung**. Dies können Arbeitsverträge, Daten zu Lohn, Steuern und Sozialversicherungsbeiträgen, Betriebszugehörigkeit, Qualifikationen, Schwerbehinderteneigenschaft, Teilzeit, Geburtstag/Alter, Leasing-Fahrzeug-Daten, Fehlzeiten etc. sein. Hierzu zählen jedoch auch – soweit sie im Rahmen der M&A-Transaktion untersucht werden – die von den Beschäftigten hinterlassenen „Datenspuren" bei der Zielgesellschaft, also gesendete E-Mails, Überwachungsdaten, Protokolldaten (Maschinennutzung, Zeitstempel, Schließsysteme etc.), verfasste Schriftstücke (auch etwa Patentschriften und Quellcode von Software) und

Anmerkungen/Aktenvermerke etc., d. h. letztlich jegliche Information im Unternehmen, die einem bestimmten Mitarbeiter persönlich zugeordnet werden kann.

- **Beschäftigtendaten der Mitarbeiter von Geschäftspartnern** und **laufenden Behördenkontakten der Zielgesellschaft**, insbesondere also von Lieferanten/Dienstleistern, Kunden/Abnehmern und zuständigen Behörden. In erster Linie sind dies die unternehmensbezogenen Kontaktdaten dieser Beschäftigten von Dritten sowie die Korrespondenz mit diesen. Vertreibt die Zielgesellschaft Waren oder Dienstleistungen an natürliche Personen, sind die Daten der Kunden selbst (einschließlich der Korrespondenz mit den Kunden), nicht nur die Daten der Beschäftigten der Kunden, Gegenstand der Betrachtung. Die in diesem Fall über den Kunden verarbeiteten Datenkategorien sind vom Geschäftsmodell des Zielunternehmens abhängig; typischerweise werden dies zumindest Name, Adresse, ggf. auch Geburtsdatum, IP-Adresse(n), Kreditkartendaten etc. sein. In diese Kategorie fallen aber z. B. auch die Patientendaten bei einem Praxis- oder Klinikverkauf. An das hierzu mangels pragmatischer Vorgaben aus Gesetzgebung und Rechtsprechung entwickelte „Zwei-Schrank-Modell", bei dem der Käufer bei der Suche nach Namen bestimmter Alt-Patienten im „Verkäuferschrank" auch mit den Namen anderer Alt-Patienten in Berührung kommt, soll hier aber nicht vertieft eingegangen werden.

- **Interessenten** und **sonstige Marketing- bzw. Akquisitions-Kontakte der Zielgesellschaft** oder, soweit es sich um Unternehmen, Behörden oder sonstige Institutionen handelt, die Beschäftigtendaten der Mitarbeiter dieser Institutionen (einschließlich im Bereich der Unternehmens-Verbände und im sozialen Bereich – wie gesponserte Vereine – oder im politischen Bereich). Dies betrifft die Daten von Kontakten, mit denen keine laufende Geschäfts- oder gesetzliche Beziehung besteht, aber die aus anderen Gründen für die Zielgesellschaft „relevant" bzw. „interessant" sind.

- **Inhaberbezogene Daten der Zielgesellschaft**. Immer dann, wenn der Name (Firma) der Zielgesellschaft natürliche Personen – etwa Familiengesellschafter – „bestimmt", sind unternehmensbezogene Daten – wie Umsatz und Gewinn der Zielgesellschaft zugleich personenbezogene Daten des Gesellschafters.

Dabei ist auch zu beachten, dass die DSGVO (nur) auf solche Daten keine Anwendung findet, die nicht in einem (analogen oder digitalen) „Dateisystem" gespeichert werden bzw. werden sollen. Dies wirft Abgrenzungsfragen z. B. in Bezug auf mündliche Besprechungen auf. Werden hier personenbezogene Daten mitgeteilt, die später als Notiz in

einer strukturierten Papierakte oder digital (Scan/Eingabe der Information in ein Dokument oder als E-Mail) erfasst werden sollen, so fallen auch diese Daten unter die DSGVO. Als Faustregel kann daher in „stark dokumentierten" Prozessen gelten, dass sämtliche Daten, sofern sie sich auf eine natürliche Person beziehen und einer natürlichen Person zugeordnet werden können, dem Datenschutzrecht unterliegen.

Man erkennt hieran, dass man umgekehrt die Frage stellen kann, welche transaktionsrelevanten Informationen **keine personenbezogenen Daten** sind. Dies betrifft folgende Informationen:

- **Rein unternehmensbezogene und nicht inhaberbezogene Daten der Zielgesellschaft** (oder der sonstigen Beteiligten), die keinen Bezug zu individuellen Beschäftigten der Zielgesellschaft (bzw. der sonstigen Beteiligten) aufweisen. Dies sind für die Zielgesellschaft in der Regel aggregierte Bilanz- und GuV-Daten bis hinunter zur Sachkontenebene, aber auch allgemeine Informationen zu Standorten, Unternehmenspräsentationen, aggregierte Arbeitnehmerinformationen (Mitarbeiterzahlen, Personal-Gesamtkosten etc.), technische und produktbezogene Informationen, Arbeitsanweisungen und Prozessablaufbeschreibungen, soweit jeweils kein Personenbezug hergestellt werden kann.

- **Anonymisierte Informationen**, d. h. der Personenbezug wurde (vollständig) „getilgt", oder pseudonymisierte Informationen, d. h. die betroffene Person bzw. deren Identifizierungsmerkmale wurden durch ein Pseudonym ersetzt und die Partei, bei welcher die Daten verarbeitet werden, hat keine Zugriffsmöglichkeit auf die Zuordnungsinformationen.

Ausgeklammert werden im Rahmen dieses White Papers besondere Kategorien personenbezogener Daten, also *„Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person*".

Welchen Weg nehmen die Daten?

In einem nächsten Schritt sind die personenbezogenen Daten auf ihrem Weg von der Erhebung bis zur Löschung gedanklich zu „verfolgen“ („**Lebenszyklus“ der Daten**), um die jeweilige datenschutzrechtliche Berechtigungssituation (bzw. Pflichten in Bezug auf die Daten) ermitteln zu können. Dabei ergibt sich grob folgendes Muster:

- Personenbezogene Daten werden zunächst vom datenschutzrechtlich Verantwortlichen erhoben (und beim Erhebenden gespeichert). Überwiegend wird dies beim Betroffenen selbst geschehen, bisweilen aber auch ohne dessen Beisein, z. B. bei Internet-Recherchen. Wer also erfährt, welcher Rechtsanwalt den Käufer vertritt und diesen „googelt“, erhebt personenbezogene Daten über den Rechtsanwalt.

- Die Daten werden dann in vielen Fällen an andere Parteien weitergegeben. Solange keine Auftragsverarbeitung in Bezug auf die personenbezogenen Daten vorliegt, stellt diese Weitergabe datenschutzrechtlich eine „Übermittlung“ von einem Verantwortlichen an einen anderen Verantwortlichen dar. Sie werden gewöhnlich auch vom Übermittlungsempfänger gespeichert (die Dauer der Speicherung ist stets unerheblich).

- Beim Übermittlungsempfänger (evtl. auch schon und parallel beim Erhebenden) werden die Daten dann „verwendet“, d. h. in irgendeiner Form genutzt, etwa zur Kenntnis genommen und daraus Schlüsse gezogen. Derartige Schlussfolgerungen können ihrerseits personenbezogene Daten enthalten oder „anonym“ sein, indem sie abstrahiert oder aggregiert werden. Ein Due Diligence-Bericht, der einen Sachverhalt abstrakt beschreibt oder zusammengefasste Zahlen darstellt (Summe der Personalkosten etc.), enthält insoweit in der Regel keine personenbezogenen Daten. Ein Due Diligence-Bericht hingegen, der Personen namentlich benennt („Die Zielgesellschaft hat Klage erhoben gegen den Miterfinder, Herrn Weber“) oder so individuell beschreibt, dass die Person identifizierbar wird („Von den beiden Geschäftsführern beabsichtigt der Ältere, in den nächsten fünf Jahren in den Ruhestand zu treten.“), enthält seinerseits personenbezogene Daten. Die Gerichte und die Aufsichtsbehörden neigen dazu, eine Identifizierbarkeit von Personen eher anzunehmen als abzulehnen. Dies basiert auf den sehr „wachsweichen“ Formulierungen in den „gesetzesgleichen“ Erwägungsgründen der DSGVO, Kostprobe: *„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren [...]. Bei der Feststellung, ob Mittel nach allgemeinem*

Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.“

- Daten können sich demnach durch Übermittlung vervielfältigen (denn dann sind sie sowohl beim Übermittelnden als auch beim Übermittlungsempfänger). Sie können sich aber auch durch interne Weitergabe an andere Abteilungen bzw. Ablage an weiteren Speicherplätzen (dieselbe E-Mail befindet sich im Dokumenten-Management-System, im Smartphone, im Laptop und im PC) vervielfältigen. Dasselbe gilt, wie oben dargestellt, auch beim Generieren von „Derivaten“ der Ausgangsdaten (wie Äußerungen über die oder Erkenntnisse aus den Daten), soweit diese die ursprünglichen Daten enthalten bzw. die betroffene Person weiterhin identifizierbar bleibt. In diesen Fällen sind (auch) sämtliche Kopien und Derivate der ursprünglichen Daten gedanklich weiterzuverfolgen.

- Die erhobenen, übermittelten und verwendeten personenbezogenen Daten, die sich im Laufe der Zeit auch beliebig vervielfältigt haben können, müssen dann bei Zweckerreichung (Closing) oder Zweckfortfall (Scheitern der Transaktion) gelöscht werden (unwiderruflich und inklusive sämtlicher Back-ups etc.). Intuitiv würde ein Verkäufer wohl dazu neigen, vor Löschung zumindest die Verjährungsfristen der unternehmensbezogenen Garantien (oder sonstige vertraglichen Nach-Fristen) abzuwarten, um sichergehen zu können, dass er noch über die gesamten transaktionsbezogenen Daten verfügt, wenn „etwas nachkommt“. Dies entspricht aber nicht der „reinen Lehre“ des Datenschutzrechts, wonach eine Löschpflicht nur dann nicht gegeben ist, weil die Daten noch „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen“ verarbeitet werden müssen, wenn eine Streitigkeit konkret bevorsteht. Über den Grad an Konkretheit wird gestritten. In der Praxis wirkt sich dieses Problem häufig – aber nicht immer – nicht aus, weil gesetzliche Aufbewahrungsfristen vorrangig einzuhalten sind. Das betrifft insbesondere steuerliche Aufbewahrungsfristen sowie die berufsrechtlichen Aufbewahrungspflichten für Handakten. Wer aber fein genug differenziert, wird personenbezogene Daten im Rahmen der Transaktion ausmachen können, für die keine Aufbewahrungspflichten einschlägig sind, sodass diese Daten unmittelbar nach Erschöpfung des zugrunde liegenden Zwecks gelöscht werden müssen.

Welche Daten werden von wem an wen übermittelt?

Die in der Praxis häufig bedeutsamste Frage ist, ob ein Verantwortlicher personenbezogene Daten an andere übermitteln darf. Die Übermittlung als Form der Verarbeitung ist aus datenschutzrechtlicher Perspektive deshalb besonders „gefährlich", weil die Daten damit die Sphäre des (ursprünglichen) Verantwortlichen verlassen. Es wird also für den Betroffenen schwieriger, „seinen Daten hinterherzulaufen", weil die „Laufwege" durch Übermittlungen und mögliche Weiterübermittlungen immer länger und unübersichtlicher werden. Die DSGVO sieht zwar hierfür in bestimmten Fällen die Pflicht vor, den Betroffenen oder andere Verantwortliche in der „Datenkette" zu benachrichtigen, doch selbst mit diesen „Instrumenten" wird es für den Betroffenen mit jeder Weiterübermittlung schwieriger, den Überblick und die Kontrolle über die ihn betreffenden Daten zu behalten.

Datenschutzrechtlich können folgende typische **Verarbeitungshandlungen in Form von Übermittlungen** (im Anschluss an die Ersterhebung der Daten) unterschieden werden, die im Rahmen einer M&A-Transaktion vorgenommen werden:

- Verkäufer und Käufer übermitteln sich gegenseitig die Kontaktdaten ihrer relevanten Mitarbeiter (Ansprechpartner) oder deren Korrespondenz/Arbeitsergebnisse/projekt- und personenbezogene Informationen, die sie zuvor von diesen Mitarbeitern erhoben haben.

  Beispiel: *Herr Huber als Vertreter der Müller Kapitalverkaufs GmbH (Beschäftigter des Verkäufers) versendet an Frau Bauer als Vertreterin der Schulze Kapitaleinkaufs GmbH (Beschäftigte des Käufers) eine E-Mail mit seinen Kontaktdaten, einem Link zu seinem persönlichen Profil und mit der Information, wann sein Flug von Berlin nach Frankfurt am Tag des telefonisch vereinbarten Termins landet.*

- Verkäufer und Käufer übermitteln sich gegenseitig die Kontaktdaten der Mitarbeiter ihrer Beratungshäuser, welche ihnen die Beratungshäuser zuvor jeweils übermittelt haben und welche die Beratungshäuser zuvor von diesen erhoben haben. Die Beratungshäuser übermitteln dem Verkäufer, dem Käufer und den anderen Beratungshäusern im Auftrag ihrer jeweiligen Kunden/Mandanten (Verkäufer und Käufer) Korrespondenz/Arbeitsergebnisse/projektbezogene persönliche Informationen, die sie zuvor bei ihren jeweiligen Mitarbeitern erhoben haben.

  Beispiel: *Frau Rechtsanwältin Krüger als Vertreterin der Maier Rechtsanwalts GmbH sendet für die Verkäuferseite einen Kaufvertragsentwurf an Frau Bauer als Vertreterin der Schulze Kapitaleinkaufs GmbH und teilt gleichzeitig die Kontaktdaten ihres Associate,*

Herrn Lehmann, mit. Der Kaufvertragsentwurf weist z. B. Frau Krüger als Zustellungsbevollmächtigte für Erklärungen im Zusammenhang mit dem Kaufvertrag aus. Alternativ wird der Entwurf mit begleitender Mitteilung in einen von der Maier Rechtsanwalts GmbH aufgesetzten Datenraum eingestellt, bei dem sich Frau Bauer mit Name, E-Mail-Adresse und per Einladung versendeter Zugangsdaten anmelden muss.

- Das Zielunternehmen übermittelt Verkäufer und Käufer sowie deren Beratungshäusern die Kontaktdaten seiner Mitarbeiter (Ansprechpartner) sowie von Mitarbeitern der von ihm eingesetzten Beratungshäuser, die im Zuge der Due Diligence Auskünfte erteilen.

  Beispiel: *Herr Schneider als Geschäftsführer der Schmidt GmbH, der Zielgesellschaft, teilt den Vertretern von Verkäufer, Käufer und Beratern die Kontaktdaten des Jahresabschlussprüfers der Schmidt GmbH sowie der Leiterin der Rechtsabteilung der Schmidt GmbH mit, letztere für den Fall, „dass es Fragen gibt zur Angelegenheit Weber, die wir in unserer Management Präsentation letzte Woche besprochen haben."*

- Das Zielunternehmen übermittelt personenbezogene Daten seiner Beschäftigten an Verkäufer und Käufer sowie deren Beratungshäuser. Dies ist üblicherweise Teil der arbeitsrechtlichen Due Diligence-Prüfung, aber solche Daten werden bisweilen auch (insbesondere als Anlagen) Teil des Unternehmenskaufvertrages (Share oder Asset Purchase Agreement – SPA/APA). Diese Übermittlung kann auch durch den Verkäufer bzw. dessen Berater, der diese Daten bereits zuvor von der Zielgesellschaft übermittelt erhalten hatte, an den Käufer bzw. dessen Berater stattfinden.

  Beispiel: *In den vom Verkäufer aufgesetzten elektronischen Datenraum stellt der Berater des Verkäufers eine Excel-Liste ein, in der sämtliche Mitarbeiter der Schmidt GmbH namentlich aufgelistet sind (mit Daten wie Geburtsdatum, Betriebszugehörigkeit, Abteilung, arbeitsrechtlicher Sonderstatus, vorgesehen für eine Kündigung im Rahmen einer Umstrukturierungsmaßnahme etc.) und die er zuvor von der Leiterin der Personalabteilung der Schmidt GmbH erhalten hatte. Die Liste wird später dem SPA beigefügt.*

- Das Zielunternehmen übermittelt personenbezogene Daten von Mitarbeitern Dritter (einschließlich Lieferanten/Kunden/Interessenten) sowie ggf. von sonstigen natürlichen Personen (Kunden/Marketing-Kontakte etc.) an Verkäufer und/oder Käufer sowie deren Beratungshäuser. Dies ist üblicherweise Teil der übrigen Due Diligence-Prüfung, aber auch solche Daten werden bisweilen Bestandteil des SPA/APA. Diese Übermittlung kann auch durch den Verkäufer bzw. dessen Berater, der diese Daten bereits zuvor von

der Zielgesellschaft übermittelt erhalten hatte, an den Käufer bzw. dessen Berater stattfinden.

Beispiel: *Auf Nachfrage des Käufers werden von einem Mitarbeiter der Schmidt GmbH in den elektronischen Datenraum Protokolle von Verhandlungen mit Lieferantenvertretern, die Kündigung eines Vertrages mit einem Kunden, der eine natürliche Person ist, ein Bewilligungsbescheid einer Behörde, die den zuständigen Behördenmitarbeiter ausweist sowie eine Korrespondenz mit einem Verbandsvertreter zu aktuellen lokalpolitischen Entwicklungen im Zusammenhang mit einer möglichen Erweiterungsfläche eingestellt.*

- Der Verkäufer oder das Zielunternehmen übermitteln inhaberbezogene Daten der Zielgesellschaft an den Käufer bzw. dessen Berater. Auch derartige Daten, insbesondere der Kaufpreis, sofern er ein inhaberbezogenes Datum darstellt, können Bestandteil des SPA/APA werden.

  Beispiel: *Herr Becker ist 100%-Kommanditist der nicht veröffentlichungspflichtigen Becker GmbH & Co. KG. Sein Wirtschaftsprüfer versendet die Bilanz/GuV der Becker GmbH & Co. KG sowie eine Kaufpreisindikation an den Repräsentanten des Käufers.*

- Daneben werden beim Vollzug eines Asset Deals personenbezogene Daten vom Verkäufer an den Käufer übermittelt. Die Daten dienen dann nicht mehr der Vertragsanbahnung (Verhandlungen, Due Diligence-Prüfung etc.), sondern sind selbst Teil des Vertragsobjekts des Asset Deals (Unternehmen bzw. Unternehmensteil). Dies betrifft sämtliche Datenkategorien, die oben als vom Zielunternehmen übermittelte Daten aufgeführt wurden. Beim Share Deal ist der Vollzug als solcher (Anteilsübergang) datenschutzrechtlich nicht relevant, weil die relevanten Daten beim Verantwortlichen (der Zielgesellschaft) verbleiben. Diesbezüglich ist jedoch darauf zu achten, dass der Käufer als neuer „aktueller" Gesellschafter unter Anwendung der zum EU-Kartellrecht entwickelten Haftungsgrundsätze ggf. für vergangene Datenschutzverstöße der Zielgesellschaft haftbar gemacht werden könnte. Unmittelbar datenschutzrechtlich relevant sind jedoch Übermittlungen personenbezogener Daten bei bzw. nach Vollzug eines Share Deals durch die Zielgesellschaft an den neuen Gesellschafter (Käufer).

  Beispiel (Asset Deal): *Frau Maier ist im Unternehmensbereich „Merchandising" bei der Huber AG angestellt. Die Huber AG veräußert diesen Unternehmensbereich an die Schulze GmbH und übermittelt sämtliche Personaldaten über Frau Maier an die Schulze GmbH. Zudem hatte die Huber AG u. a. einen Vertrag zur Lieferung von Merchandising-Artikeln mit Herrn Wolf abgeschlossen, dessen Erfüllung (durch Lieferung) erst nach der*

Unternehmensveräußerung ansteht. Die Huber AG übermittelt der Schulze GmbH die personenbezogenen Daten (Kundenstammdaten, Bestelldaten, Bestellhistorie etc.) von Herrn Wolf.

Man erkennt an den Beispielen schnell, dass die Grundidee des Datenschutzrechts, es gebe „ein (!) Datum eines (!) Betroffenen", das isoliert als solches der Verarbeitung unterliegt, grob vereinfachend ist (man kann nicht einmal sagen „aus der Zeit gefallen", weil es solche Idealzustände nie gab). Die Praxis operiert demgegenüber mit (willkürlichen) Informationsblöcken, sprich Dokumenten bzw. Dateien, und solche Blöcke können personenbezogene Daten verschiedenster Betroffener gleichermaßen und in unterschiedlicher Ausprägung bzw. Intensität enthalten. Und selbst wenn das Dokument ausdrücklich Namen enthält – der Name ist die deutlichste Form des „Identifiers" einer Person –, heißt das noch nicht, dass allein deren Schwärzung das Dokument datenschutzrechtlich „anonym" werden lässt. Denn es gibt noch jede Menge andere „Identifier", die nach erfolgter Schwärzung des Namens immer noch im Dokument enthalten sein und die Person identifizierbar machen könnten.

Praxistipp:

Verkäufer, Zielunternehmen und Kaufinteressent sollten sich frühzeitig bewusst machen, dass und welche personenbezogenen Daten über welche Betroffenen von wem an wen übermittelt werden. Dafür sollten „Klassen" bzw. „Kategorien" von Betroffenen, Daten und Übermittlungen gebildet werden. Diese „Awareness" ist der erste Schritt, um ein Datenschutz-Management-System für das Handling personenbezogener Daten im Rahmen einer M&A-Transaktion aufsetzen zu können. Dieses transaktionsspezifische Datenschutz-Management muss bei jedem Beteiligten integrierter Teil seines allgemeinen Datenschutz-Compliance-Management-Systems sein, dessen Implementierung der DSGVO-Gesetzgeber für jeden Verantwortlichen fordert.

Welches Verhältnis besteht zwischen den Verantwortlichen?

Im datenschutzrechtlichen Sinne sind die Beteiligten (Käufer, Verkäufer, Zielgesellschaft, Beratungshäuser) zunächst einmal „Verantwortliche". Dies bedeutet, dass sie jeweils eigenverantwortlich sicherzustellen haben, dass die von ihnen erhobenen, übermittelten oder empfangenen personenbezogenen Daten rechtmäßig verarbeitet wurden bzw. werden. Jeder Verantwortliche haftet auch für in der Übermittlungskette „vor" und „nach" ihm begangene Datenschutzverstöße, sofern er nicht alles in seiner Macht Stehende veranlasst, um die Rechtmäßigkeit der Verarbeitung sicherzustellen. Der übermittelnde Verantwortliche (beispielsweise der Verkäufer oder das Zielunternehmen im Rahmen einer Due Diligence-Prüfung) muss daher den Übermittlungsempfänger (Kaufinteressent) verpflichten, bestehende Restriktionen, insbesondere Zweckbindungen, in Bezug auf die übermittelten Daten zu beachten. Der Übermittlungsempfänger (Kaufinteressent) muss sicherstellen, dass die ihm (vom Verkäufer oder dem Zielunternehmen) übermittelten Daten rechtmäßig erhoben und übermittelt wurden. Wie weit diese Pflichten im Einzelnen gehen und wie vorzugehen ist (bzw. welche Haftung droht), wenn hier ein Verantwortlicher an die Grenzen seiner Verhandlungsmacht stößt – also derartige Regelungen von der anderen Seite nicht akzeptiert werden –, ist unklar. Es bietet sich jedenfalls an, die datenschutzrechtlichen Modalitäten etwa der Due Diligence-Prüfung bereits in einem LOI zwischen Verkäufer und Kaufinteressent zu regeln, so wie es früher bei physischen Datenräumen „Benutzungsregeln" gab.

Liegt darüber hinaus eine Stellung als „gemeinsam Verantwortliche" vor, müssten sie eine datenschutzrechtliche Innenvereinbarung zur Abgrenzung der Verantwortlichkeit zwischen ihnen treffen. Wann diese Situation vorliegt, ist aufgrund der unscharfen Abgrenzungskriterien in der Praxis nicht einfach zu bestimmen. In der Theorie ist dies dann der Fall, wenn die Verantwortlichen gemeinsam „die Zwecke der und die Mittel zur Verarbeitung" festlegen – eine Formel, deren Vorliegen in der Praxis oft schwierig zu bestimmen ist. Nach der Rechtsprechung sind Verantwortliche beispielsweise schon dann gemeinsam verantwortlich, wenn eine von einer Partei betriebene Plattform-Infrastruktur von einer anderen Partei derart mit Inhalten befüllt wird, dass sie Betroffene „anlockt", die dann dort personenbezogene Daten (ggf. als weitere Inhalte) hinterlassen, die von einer der Parteien „getrackt" bzw. „gescreent" werden. Es ist daher denkbar, dass bei einem gemeinsam vom Verkäufer und der Zielgesellschaft oder bei einem gemeinsam von einer Partei und ihrem Beratungshaus aufgesetzten bzw. betriebenen elektronischen Datenraum eine solche Stellung vorliegt. Dies bezieht sich auf die im Datenraum hinterlassenen Datenspuren der Datenraum-Benutzer, möglicherweise aber auch auf die eingestellten „Nutzdaten" der Zielgesellschaft: Wenn der

Verkäufer den Datenraum (ggf. über einen Dienstleister) „aufsetzt“ und die Zielgesellschaft personenbezogene Daten ihrer Beschäftigten „einstellt“, können beide „gemeinsam Verantwortliche“ gegenüber diesen Beschäftigten der Zielgesellschaft sein. Abgesehen von der Verpflichtung, eine entsprechende Innenvereinbarung abzuschließen (deren Fehlen von der DSGVO sanktioniert wird), sind die Folgen (bzw. die Privilegierung) dieser Stellung als „gemeinsam Verantwortliche“ sehr gering. Insbesondere bedarf – was für den nachfolgenden Abschnitt wichtig ist – jede Übermittlung von personenbezogenen Daten zwischen den „gemeinsam Verantwortlichen“ einer datenschutzrechtlichen Legitimation.

Beauftragen die Beteiligten Dritte mit Datenverarbeitungs-Dienstleistungen, etwa einen Datenraum-, Cloud- oder Rechenzentrums-Dienstleister, so liegt eine Auftragsverarbeitung dieses Dienstleisters für den betreffenden Beteiligten vor. Hier ist ein spezifischer Auftragsverarbeitungsvertrag mit gesetzlich vorgegebenen „Pflichtinhalten“ abzuschließen und der Auftragsverarbeiter laufend zu kontrollieren.

Praxistipp:

Beim „Aufsetzen“ der Due Diligence-Prüfung (Datenraum, Übermittlungsketten etc.) sollte frühzeitig geprüft und dokumentiert werden, wie das Verhältnis zu anderen Beteiligten datenschutzrechtlich einzustufen ist und welche Vereinbarungen zu den anderen Beteiligten ggf. notwendig sind. Dies können Auftragsverarbeitungsvereinbarungen, Innenvereinbarungen gemeinsam Verantwortlicher sowie Vereinbarungen „datenbezogener Garantien“ zwischen zwei eigenständig Verantwortlichen sein.

Datenschutzrechtliche Legitimationsgrundlage und Zweckänderung

Für sämtliche Verarbeitungsvorgänge – insbesondere natürlich Erhebungen, Übermittlungen, Verwendungen und Speicherungen –, die ein Verantwortlicher in Bezug auf personenbezogene Daten vornimmt, muss es eine datenschutzrechtliche Legitimationsgrundlage geben. Denn der oberste datenschutzrechtliche Grundsatz lautet: Was nicht ausdrücklich erlaubt ist, ist verboten. Dabei legitimiert die identifizierte Legitimationsgrundlage immer nur die Verarbeitung zum jeweils zugrunde gelegten und dem Betroffenen gegenüber auch transparent kommunizierten Zweck (Zweckbindung).

Zwar kann ein bestehender oder angebahnter Vertrag eine taugliche datenschutzrechtliche Legitimationsgrundlage darstellen, doch setzt dies voraus, dass der Betroffene – d. h. die natürliche Person – persönlich Partei dieses Vertrages bzw. vorvertraglichen Verhältnisses ist. Der Unternehmenskaufvertrag (und dessen vorherige Verhandlungsphase, zu der auch die Due Diligence-Prüfung zählt) kommt daher nicht als datenschutzrechtliche Legitimationsgrundlage in Betracht, weil er in der hier zugrunde gelegten Fallkonstellation nicht mit natürlichen Personen – schon gar nicht mit den Personen, deren personenbezogene Daten im Rahmen der Transaktion (zusätzlich) relevant sind – abgeschlossen wird.

In den oben umschriebenen Fallkonstellationen werden vielmehr im Wesentlichen Daten verwendet (insbesondere übermittelt), die ursprünglich in einem anderen Kontext – d. h. nicht für die konkret in Rede stehende Unternehmenstransaktion – erhoben wurden. In den wenigsten Fällen werden Beschäftigten-, Kunden-, Lieferanten- oder Marketingkontakt-Daten zum Zwecke der Durchführung einer bestimmten Unternehmenstransaktion originär erhoben. Diese Daten sind vielmehr schon „da“ und datenschutzrechtlich zunächst an den ursprünglichen Erhebungs-Zweck „gebunden“ (Zweckbindung). Mit anderen Worten: Die Daten wurden für den Zweck A (Beschäftigtenverhältnis, Lieferverhältnis, Direktmarketing etc.) auf Basis der Legitimationsgrundlage X erhoben und sollen nun davon abweichend für den Zweck B (Unternehmenstransaktion bzw. Due Diligence-Prüfung) auf Basis einer tauglichen Legitimationsgrundlage verarbeitet, insbesondere übermittelt werden. Datenschutzrechtlich stellt diese Verwendung von zum Zweck A erhobener Daten zum Zweck B (Unternehmenstransaktion bzw. Due Diligence-Prüfung) eine Zweckänderung dar, die im Grundsatz nur zulässig ist, wenn die Zwecke A und B zueinander „kompatibel“ sind. Auch wenn die Definition der „Kompatibilität“ von Zwecken in der DSGVO sehr wortreich ausgefallen ist, sind die Details höchst unklar.

Beispiel: *Nehmen wir an, Frau Maier ist leitende Angestellte der Huber AG. Die Aktien an der Huber AG sollen von der Müller Kapitalverkaufs GmbH an die Schulze Kapitaleinkaufs GmbH veräußert werden. Frau Maier – wie auch die übrigen Angestellten der Huber AG – sollen hiervon erst erfahren, wenn Signing oder Closing abgeschlossen wurden. Die Schulze Kapitaleinkaufs GmbH hat im Rahmen der Due Diligence-Prüfung großes Interesse am Anstellungsvertrag mit Frau Maier. Die Müller Kapitalverkaufs GmbH lässt sich diesen Anstellungsvertrag von der Huber AG geben und stellt diesen im Rahmen der Due Diligence-Prüfung in den Datenraum ein.*

Das Problem besteht in diesem Fall darin, dass der Zweck der ursprünglichen Erhebung der personenbezogenen Daten im Anstellungsvertrag (Name, Privatadresse, Gehalt etc.) durch die Huber AG die Durchführung bzw. Erfüllung des Anstellungsvertrages war. Dass dieser Vertrag später zwischen Dritten (der Müller Kapitalverkaufs GmbH und der Schulze Kapitaleinkaufs GmbH) übermittelt wird bzw. werden soll, war ursprünglich weder beabsichtigt noch Teil der Pflichthinweise, die Frau Maier durch die Huber AG bei (Erst-) Erhebung ihrer personenbezogenen Daten mitgeteilt wurden. Diese Pflichthinweise mussten neben der Festlegung des (Erhebungs-) Zwecks u. a. die Angabe umfassen, an welchen Empfänger (Dritten) der Verantwortliche (d. h. der die Daten Erhebende) die Daten weiterübermitteln möchte. Bei Frau Maier als Angestellter waren hier etwa Sozialversicherungsträger und Steuerbehörden anzugeben, was auch dem primären Zweck – der Erfüllung des Beschäftigungsverhältnisses – entspricht. Es ist unklar, ob die Aufnahme einer vorsorglichen Floskel „Übermittlung der personenbezogenen Daten für Due Diligence-Zwecke an einen möglichen Kaufinteressenten der Aktien an der Huber AG“ in die Pflichthinweise schon bei der ursprünglichen Erhebung der Daten datenschutzrechtlich zulässig wäre. Denn in aller Regel wird zum Zeitpunkt der Datenerhebung (Abschluss des Anstellungsvertrages) völlig unklar sein, ob, wann und an wen das Unternehmen jemals verkauft wird. Zudem bedürfte diese anfängliche Festlegung eines erweiterten Verarbeitungszwecks einer weiteren Legitimationsgrundlage in Form einer Interessenabwägung (dazu noch unten). Denn die Übermittlung von Beschäftigtendaten an einen Unternehmensinteressenten wäre nicht von der üblichen Legitimationsgrundlage für Beschäftigtendaten abgedeckt, wonach diese zur „Durchführung des Beschäftigungsverhältnisses“ verarbeitet werden dürfen. Ohne eine solche erweiternde Floskel entspricht schon die Übermittlung von der Huber AG an die Müller Kapitalverkaufs GmbH, mehr aber noch die Übermittlung von der Müller Kapitalverkaufs GmbH an die Schulze Kapitaleinkaufs GmbH nicht dem ursprünglichen Zweck. Ist aber nun der ursprüngliche Erhebungszweck mit dem späteren, geänderten Zweck „kompatibel“?

Hier ist zu differenzieren:

- Unproblematisch wird die Zweckkompatibilität im Bereich der unternehmensbezogenen Kontaktdaten der Repräsentanten der Verkäufer- und der Käuferseite sowie der eingesetzten Beratungshäuser sein, da die Vorbereitung, Verhandlung und Umsetzung von Unternehmenstransaktionen zu deren Funktionsträgereigenschaft bzw. Rollenbild innerhalb ihrer Organisation zählt.

- Beim Asset Deal kann im Grundsatz davon ausgegangen werden, dass der eigentlich hinter der Transaktion stehende Zweck der Fortführung des Geschäftsbetriebs als relevante (neue) Zweckbestimmung mit dem ursprünglichen Erhebungszweck kompatibel ist. Die Frage aber, ob diese Kompatibilität auch die Übermittlung einer großen Menge personenbezogener Daten im Rahmen der Due Diligence-Phase eines Asset Deals rechtfertigt („Massenübertragung"), ist noch ungeklärt. Auch die Datenschutzkonferenz äußert sich in ihrem „Asset Deal-Beschluss" vom 24. Mai 2019 nicht zu dieser Frage. Eine Due Diligence-Prüfung (als Vorab-Unternehmensprüfung, möglicherweise durch mehrere Erwerbsinteressenten) und der Asset Deal selbst (als Unternehmensübernahme durch einen Erwerber auf Basis eines abgeschlossenen Unternehmenskaufvertrages) könnten zwei unterschiedliche (Folge-) Zwecke darstellen. Die Due Diligence-Prüfung würde dann nur insoweit einen kompatiblen Zweck darstellen, als für die Bewertung der Transaktion unerlässliche „Schlüsseldaten" übermittelt werden sollen, während nur der Asset Deal selbst einen für die Übertragung sämtlicher personenbezogener Daten kompatiblen Zweck konstituiert.

- Für die Due Diligence-Phase von Share Deals ist die Zweckkompatibilität schon im Grundsatz eher zweifelhaft. Denn ein Share Deal und damit auch die ihn vorbereitende Due Diligence-Prüfung vollzieht sich außerhalb der „Sphäre" der Zielgesellschaft selbst bzw. von deren Geschäftsbetrieb. Der Share Deal ist mit anderen Worten (wesentlich) weniger mit der Führung bzw. Fortführung des Geschäftsbetriebs der Zielgesellschaft verknüpft als der Asset Deal. Es kann daher zur datenschutzrechtlichen Zulässigkeit der Verarbeitung personenbezogener Daten aus der Sphäre der Zielgesellschaft im Rahmen der Due Diligence-Prüfung vor einem Share Deal notwendig sein, gesonderte datenschutzrechtliche Legitimationsgrundlagen zu identifizieren, die eine Verarbeitung unabhängig vom ursprünglichen Erhebungszweck und der ursprünglichen Legitimationsgrundlage rechtfertigen.

Die Zweckänderungsmitteilung

Unabhängig von der Frage der Zweckkompatibilität muss der Betroffene bei jeder Zweckänderung vorab über diese informiert werden. Die Huber AG wäre also verpflichtet, vor der Übermittlung des Anstellungsvertrages an die Müller Kapitalverkaufs GmbH Frau Maier mitzuteilen, welche ihrer personenbezogenen Daten zu welchem neuen Zweck verarbeitet und in diesem Rahmen an welche Empfänger weitergeleitet werden sollen. Die Vorgaben für die bei Erhebung mitzuteilenden Pflichthinweise – z. B. der/die Empfänger künftiger Übermittlungen – gelten auch für die „Zweckänderungsmitteilung". Wenn zum Zeitpunkt der Zweckänderung der Kaufinteressent schon namentlich bekannt ist, stellt sich die Frage, ob nur die Übermittlung „an einen möglichen Kaufinteressenten der Aktien an der Huber AG" als Empfänger angekündigt werden darf oder ob der konkrete Kaufinteressent (bzw. dessen Beratungshäuser) als Empfänger genannt werden muss. Im Sinne der Transparenz ist eigentlich von einer Offenlegung des konkret bekannten Empfängers auszugehen. Daneben macht die Zweckänderungsmitteilung die (Weiter-) Übermittlung von personenbezogenen Daten an (viele) andere Parteien natürlich zu einer administrativen Herausforderung.

War die Legitimationsgrundlage im Rahmen des ursprünglichen Zwecks ein Vertrag mit dem Betroffenen – hier das Beschäftigungsverhältnis zwischen der Huber AG und Frau Maier –, dann besteht kein Recht des Betroffenen auf Widerruf oder Widerspruch in Bezug auf die (Weiter-) Verarbeitung zum neuen Zweck. Dies gilt (paradoxerweise) auch für den geänderten Zweck, d. h. Frau Maier kann, wenn sie von der Zweckänderung benachrichtigt wird – sodass sie dann natürlich auch von der angedachten Unternehmenstransaktion erfährt, in welchem Konkretisierungsgrad auch immer –, der weiteren Verarbeitung (inkl. Übermittlung) nicht widersprechen. Auch dieser Umstand – aus der Perspektive des Betroffenen wird ihm ein neuer Zweck „aufoktroyiert" – dürfte dazu führen, dass die Zweckkompatibilität von einem Gericht oder einer Aufsichtsbehörde sehr kritisch untersucht werden wird.

Die Schwärzung des Namens oder des Gehaltes von Frau Maier würde übrigens, worauf oben schon hingewiesen wurde, datenschutzrechtlich nichts ändern, wenn man Frau Maier auch aus anderen Informationen aus dem Vertrag bzw. „aus den übrigen Umständen" heraus identifizieren könnte. Insbesondere gilt dies natürlich dann, wenn mündlich angekündigt wurde, dass der Vertrag von Frau Maier „nur geschwärzt" in den Datenraum eingestellt wird. Datenschutzrecht ist nicht Geheimnisschutz, sondern betrifft den Schutz (sämtlicher) personenbezogener Daten. Personenbezogene Daten müssen demnach ihren Personenbezug vollständig verlieren, um als anonyme Daten nicht mehr dem Datenschutzrecht zu unterliegen.

Ein weiterer Beispielsfall betrifft eine andere Legitimationsgrundlage sowie Daten, die schon das Zielunternehmen seinerseits übermittelt erhielt.

Beispiel: *Eine Tochtergesellschaft der Huber AG, die Hofmann GmbH, führt einen bedeutenden patentrechtlichen Rechtsstreit gegen einen Erfinder, Herrn Krause. Die Unterlagen zu diesem Rechtsstreit hatte die Hofmann GmbH der Konzernrechtsabteilung Huber AG übermittelt, damit diese den Sachverhalt prüft und das Klageverfahren begleitet. In diesem Fall war die ursprüngliche datenschutzrechtliche Legitimationsgrundlage eine Interessenabwägung. Vor der ursprünglichen Weitergabe der Daten an die Huber AG hatte die Hofmann GmbH Herrn Krause bereits eine Zweckänderungsmitteilung zukommen lassen. Auf diese hatte Herr Krause wütend reagiert, zumal er über einen befreundeten Mitarbeiter der Hofmann GmbH erfahren hatte, dass die Daten zum Rechtsstreit mit ihm in einen Datenraum der Konzernrechtsabteilung der Huber AG eingestellt wurden, auf den auch sämtliche anderen Tochterunternehmen der Huber AG Zugriff haben; er hatte seinerzeit der weiteren Verarbeitung (insbesondere der Übermittlung an die Huber AG) widersprochen und nimmt seitdem die Huber AG gerichtlich auf Löschung der übermittelten Daten in Anspruch.*

Ist nämlich eine Interessenabwägung Legitimationsgrundlage der Verarbeitung, so steht dem Betroffenen ein Widerspruchsrecht gegenüber dem Verantwortlichen zu; trotz Widerspruchs darf dann eine weitere Verarbeitung nur noch erfolgen, wenn der Verantwortliche „*zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen*“. Herr Krause ist der Meinung, dass die letztgenannte Ausnahme nicht für die Huber AG, sondern ausschließlich für die Hofmann GmbH gelten kann. Die Huber AG geht davon aus, dass jeder Unternehmenskäufer die Unterlagen zum Rechtsstreit mit Herrn Krause im Detail studieren wollen wird, zumal die Angelegenheit bereits öffentlich „breitgetreten“ wurde. Eine erneute Zweckänderungsmitteilung an Herrn Krause soll unbedingt vermieden werden, denn sie birgt nicht nur die Gefahr eines sofortigen Widerspruchs, sondern auch, dass dann der Unternehmensverkäufer und der Kaufinteressent in den laufenden Streit mit hineingezogen werden. Hier wird es auch schwer bis unmöglich, die Daten tatsächlich zu anonymisieren, da für jeden Kaufinteressenten die „Zuordnung“ zu Herrn Krause evident ist und damit Herr Krause als Betroffener (natürlich) identifizierbar wird.

Neue Legitimationsgrundlagen für die Transaktion

Ist der neue Zweck mit dem ursprünglichen Erhebungszweck nicht kompatibel, kann dies immer dadurch „geheilt“ werden, dass der Betroffene in die Weiterverarbeitung zum neuen Zweck einwilligt. Dies setzt allerdings voraus, dass die Einwilligung wirksam ist und nicht widerrufen wird. Und hier steckt der Teufel im Detail. Dies fängt bereits damit an, dass der Betroffene vor der Einwilligung sowohl über den (neuen) Verantwortlichen als auch über den Zweck der Datenverarbeitung und über die Möglichkeit zum jederzeitigen Widerruf aufgeklärt werden muss. Auch hier muss also – wie bei der Zweckänderungsmitteilung bei kompatiblen Zwecken – dem Betroffenen gegenüber die Unternehmenstransaktion offengelegt werden. Überhaupt muss der Betroffene neben diesen für die Wirksamkeit bzw. Freiwilligkeit seiner Einwilligung essentiellen Informationen auch sämtliche Pflichtangaben einer Zweckänderungsmitteilung mitgeteilt bekommen, denn die Pflicht des Verantwortlichen zur Zweckänderungsmitteilung ist unabhängig von der Frage, wie die Zweckänderung legitimiert wird. Weiter ist eine freiwillige Einwilligung im Rahmen eines bestehenden Beschäftigungsverhältnisses, also gegenüber dem Arbeitgeber, nur in sehr eng begrenzten Fallkonstellationen möglich. Der Gesetzgeber unterstellt, dass ein Arbeitnehmer, plakativ gesagt, „alles unterschreiben wird, um seinen Job nicht zu verlieren“ – das ist dann aber nicht „freiwillig“. Und schließlich kann die Einwilligung jederzeit vom Betroffenen widerrufen werden, sodass der Verarbeitung ab diesem Zeitpunkt „der Boden unter den Füßen weggezogen“ wird. Sprich: Die Daten sind – sofern keine Aufbewahrungspflichten bestehen – sofort zu löschen und das Löschverlangen des Betroffenen ist daneben an diejenigen Verantwortlichen, welche die Daten zwischenzeitlich übermittelt bekommen haben, weiterzuleiten.

Wenn keine Zweckkompatibilität gegeben ist und keine Einwilligung (als neue Legitimationsgrundlage) eingeholt werden kann bzw. soll oder diese nicht wirksam ist (bzw. wäre), dürfen die Daten dennoch für den veränderten Zweck verarbeitet werden, wenn für diesen eine eigene Legitimationsgrundlage identifiziert werden kann. Wenn man also die Daten auch vollständig neu unter dieser Legitimationsgrundlage erheben dürfte, darf man sie auch unter dieser Legitimationsgrundlage „weiterverarbeiten“. In den meisten Fällen wird die neue Legitimationsgrundlage eine Interessenabwägung sein. Vor der eigentlichen Abwägung muss aber feststehen, dass die durch die Interessenabwägung zu rechtfertigende Datenverarbeitung tatsächlich „erforderlich“ ist, d. h. es ist kein für den Betroffenen „milderes Mittel“ ersichtlich oder zumindest dem Verantwortlichen nicht zumutbar. Im obigen Beispielsfall der leitenden Angestellten Frau Maier, müsste es also für die anvisierte Transaktion „existenziell“ sein, dass der Kaufinteressent den vollständigen Anstellungsvertrag erhält und nicht

nur ein (vollständig) anonymisiertes Exemplar oder Daten über (mehrere) leitende Angestellte (Gehälter etc.) in aggregierter Form. Ob es für die „Erforderlichkeit" ausreicht, wenn der Kaufinteressent einfach nur erklärt, dass er ohne diesen Vertrag die Transaktion abbrechen werde, ist angesichts der starken Fokussierung des Datenschutzrechts auf den Betroffenen und dessen Grundrecht auf Schutz seiner personenbezogenen Daten zweifelhaft.

Ist die Verarbeitung (bzw. Übermittlung) für Transaktionszwecke hiernach „erforderlich", muss das (legitime) Interesse des Verantwortlichen an der Verarbeitung – die Vorbereitung und Durchführung einer Unternehmenstransaktion – mit dem Interesse des Betroffenen am „Schutz" seiner personenbezogenen Daten, abgewogen werden. Das ist so „wachsweich" wie es klingt, aber häufig wird das Interesse des Verantwortlichen überwiegen, wenn nicht besondere Gefahren für den Betroffenen oder spezifische Interessen desselben im Einzelfall ersichtlich sind und Verarbeitungssicherheit (s. u.) hinsichtlich der Daten gegeben ist. Unabhängig davon kann übrigens bei der Interessenabwägung der Betroffene der Verarbeitung widersprechen. Im Falle eines Widerspruchs ist die weitere Verarbeitung – worauf oben schon im Zusammenhang mit dem Beispielsfall des Erfinders Herrn Krause hingewiesen wurde – nur noch in ganz engen Ausnahmefällen zulässig. Die Interessenabwägung ist übrigens vom Verantwortlichen zu dokumentieren, damit im Rahmen einer Prüfung durch die Datenschutzaufsichtsbehörden oder in gerichtlichen Streitigkeiten nachgewiesen werden kann, dass sorgfältig abgewogen wurde.

Eine Zweckänderungsmitteilung an den Betroffenen ist – darauf wurde oben schon zur Einwilligung hingewiesen – auch dann notwendig, wenn keine Zweckkompatibilität vorliegt und der weiteren Verarbeitung der personenbezogenen Daten eine neue Legitimationsgrundlage „untergeschoben" wird. Frau Maier müsste also in jedem Fall eine Zweckänderungsmitteilung erhalten, aber im einen Fall (Zweckkompatibilität) könnte sie der Weiterverarbeitung (Übermittlung) ihrer ursprünglich auf Grundlage einer Vertragsbeziehung erhobenen Daten nicht widersprechen, im anderen Fall (keine Zweckkompatibilität und Interessenabwägung als neue Legitimationsgrundlage) schon. Ob dieser Widerspruch nicht eines Tages vom Europäischen Gerichtshof im Rahmen einer kreativen Gesetzesauslegung „richtiggedreht" wird, bleibt abzuwarten.

Ein besonderer Fall liegt übrigens dann vor, wenn – wie in internationalen M&A-Transaktionen häufig – personenbezogene Daten in ein „Drittland" außerhalb der EU übermittelt werden sollen. Eine derartige Übermittlung bedarf neben der oben besprochenen datenschutzrechtlichen Legitimationsgrundlage einer besonderen „Drittland-Übermittlungsgrundlage".

Soweit nicht die EU-Kommission beschlossen hat, das jeweilige Drittland datenschutzrechtlich als privilegiert anzusehen (d. h. es herrscht dort ein der EU vergleichbares Datenschutzniveau), und soweit nicht besondere Vorkehrungen (Nutzung von datenschutzrechtlichen Standardvertragswerken der EU oder von den Aufsichtsbehörden freigegebenen „binding corporate rules“) getroffen werden, wird häufig eine besondere Einwilligung in die Drittlands-Übermittlung die einzige Möglichkeit der Legitimation sein. Denn eine weitere theoretisch denkbare Ausnahmeregelung für eine Drittlandsübermittlung auf Basis „zwingender berechtigter Interessen des Verantwortlichen“ erfordert zusätzlich, dass die Aufsichtsbehörde von der Übermittlung in Kenntnis gesetzt wird, was kaum praktikabel sein dürfte und auch das Risiko unterschiedlicher Sichtweisen über die Berechtigung im Einzelfall birgt. Für die genannte besondere Einwilligung muss die betroffene Person „ausdrücklich“ in die Übermittlung in den Drittstaat einwilligen, nachdem sie „über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde“. Man kann sich ausmalen, dass vielen Betroffenen eine Einwilligung nach einer Unterrichtung, dass ihre Daten nun – aus europäischer Perspektive – in datenschutzrechtliches „Niemandsland“ übermittelt werden sollen, schwerfallen könnte. Besonders gilt dies für die „freiwillige“ Einwilligung in eine Drittlandsübermittlung gegenüber dem Arbeitgeber im Rahmen von Beschäftigungsverhältnissen.

Praxistipp:

Verkäufer und Zielunternehmen sollten im Rahmen der Vorbereitung der Transaktion in Bezug auf die voraussichtlich für die Due Diligence-Prüfung benötigten Daten prüfen, zu welchen Zwecken und mit welchen Pflichthinweisen diese ursprünglich erhoben wurden. Denn nur wenn schon der ursprüngliche Erhebungszweck die Übermittlung an den Kaufinteressenten abdeckt, was in der Praxis aber nur selten der Fall sein dürfte, kann bei einer Weitergabe personenbezogener Daten im Rahmen der Due Diligence-Prüfung auf eine Zweckänderungsmitteilung an den Betroffenen verzichtet werden.

Deshalb ist parallel zu überlegen, ob und in welchem Umfang personenbezogene Daten für die Übermittlung an Kaufinteressenten (einschließlich der Einstellung in Datenräume) anonymisiert werden können. Alternativ kann auch über eine Pseudonymisierung der Daten nachgedacht werden (indem z. B. Namen durch Nummern ausgetauscht werden, deren Zuordnung zu den Namen nur das Zielunternehmen kennt) mit dem Ziel, dass dem Kaufinteressenten keine Zuordnung zu den betroffenen Personen möglich ist.

Es kann sein, dass die Aussicht, den Betroffenen Zweckänderungsmitteilungen zukommen lassen zu müssen, die eigentlich nicht gewollte Anonymisierung oder Pseudonymisierung von personenbezogenen Daten doch als bessere Alternative erscheinen lässt. Zusätzlich sollte die Reaktion des Betroffenen auf die Zweckänderungsmitteilung (Widerspruch, Widerruf, Löschungsverlangen etc.) im Voraus bedacht werden. Bei Drittlandsübermittlungen muss zudem vorab das Vorliegen einer spezifischen Drittlandsübermittlungs-Legitimationsgrundlage geprüft werden.

Die datenschutzrechtliche Grundlage beim Vollzug eines Asset Deals

Oben wurde bereits hinsichtlich der Zweckkompatibilität beim Asset Deal zwischen Due Diligence-Prüfung und Vollzug eines konkret abgeschlossenen Unternehmenskaufvertrages unterschieden. Da die ursprünglichen Legitimationsgrundlagen die Übermittlung der personenbezogenen Daten an den Erwerber zunächst einmal nicht rechtfertigen, weil sie den Zweck des Asset Deals nicht abdecken, liegt jeweils eine Zweckänderung vor. Nachdem oben auf die Due Diligence-Phase abgestellt wurde, soll nachfolgend noch kurz auf die Unternehmensübertragung selbst, d. h. den Vollzug eines Asset Deals, eingegangen werden.

- Ziel des Asset Deals ist es u. a., dass die zwischen dem Verkäufer und verschiedenen Dritten (Arbeitnehmer, Lieferanten/Dienstleister, Kunden/Abnehmer) bestehenden **Vertragsverhältnisse auf den Käufer übergehen**. Im Regelfall ist diese „Vertragsübernahme" eine Vereinbarung zwischen Verkäufer und Käufer, welcher der dritte Vertragspartner zustimmen muss – sonst verbleibt das Vertragsverhältnis beim Verkäufer. Arbeitsverhältnisse gehen hingegen „automatisch" über (§ 613a BGB), sofern der jeweilige Arbeitnehmer nicht widerspricht. Nach der DSGVO sind nun solche Verarbeitungsvorgänge legitimiert, die für die Erfüllung von Verträgen mit dem Betroffenen „erforderlich" sind. Mit anderen Worten: Wenn man einen Vertrag mit dem Betroffenen – der Betroffene hat ja dem Vertrag als solchem zugestimmt – nur erfüllen kann, wenn man bestimmte personenbezogene Daten des Betroffenen verarbeitet, dann sollte das Datenschutzrecht nicht die Vertragserfüllung behindern. Ein Betroffener könnte also nicht sagen: Ich möchte die bestellten Stiefel geliefert erhalten, stimme aber nicht zu, dass dafür meine Lieferadresse verarbeitet (z. B. an den Lieferdienst übermittelt) wird. Steht die Huber AG in einem Vertragsverhältnis mit ihrer Kundin, Frau Becker, und soll dieses im Rahmen eines Asset

Deals an den Erwerber, die Schäfer SE & Co. KGaA, übertragen werden, so wird also Frau Becker im Regelfall ein Schreiben der Huber AG erhalten, indem ihre Zustimmung erbeten wird. Dieses Schreiben ist vertragsrechtlicher, nicht datenschutzrechtlicher Natur. Eine Fiktion der vertragsrechtlichen Zustimmung („Wenn Sie sich nicht melden, gilt das als Zustimmung") scheitert in aller Regel an AGB-rechtlichen Hürden. Solange also Frau Becker der erwünschten Vertragsübernahme nicht zugestimmt hat, besteht der Vertrag noch (ausschließlich) mit dem ursprünglichen Vertragspartner, der Huber AG. Man könnte dies neudeutsch als „opt-in" bezeichnen. Die Weitergabe von Kundendaten – und dies gilt für andere vertragsbezogenen Daten Dritter in gleicher Weise – durch die Huber AG an die Schäfer SE & Co. KGaA kann also nur und erst für die Erfüllung des mit Frau Becker bestehenden Vertrages „erforderlich" sein, wenn Frau Becker der Vertragsübernahme zugestimmt hat. Vorher besteht kein Vertrag zwischen der Schäfer SE & Co. KGaA und Frau Becker. In dieser Phase vor der Zustimmung von Frau Becker kann die Weitergabe der Daten nur für die Erfüllung einer Vertragsübernahmevereinbarung zwischen der Huber AG und der Schäfer SE & Co. KGaA als Teil des APAs „erforderlich" sein. Das ist aber datenschutzrechtlich unerheblich. Für die Erfüllung eines Vertrages „mit" Frau Becker ist die Weitergabe der Daten zunächst datenschutzrechtlich nicht „erforderlich".

Diese Fallkonstellation ist ein Gegenstand des Beschlusses der Datenschutzkonferenz vom 24. Mai 2019 zum Thema Asset Deal. Die Datenschutzkonferenz geht davon aus, dass neben der notwendigen Zustimmung eines (B2C-)Kunden zur Vertragsübernahme (von der Datenschutzkonferenz als „Schuldübernahme" bezeichnet) auch eine datenschutzrechtliche Einwilligung (von der Datenschutzkonferenz als „Zustimmung" bezeichnet) notwendig ist, damit die Daten „übergehen" können:

„In dieser zivilrechtlichen Genehmigung wird als Minus auch die datenschutzrechtliche Zustimmung zum Übergang der erforderlichen Daten gesehen. Damit sind die Gegeninteressen der Kundin oder des Kunden gewahrt."

Genaugenommen dürfte dies aber gar nicht notwendig sein. Denn wenn die bisherige datenschutzrechtliche Legitimationsgrundlage der mit dem Betroffenen bestehende Vertrag war und dieser zivilrechtlich korrekt – ob mit Zustimmung des Betroffenen oder anderweitig (z. B. bei einer Gesamtrechtsnachfolge im Falle einer umwandlungsrechtlichen Verschmelzung) – auf einen neuen Rechtsträger übergeht, muss das Datenschutzrecht diesem (im Hinblick auf die Identität einer der Vertragsparteien) veränderten Zweck folgen. Denn datenschutzrechtlich legitim sind sämtliche Verarbeitungen, die für

die Erfüllung des Vertrages – nach dessen jeweiligem Inhalt, der sich auch verändern kann – erforderlich sind. Es ist nicht ersichtlich, dass die DSGVO nur auf den „Vertragszustand“ zum Zeitpunkt des Vertragsabschlusses abstellt.

Auch wenn nun immer wieder behauptet wird, die verschiedenen datenschutzrechtlichen Legitimationsgrundlagen stünden völlig gleichberechtigt und isoliert nebeneinander, wird angesichts dieser Aussage deutlich, dass in einer derartigen Situation, in der „eigentlich“ ein Vertrag mit dem Betroffenen besteht und dessen Zustimmung zur Vertragsübernahme ansteht, eine „alternative“ (der Jurist würde vielleicht sagen: „hilfsweise“) Rechtfertigung der Datenübermittlung an einen bislang vertragsfremden Dritten (die Schäfer SE & Co. KGaA) über eine Interessenabwägung kritisch zu sehen ist. Noch klarer wird dieses Argument, wenn Frau Becker auf die Bitte zur Zustimmungserteilung hin der Huber AG explizit zurückschreibt, dass sie ihre Zustimmung nicht erteile, weil sie die Unternehmenspolitik der Schäfer SE & Co. KGaA nicht gutheißt. Darf in diesem Fall davon ausgegangen werden, dass die Datenübermittlung dennoch auf Basis einer Interessenabwägung zulässig ist? Wohl nicht. Das wiederum birgt Probleme für den Asset Deal. Denn üblicherweise wird vereinbart, dass sich die Parteien bei verweigerter Zustimmung des Dritten zur Vertragsübernahme im Innenverhältnis (wirtschaftlich) so stellen, als sei die Zustimmung erteilt worden. Die Durchführung dieser Innenvereinbarung wird demnach erschwert, wenn die Kundendaten von Frau Becker nicht an die Schäfer SE & Co. KGaA übermittelt werden dürfen.

Tritt allerdings das veräußernde Unternehmen im Rahmen des Asset Deals nicht das gesamte Vertragsverhältnis, sondern nur (Geld-)**Forderungen gegenüber dem Betroffenen ab**, bedarf es zivilrechtlich nicht der Zustimmung des Betroffenen, d. h. des Schuldners der Forderung. Entsprechend geht die Datenschutzkonferenz für diesen Fall auch nicht davon aus, dass für die Übermittlung der forderungsbezogenen (Schuldner-)Daten die datenschutzrechtliche Einwilligung des betroffenen Schuldners erforderlich ist. Die Datenübertragung ist laut Datenschutzkonferenz als durch eine Interessenabwägung legitimiert anzusehen. Richtigerweise dürfte aber die datenschutzrechtliche Legitimationsgrundlage in einer rechtlichen Verpflichtung des veräußernden Unternehmens (bisherigen Gläubigers) gegenüber dem Erwerber (neuer Gläubiger) bestehen: Nach § 402 BGB ist *„der bisherige Gläubiger verpflichtet, dem neuen Gläubiger die zur Geltendmachung der Forderung nötige Auskunft zu erteilen“*. Das umfasst natürlich – neben anderen Informationen – auch Name und Anschrift des Schuldners.

- Anders ist dies bei Arbeitsverträgen zu sehen, bei denen der Vertragsübergang auf den neuen Arbeitgeber zunächst einmal gesetzlich angeordnet wird. Das Arbeitsverhältnis geht also erst einmal über. Der Betroffene (Arbeitnehmer) kann jedoch durch einen Widerspruch ein „Zurückfallen" des Arbeitsverhältnisses auf den ursprünglichen Arbeitgeber bewirken. Das wäre dann der „opt-out"-Fall. Solange kein Widerspruch innerhalb der arbeitsrechtlichen Monatsfrist erhoben wird, ist demnach die Datenübermittlung an den neuen Arbeitgeber zur Erfüllung des – kraft Gesetzes – auf diesen übergegangenen Arbeitsverhältnisses „erforderlich". Denn der neue Arbeitgeber könnte sonst seine Pflichten gegenüber seinem (neuen) Arbeitnehmer nicht erfüllen. Widerspricht der Arbeitnehmer allerdings, entfällt diese Legitimationsgrundlage wieder und die erhaltenen Daten müssen beim Übermittlungsempfänger gelöscht werden, sofern nicht ausnahmsweise eine andere Legitimationsgrundlage fortbesteht.

- In Fällen, in denen kein Vertragsverhältnis mit dem Betroffenen selbst besteht, kommt hingegen eine Interessenabwägung als datenschutzrechtliche Legitimationsgrundlage für die Übermittlung an den Unternehmenskäufer in Betracht. Dies gilt beispielsweise bei der Übermittlung der personenbezogenen Daten zu „Marketing-Kontakten", zu früheren Vertragspartnern, zu Ansprechpartnern von Unternehmen oder Behörden, von Schriftverkehr mit Dritten oder von historischen Verträgen. Auch wenn der Unternehmensverkäufer in diesen Fällen die Daten nach der Übermittlung bei sich löscht, liegt dennoch datenschutzrechtlich eine Übermittlung an einen Dritten (und nicht etwa ein datenschutzrechtlich irrelevanter „Hand-over") vor.

  Der oben genannte Beschluss der Datenschutzkonferenz hat nun diese Übermittlung insoweit einer genaueren Betrachtung unterzogen, als es um (B2C-)„Bestandskunden" des veräußernden Unternehmens eines Asset Deals geht. Dabei ist vorweg darauf hinzuweisen, dass der Beschluss der Datenschutzkonferenz gegen die Stimmen aus Berlin (Berliner Beauftragte für Datenschutz und Informationsfreiheit) und Sachsen (Sächsischer Datenschutzbeauftragter) erging, da diese einerseits die Frage, ab wann Kontakte so „abgekühlt" sind, dass sie datenschutzrechtlich gelöscht werden müssen, und andererseits die Frage, ob bei Forderungsabtretungen eine Übermittlung von Schuldnerdaten an den neuen Gläubiger zulässig ist, strenger als die übrigen „Landesvertreter" sehen. Auch zeigen die obigen und nachfolgenden Bemerkungen zum Beschluss der Datenschutzkonferenz im Ergebnis, dass diese sich, provokant gesagt, „das Recht selber macht", welches sie dann wohl auch in entsprechenden Verfahren vollziehen will. Das ist nicht gerade geeignet, das Vertrauen in die Datenschutzbehörden zu stärken, die in ihrer rechtsstaatlichen Unabhängigkeit doch gerade auf die Kraft überzeugender (Sach-)Argumente auf

der Basis des Gesetzestextes setzen sollten. Eine detaillierte argumentative Herleitung der von der Datenschutzkonferenz apodiktisch formulierten Grundsätze auf dem Boden des Texts der DSGVO wäre in jedem Fall wünschenswert gewesen. Es bleibt daher zu hoffen, dass datenschutzunkundige Richter diese behördlichen „Vorgaben" nicht mit dem Gesetzestext verwechseln.

Die Datenschutzkonferenz unterscheidet für Betroffene, mit denen keine laufende Vertragsbeziehung (Dauerschuldverhältnis) besteht, zwischen „alten" Bestandskunden, bei denen die letzte (Austausch-)Vertragsbeziehung (z. B. Kauf im Webshop) länger als drei Jahre zurückliegt, und „neuen" Bestandskunden, bei denen die letzte Vertragsbeziehung jünger als drei Jahre ist. Für die Übernahme von Kunden mit noch „aktiven" Vertragsbeziehungen ist ohnehin eine Zustimmung zur Vertragsübernahme notwendig (s. o.). Allerdings mag es auch Grenzfälle geben, in denen vom Vorliegen einer „ungekündigten Rahmenbeziehung" auszugehen ist, die aber nicht mehr aktiv betrieben und auch nicht gekündigt wird, weil sie keine laufenden Leistungs- und Zahlungspflichten begründet, aber dennoch (aus zivilrechtlicher Sicht) rahmenvertraglichen Charakter aufweist und damit eine Rechtsbeziehung mit Nebenpflichten darstellt. Auch derartige rahmenvertragliche Beziehungen können zivilrechtlich – mit Zustimmung des Vertragspartners „auf der anderen Seite des Tisches" – durch eine Vertragsübernahme übernommen werden. Hierauf geht der Beschluss der Datenschutzkonferenz aber nicht ein – und auch nicht auf die Übertragung der unternehmensbezogenen Kontaktdaten der Ansprechpartner (Mitarbeiter) eines B2B-Kunden bzw. -Lieferanten.

Hinsichtlich der Daten „alter" (B2C-)Bestandskunden geht die Datenschutzkonferenz offensichtlich von noch aktiven Aufbewahrungspflichten (insbesondere aus § 147 AO – steuerlich relevante Unterlagen) aus. Diese Daten dürfen zwar für derartige Archivzwecke übergehen (wenn das neue Unternehmen das „Archiv" des alten Unternehmens übernimmt), aber nicht produktiv genutzt werden (Werbung etc.). Im Rahmen eines sehr engen Berechtigungskonzepts sind sie demnach für die meisten internen Abteilungen bzw. Mitarbeiter zu sperren. Für die Daten „aktiver" Bestandskunden geht die Datenschutzkonferenz hingegen im Rahmen einer Interessenabwägung von einer Legitimation zur Übermittlung an und Nutzung durch den Erwerber aus. Offensichtlich sollen in diesem Zusammenhang allerdings sämtlichen Betroffeneninformationen mit einem Hinweis auf ein Widerspruchsrecht zur Verfügung gestellt werden. Dies gilt jedoch nicht für Bankdaten der Betroffenen: Diese dürfen nicht im Rahmen einer Interessenab-

wägung, sondern nur auf Einwilligung des Betroffenen hin übernommen werden. Dasselbe gilt (natürlich) für besondere Kategorien personenbezogener Daten, etwa Gesundheitsdaten.

Für die „Demarkationslinie" von drei Jahren führt die Datenschutzkonferenz in einer Fußnote zwei kurze Gründe an. Einerseits handele es sich um die zivilrechtliche Regelverjährungsfrist, andererseits *„haben erfahrungsgemäß nichtaktive Kundendaten älter als 3 Jahre für die erwerbende Stelle keine Bedeutung mehr und sind veraltet"*. Beide Gründe sind nicht sehr überzeugend. Warum drei Jahre alte Kaufverträge – die Gewährleistungsverjährung beträgt in aller Regel zwei Jahre und der Kaufpreis wird üblicherweise bei Lieferung bezahlt – gerade aufgrund der Regelverjährung ihre datenschutzrechtliche Bedeutung verlieren sollten, erschließt sich nicht. An anderer Stelle weisen die Datenschutzbehörden regelmäßig darauf hin, dass den Verjährungsfristen als solchen gerade keine datenschutzrechtliche Relevanz (etwa zur Unterlegung eines Aufbewahrungsrechts) zukommt – je länger die Verjährungsfristen, desto intensiver wird auf die „Abkopplung" des Datenschutzrechts hingewiesen. Und die Argumentation mit „Erfahrungen" quer durch alle Branchen, Produkte, Dienstleistungen, Altersstufen, B2B/B2C-Besonderheiten etc. erscheint höchst fragwürdig. Beide Argumente lassen sich nicht direkt der DSGVO entnehmen und die Datenschutzbehörden machen sich hier nicht einmal die Mühe einer genaueren Herleitung.

In Bezug auf die „aktiven" Bestandskunden erläutert die Datenschutzkonferenz nicht, warum, wann, von wem und welche Informationen den Kunden zur Verfügung zu stellen sind. Es bleibt unklar, ob das veräußernde Unternehmen die Kunden mit der vorgeschlagenen Sechs-Wochen-Widerspruchsfrist anschreiben und diese abwarten soll, bis die Daten übermittelt werden. Einen derartigen Mechanismus sieht die DSGVO nicht vor. Ebenso bleibt offen, ob es sich bei der Nachricht an den Kunden der Sache nach um eine Zweckänderungsmitteilung handelt bzw. ob und welche Pflichtinformationen (Art. 13/14 DSGVO) mitzuteilen sind. Der Hinweis der Datenschutzkonferenz „viele Kundinnen und Kunden sind bei einer Aufforderung zu einer ausdrücklichen Einwilligung eher überrascht" gibt zu der Spekulation Anlass, ob die Datenschutzbehörden „eigentlich" die Auffassung vertreten, dass es nach der DSGVO einer Einwilligung bedürfte, auf der Umsetzung dieser Vorgabe aber nicht bestehen, weil die mutmaßliche Überraschung der Betroffenen schwerer wiegt. Nicht weiter erklärt wird seitens der Datenschutzbehörden auch, weshalb im Gegensatz zum Vorstehenden (nur) die Übermittlung von Bankdaten, nicht aber die Übermittlung der Informationen über das Zahlungsverhalten einer Einwilligung des Betroffenen bedarf. Hier hat die Datenschutzkonferenz

anscheinend eine „pauschale“ Interessenabwägung vorgenommen und entschieden, dass – im Unterschied zu den Kontaktdaten – das Interesse des Betroffenen an der Nichtweitergabe seiner Bankdaten an den Erwerber seiner „Kundenbeziehung“ stets und ausnahmslos größer ist als das Interesse des Erwerbers, diese Bankdaten nicht zu erhalten. Weder diese Bewertung als solche (sondern nur das Ergebnis) noch die Gründe für dieses Abwägungsergebnis lassen sich dem Beschluss entnehmen. Auch dies überrascht, da die Datenschutzbehörden an anderer Stelle häufig darauf hinweisen, dass eine datenschutzrechtliche Interessenabwägung eine Einzelfallentscheidung anhand der in der individuellen Fallkonstellation bestehenden Interessen darstellt, die auch als solche zu dokumentieren ist.

Sowohl bei Bestehen eines Vertragsverhältnisses mit dem Betroffenen als auch in den vorgenannten weiteren Fällen stellt sich ungeachtet der vorstehenden Diskussionen um die richtige Legitimationsgrundlage und deren Reichweite die Frage, ob beim Vollzug eines Asset Deals (zur Due Diligence-Prüfung siehe schon oben) in der Übermittlung an den neuen Unternehmensinhaber eine Zweckänderung vorliegt. Dies hätte datenschutzrechtlich zur Folge, dass dem Betroffenen eine „Zweckänderungsmitteilung“ zugehen muss. Wie oben dargestellt, muss diese Mitteilung vor der Verarbeitung zum geänderten Zweck, also vor der Übermittlung an den Unternehmenskäufer, stattfinden. In Anknüpfung an den obigen Fall der leitenden Angestellten Frau Maier soll nun exemplarisch deren Anstellungsverhältnis – mit Übermittlung der zugehörigen personenbezogenen Daten – im Rahmen eines Asset Deals von der Huber AG an die Schäfer SE & Co. KGaA übergehen. Und stellvertretend für Situationen ohne Vertragsverhältnis sollen die Kontaktdaten von und archivierte Korrespondenz mit Herrn Walter, einem Vorstand des örtlichen Sportvereins, den die Huber AG in der Vergangenheit immer mal wieder mit Sponsoring-Maßnahmen unterstützt hat, an die Schäfer SE & Co. KGaA übermittelt werden. In einem archivierten E-Mail-Verkehr berichtet Herr Walter zusätzlich gegenüber dem vormaligen Vorstand der Huber AG von seiner bettlägerigen Frau, die sich sehr über den Blumenstrauß der Huber AG gefreut und zwischenzeitlich das Krankenhaus wieder verlassen habe.

Die Frage, ob in diesen Beispielsfällen mit der Übermittlung an den Unternehmenskäufer eine Änderung des Zwecks einhergeht, hängt davon ab, wie der „Zweck“ ursprünglich definiert wird. Hier soll der Fall betrachtet werden, dass auf Basis der Legitimationsgrundlage Interessenabwägung der Zweck in den ursprünglichen Pflichtinformationen inhaltlich als Direktmarketing (im weitesten Sinne) gegenüber dem Betroffenen definiert wurde. Von dieser Sachverhaltsgestaltung kann etwa im Fall von Herrn Walter oben ausgegangen werden; auch karitative, soziale und politische Kontaktpflege stellt datenschutzrechtlich eine Form von

„Direktmarketing“ dar. Diese Zwecksetzung kann nun entweder nur Direktmarketing durch den ursprünglichen Verantwortlichen, der die Daten erhoben hat, gegenüber dem Betroffenen umfassen, oder alternativ auch von Anfang an Rechtsnachfolger (Unternehmenskäufer im Rahmen eines Asset Deals) mit einschließen. Üblicherweise wird in datenschutzrechtlichen Pflichthinweisen zum Erhebungszeitpunkt nicht ausdrücklich darauf hingewiesen, dass „der Zweck auch die Übermittlung der erhobenen Daten an einen etwaigen späteren Asset-Deal-Käufer“ mit einbezieht. Ist der Zweck also „verantwortlichenunabhängig“ oder nicht?

Datenschützer würden hier nun vermutlich wie folgt „vom Ergebnis her“ argumentieren: Der Legitimationsgrund der Interessenabwägung gibt Herrn Walter jederzeit das „opt-out“-Recht (Widerspruch), um die Verarbeitung – von Ausnahmen abgesehen – beenden zu können. Dieses kann er gegenüber der Schäfer SE & Co. KGaA, die den ursprünglichen Verantwortlichen Huber AG „beerbt“, überhaupt nur geltend machen, wenn er weiß, dass die Daten weitergegeben werden. Würde Herr Walter nicht über die Übermittlung (infolge einer Zweckänderung) informiert, könnte die Schäfer SE & Co. KGaA die „erworbenen“ Daten auch für einen längeren Zeitraum „still“ – also ohne dass Herr Walter davon erfährt – nutzen, obwohl Herr Walter dem eigentlich hätte widersprechen wollen. Nicht jeder Betroffene möchte beispielsweise, dass „sein“ Verantwortlicher, der „seine“ Daten verarbeitet, an Google oder Amazon oder Facebook verkauft wird und der jeweilige Konzern sich die Daten so „einverleibt“ und dann (immer noch zum inhaltlichen Zweck der „Direktwerbung“) mit eigenen Daten zusammenführt und verwendet. Der Zweck würde sich nach dieser Argumentation also ursprünglich nur auf Direktmarketing gerade durch die Huber AG beschränken; die Übermittlung an die Schäfer SE & Co. KGaA ändert zwar die inhaltliche Komponente dieses Zwecks nicht, wohl aber die „Verantwortlichen-Komponente“. Hierfür würde auch eine fehlende (ausdrückliche) Information in den ursprünglichen Pflichthinweis sprechen. Mit dieser Begründung kann demnach – im Ergebnis ähnlich wie von der Datenschutzkonferenz gefordert (s. o.) – eine Zweckänderungsmitteilung, verbunden mit den geänderten Pflichtinformationen, gefordert werden. Es bleibt aber gleichwohl unklar, auf welcher Grundlage die Datenschutzkonferenz in diesen Fällen eine „Widerspruchsfrist“ (und deren Abwarten?) einfordert, die von der DSGVO weder im Kontext der Interessenabwägung noch im Kontext der Zweckänderung (ausdrücklich) gefordert wird.

Diese mögliche Argumentation wirft die Frage auf, ob nicht generell in jedem Pflichthinweis bei Erhebung personenbezogener Daten auf einen zukünftigen Unternehmenskäufer als Übermittlungsempfänger hingewiesen werden sollte. Zumindest solange der Empfänger nicht namentlich feststeht, genügt nach der DSGVO die Angabe der „Kategorien von Emp-

fängern“. Verbindlich entscheiden kann über die Zulässigkeit eines solchen „Übermittlungsvorbehalts auf Vorrat“ – ebenso wie über die Frage, ob eine Zweckänderung vorliegt – nur (dereinst) der Europäische Gerichtshof.

Praxistipp:

Bei Abschluss und Vollzug eines Asset Deals sollten Verkäufer und Käufer gemeinsam frühzeitig die datenschutzrechtlich zulässige Abwicklung des „Datenübergangs“ erörtern und festlegen. Hierzu zählt zunächst eine Bestandsaufnahme der personenbezogenen Daten, die Gegenstand des Asset Deals sind sowie die Frage, in welchen Fällen von einer Änderung der ursprünglichen datenschutzrechtlichen Zweckbestimmung auszugehen ist.

Bei Zweckänderungen ist durch den Unternehmensverkäufer eine zwischen den Parteien abgestimmte Zweckänderungsmitteilung an den Betroffenen abzusetzen. Dies kann in den Fällen, in denen ein Vertragsverhältnis mit dem Betroffenen die datenschutzrechtliche Legitimationsgrundlage bildet, mit der Bitte um vertragsrechtliche Zustimmung zur Vertragsübernahme verbunden werden. Zudem sind – am besten bereits im APA selbst – Regelungen zwischen den Parteien des Unternehmenskaufvertrages für den Umgang mit Konstellationen vorzusehen, in denen sich ein Betroffener gegen die Übermittlung der ihn betreffenden Daten an den Unternehmenskäufer wehrt.

Dabei sollten die Parteien jeweils auch prüfen, inwieweit der Beschluss der Datenschutzkonferenz zu Asset Deals für den konkreten Fall einschlägig ist und ob die Parteien – um Risiken zu minimieren – nach den behördlichen Vorgaben vorgehen wollen.

Verarbeitungssicherheit: „Need to know“ and TOMs

Steht nun auf Basis der obigen Fragestellungen im Einzelfall fest, welcher Verantwortliche welche personenbezogenen Daten wie verarbeitet und wann die Betroffenen in welcher Weise darüber aufzuklären sind, müssen – neben der notwendigen internen Dokumentation – „nur noch“ die Modalitäten der Verarbeitung richtig strukturiert werden. Insoweit ergeben sich für die hier in Rede stehenden M&A-Fallgestaltungen keine Besonderheiten gegenüber dem Normalfall „Datenschutz im Unternehmen“, d. h. gegenüber dem von der DSGVO vorgegebenen Datenschutz-Compliance-Management-System, das jedes Unternehmen als Verantwortlicher zu etablieren hat.

Neben den oben behandelten Fragen der datenschutzrechtlichen Legitimationsgrundlage und der Transparenz gegenüber den Betroffenen (Pflichthinweise) betreffen die entsprechenden Compliance-Vorgaben im Wesentlichen die Verarbeitungssicherheit im weitesten Sinne. Einerseits muss der Verantwortliche (positiv) sicherstellen, dass die Daten so verarbeitet werden, wie dies die DSGVO vorsieht bzw. erlaubt (und nicht anders). Diese Compliance-Verpflichtung wird umgesetzt durch (präskriptive) technische Maßnahmen, insbesondere Software-Funktionen, und organisatorische Maßnahmen, insbesondere Vorgaben an Mitarbeiter des Verantwortlichen. Frühzeitig wird auch die Beschaffungsphase neuer Hard- und Software hiervon erfasst; die „privacy by design“-Vorgabe fordert nämlich, möglichst datenschutzfreundliche Technik zu verwenden. Andererseits muss der Verantwortliche – als „die andere Seite der Medaille“ – (negativ) verhindern, dass die Daten unrechtmäßig verarbeitet werden. Auch dies geschieht durch (präventive) technisch-organisatorische Maßnahmen in Form der Gewährleistung ausreichender Datensicherheit, insbesondere durch Zutritts-, Zugangs-, Zugriffs- und Übermittlungskontrollen. Ziel ist der Schutz der Daten vor unbefugtem „Abzug“, insbesondere – aber nicht nur – durch Kriminelle (Stichwort „Hacker“). Die hierfür notwendigen Maßnahmen lassen sich aus dem Risikoprofil der verarbeiteten Daten bzw. der Betroffenen und aus dem „Stand der Technik“ im Bereich der Daten- bzw. Cybersicherheit gewinnen.

Ein wesentliches Ziel bei der „Abwehr des Zugriffs durch Unbefugte“ besteht neben der Prävention gegen Angriffe von außen auch darin, Zugriffe nicht befugter Mitarbeiter zu unterbinden. Die DSGVO sagt dies zwar nicht ausdrücklich, aber Datenschutzrechtler gehen wie selbstverständlich davon aus, dass innerhalb der Organisation eines Verantwortlichen nur diejenigen dem Verantwortlichen unterstellten Personen „befugt“ sind bzw. Zugriff auf personenbezogene Daten haben dürfen, die diese Daten bei deren zweckgemäßen Verar-

beitung benötigen („need to know"-Grundsatz). Wenn also bei der Schulze Kapitaleinkaufs GmbH die beiden Investment-Managerinnen Frau Koch und Frau Bauer tätig sind und der mögliche Erwerb der Aktien an der Huber AG ausschließlich in das „Ressort" von Frau Koch fällt, dann darf Frau Bauer keinen Zugriff auf diejenigen personenbezogenen Daten haben, die im Rahmen dieses Projekts verarbeitet werden. Entsprechende Sicherheitsmechanismen und Berechtigungskonzepte (Passwortschutz etc.) müssen diese „Sphären" voneinander abgrenzen.

Die interne „Silobildung" in Bezug auf die Daten nach dem „need to know"-Grundsatz ist jedoch nur ein kleiner Teil der gesamten „technisch-organisatorischen Maßnahmen" (TOMs), die von der DSGVO gefordert werden und mit denen der Verantwortliche sicherzustellen hat, dass die DSGVO eingehalten wird. Letztlich fordert der Gesetzgeber das Design und die Implementierung unternehmensinterner Prozesse und Kontrollen, die in ihrer Gesamtheit die „Compliance" mit der DSGVO sicherstellen. Oft steht am Ende dieser Entwicklung ein „Datenschutzhandbuch" des Verantwortlichen, in dem sämtliche einschlägigen (Prozess-)Inhalte festgehalten und idealerweise auch in ihrer Herleitung begründet werden. Der „Verkaufsfall" dürfte allerdings für ein Zielunternehmen – im Gegensatz zu „typischen" Unternehmensverkäufern und Unternehmenskäufern – einen atypischen Prozess darstellen, d. h. die entsprechenden Überlegungen hierzu müssen im Vorfeld der Unternehmenstransaktion „ad hoc" entwickelt und umgesetzt werden.

Bearbeitung von Betroffenenrechten

Zu den genannten Prozessen und Kontrollen zählt auch die zügige Bearbeitung von Betroffenenrechten. Oben wurde bereits auf das Recht von Betroffenen hingewiesen, zum Zeitpunkt der Erhebung von Daten und der Zweckänderung ihrer Verarbeitung bestimmte Pflichthinweise mitgeteilt zu erhalten. Hierzu kommen weitere Betroffenenrechte, auf die der Verantwortliche reagieren können muss. Dazu zählen insbesondere das Recht auf Auskunft und auf Löschung (wenn der Zweck erreicht oder fortgefallen ist, z. B. auch bei Widerruf/Widerspruch des Betroffenen). Solche Rechte müssen in der Regel innerhalb eines Monats bearbeitet werden, was den angesprochenen Verantwortlichen und dessen unternehmensinterne Prozesse (und Ressourcen) immer dann vor große Herausforderungen stellen wird, wenn – wie möglicherweise bei einer M&A-Transaktion (Due Diligence-Phase, Asset Deal-Vollzug) – viele Betroffene ihre Rechte innerhalb eines kurzen Zeitraums geltend machen.

Sanktionen

Über die in der DSGVO vorgesehenen Sanktionen, insbesondere Bußgelder, ist im Zuge der Einführung der DSGVO viel geschrieben worden. Dies soll hier nicht weiter vertieft werden, zumal sich hier keine prinzipiellen Besonderheiten im Bereich M&A ergeben. Aber gerade in diesem Bereich könnte die Möglichkeit der Verletzten (d. h. der Betroffenen, in Bezug auf deren Daten die DSGVO verletzt wurde), neben dem Ersatz materieller Schäden gleichermaßen auch Ersatz immaterieller Schäden verlangen zu können, enorme praktische Bedeutung gewinnen. Dies zumal dann, wenn Ansprüche mehrerer gleichartig Verletzter „gepoolt“ werden. Man denke an eine Due Diligence-Prüfung einer später gescheiterten Transaktion, in der massenhaft personenbezogene (z. B. Beschäftigten-) Daten ohne eine notwendige Zweckänderungsmitteilung übermittelt werden und dies der Arbeitnehmervertretung bekannt wird.

Fazit zum M&A-Prozess

M&A-Prozesse sind komplex und in deren Rahmen werden viel mehr personenbezogene Daten benötigt, übermittelt und ausgewertet als dies auf den ersten Blick scheinen mag. Das Datenschutzrecht ist ebenfalls komplex und auf viele Auslegungsfragen gibt es bislang keine eindeutigen Antworten. Das ist insbesondere deshalb unglücklich, weil ein datenschutzwidriger Umgang mit personenbezogenen Daten – im Gegensatz zum vormaligen Datenschutzrecht, das in vielen Aspekten schon gleichartig ausgestaltet war – immense Sanktionen nach sich ziehen kann.

Es gibt nun drei Möglichkeiten, damit umzugehen:

- Erstens kann man das Thema mit dem Ansatz „wo kein Kläger, da kein Richter" ignorieren. Das kann über kurz oder lang Betroffene auf den Plan rufen, die sich datenschutzwidrig behandelt fühlen und Behörden oder Gerichte anrufen. Man kann dieses Risiko – rechtswidrigerweise! – ignorieren. Das wäre aber in etwa so, als wenn man vorsätzlich die kartellrechtliche Fusionskontrolle ignorieren würde – ein rechtlicher Themenkomplex, den zu ignorieren in der Praxis keinem Unternehmensverkäufer oder -käufer einfallen würde, weil dort im Falle eines Rechtsverstoßes die Transaktion (Anteilsübertragung) als solche unwirksam ist.

- Zweitens kann das Thema zur sprichwörtlichen „Doktorarbeit" überhöht werden und sich so als „initialer Stolperstein" für gut gemeinte Transaktionen erweisen. Getreu dem Motto: Wer überall datenschutzrechtliche Risiken sieht, sollte besser keine Unternehmen (ver)kaufen. Dies betrifft insbesondere das Problem, dass zumindest bestimmte Datenübermittlungen die Mitteilung gewisser Informationen über die Transaktion an solche Dritten (Betroffenen) notwendig machen, die aus anderen Gründen von der – noch unfertigen – Transaktion nicht erfahren sollten. Gerade in großen Transaktionen mit Heerscharen von Beratern könnten solche Fragen drohen „totgeprüft" zu werden – was sich als rechtlicher „deal killer" erweisen kann –, weil hier keine Rechtssicherheit gegeben ist.

- Drittens kann Datenschutz in M&A-Transaktionen vorausschauend, aber mit Augenmaß umgesetzt werden. Dann wird zunächst einmal anonymisiert und pseudonymisiert, wo immer das irgend möglich ist. Das erfordert einigen Aufwand, der aber eventuell in Zukunft, zumindest in großen Teilen, automatisiert werden könnte. Die Richtigkeit der anonymisierten Informationen, die durch die Anonymisierung möglicherweise an „Beweiswert" einbüßen, muss dann durch entsprechende vertragliche Garantien im Unternehmenskaufvertrag abgesichert werden. Und die Fälle, in denen der Kaufinteressent wirklich die betroffene Person „hinter" den Daten namentlich kennen muss, werden dann von den Parteien „in good faith" erörtert und jeweils im konkreten Fall Wege gefunden, wie sowohl transaktionsschonend als auch datenschutzkonform vorgegangen werden kann. Diese Vorgehensweise wird die Transaktionskultur verändern; der Austausch personenbezogener Daten im Vorfeld einer Transaktion wird nicht mehr die Regel sein, sondern die Ausnahme.

Datenschutzrechtliche Risiken durch den Unternehmenserwerb

Unabhängig vom Prozess, mit dem die Parteien zu einer Unternehmenstransaktion gelangen, stellt sich die Frage aktueller und historischer datenschutzrechtlicher Risiken des Zielunternehmens im Rahmen von dessen Geschäftsbetrieb. Mit anderen Worten: Das Zielunternehmen kann – in welchem Zusammenhang auch immer – gegen geltendes Datenschutzrecht verstoßen haben oder noch verstoßen und damit besteht das Risiko künftig zu zahlender Abmahngebühren, Bußgelder, Schadensersatzzahlungen und dergleichen.

Diese Problematik betrifft in erster Linie den Share Deal, wenn nämlich der Schuldner solcher Zahlungen – die Zielgesellschaft – vom Käufer erworben wird. Beim Asset Deal werden, da der „Verantwortliche" im Sinne des Datenschutzrechts nicht Gegenstand der M&A-Transaktion ist, derartige Risiken in der Regel nicht mit übergehen. Der Erwerber (bzw. das Erwerbsvehikel) eines Asset Deals kauft sich das Risiko jedoch in zwei anderen Hinsichten ein. Übernimmt er risikobehaftete Strukturen (Prozesse, Mitarbeiter etc.), ohne diese zu ändern, kann der Datenschutzverstoß „am Tag Null" auch beim Erwerber auftreten. Und außerdem kann die Haftung für vergangene Datenschutzverstöße auch die übernommenen Mitarbeiter persönlich betreffen, d. h. wenn nach der Transaktion Vorwürfe von Datenschutzverstößen gegen die Mitarbeiter erhoben werden, sind diese mit der Abwehr der Vorwürfe beschäftigt. Der resultierende Aufwand an Zeit, Geld und Nerven der Mitarbeiter (inkl. Zeugenaussagen) beeinträchtigt deren Arbeitskraft beim Erwerber.

Es handelt sich dabei keinesfalls um ein theoretisches Risiko, wenn man sich den Fall der Marriott-Hotelkette vergegenwärtigt, der im Juli 2019 von der britischen Datenschutzaufsichtsbehörde auf Basis der DSGVO beurteilt und im Rahmen einer „Absichtserklärung zur Verhängung einer Geldbuße" erstmals veröffentlicht wurde. Bei der 2016 von Marriott per Share Deal erworbenen Starwood-Hotelgruppe waren bereits ab 2014 Kundendaten unbemerkt aus den Systemen abgezogen worden. Der Grund hierfür waren IT-Sicherheitsmängel bei Starwood, die es Hackern ermöglichten, bis zur Aufdeckung 2018 unbemerkt in die Starwood-Systeme einzudringen und die Daten abzuziehen. Aus Sicht der britischen Aufsichtsbehörde ist es die (datenschutzrechtliche?) Aufgabe der Erwerbers im Rahmen eines Unternehmenskaufs, nicht nur den Bestand an personenbezogenen Daten, sondern auch die Sicherheitsmaßnahmen zu deren Schutz (einschließlich möglicher Sicherheitslücken) zu erforschen. Angesichts des zeitlichen Verlaufes, währenddessen zumindest zwei Jahre lang auch nach der Übernahme noch Daten abgezogen wurden, sodass auch Marriott (bzw. Star-

wood unter der Ägide von Marriott) die fortwirkenden (und eigentlich auch im Rahmen periodischer Überprüfungen auffälligen) Sicherheitsmängel weiterhin hätte abstellen müssen, musste der Fall aber eigentlich gar nicht unbedingt zu einem Due Diligence-Thema gemacht werden. Es bleibt ohnehin unklar, wie Ereignisse aus der Zeit vor dem Inkrafttreten der DSGVO noch zum Anknüpfungspunkt für Sanktionen unter der DSGVO herangezogen werden konnten. Nur dann, wenn nach dem 25. Mai 2018 noch weiterhin Daten abgezogen wurden, wäre dies ein DSGVO-Verstoß gewesen; aber dann hätte dies nichts mehr mit der Due Diligence des Jahres 2016 zu tun. Unabhängig von diesen Unklarheiten – und unter dem Vorbehalt der Übertragbarkeit in die deutsche „Rechtslandschaft" – zeigt der Fall aber, dass die zivilrechtliche (und organhaftungsrechtliche) Frage, inwieweit (und in welcher Detailtiefe) der Käufer eines Unternehmens zur Durchführung einer Due Diligence verpflichtet ist, nicht unbedingt mit der datenschutzrechtlichen Sichtweise korrelieren muss. Doch selbst eine originär datenschutzrechtliche Sichtweise auf das Thema Due Diligence muss erklären können, wie eine spezifische „Pflicht zur Due Diligence" beim Unternehmenserwerb aus der DSGVO herausgelesen werden kann: Nach der DSGVO ist vorrangig (oder ausschließlich?) entscheidend, ob der jeweilige Verantwortliche (vorher Starwood, nachher auch Marriott) DSGVO-konforme technische und organisatorische (Sicherheits-)Maßnahmen betreibt oder nicht. Die beim Share Deal betroffene Gesellschafterebene regelt das Datenschutzrecht eigentlich nicht – mit der noch unten beschriebenen Ausnahme, dass die Höhe verhängter Bußgelder auf den „Gesamtgruppenumsatz" abstellt.

Gleich, ob derartige Themen nun im Rahmen einer Due Diligence-Prüfung vertieft untersucht bzw. identifiziert werden, fällt das Risiko im vertragsrechtlichen Kontext eines SPA in die Kategorie der Compliance-Garantie(n). Kurz gesagt soll der Verkäufer garantieren, dass das Zielunternehmen stets im Einklang mit sämtlichen rechtlichen Anforderungen bzw. Regelungen geführt wurde. Dies schließt datenschutzrechtliche Vorschriften ein. In der Praxis werden derartige Garantien häufig zeitlich befristet („in den letzten fünf Jahren"), auf „wesentliche" Rechtsverstöße beschränkt (was immer das heißt) oder auf Verstöße verengt, von denen der Verkäufer (oder bestimmte Kenntnispersonen) Kenntnis hatte. Verletzungen der Garantie führen dann zu einer Ersatzpflicht hinsichtlich des aus der Datenschutzverletzung resultierenden Schadens. Dazu zählen im Grundsatz auch die (externen) Kosten, die durch die Abwehr von Ansprüchen oder behördliche Verfahren ausgelöst werden, wobei etwa die zum Schaden zählenden Anwaltskosten nur durch entsprechende Vereinbarung mit dem Verkäufer hinreichend sicher auch oberhalb der gesetzlichen Gebührenordnungen gefordert werden können. Ob auch Bußgelder zum Schaden zählen, ist nicht ganz eindeutig. Versicherungspolicen, die Garantieansprüche aus einem Unternehmenskauf absichern, umfassen regelmäßig keine Bußgelder.

Hinzu kommt, dass – dem EU-Kartellrecht folgend – im EU-Recht zunehmend die „Unternehmensgruppe“ und nicht mehr die einzelne Gesellschaft den Anknüpfungspunkt für Bußgeld-Höhen darstellen (sog. Funktionsträgerprinzip). Wenn 4% des „Gruppenumsatzes“ mehr als 20 Mio. EUR ausmachen, wird diese „Sippenhaft“ der Unternehmensgruppe, die als wirtschaftliche Einheit angesehen wird, relevant. Wird der Verstoß spätestens bis zum Unternehmenserwerb abgestellt, dürfte der Umsatz der Verkäufer-Unternehmensgruppe (inkl. der Zielgesellschaft) für Datenschutzverstöße bis zum Unternehmensübergang herangezogen werden. Denn die Verkäufer-Unternehmensgruppe (insbesondere deren „Muttergesellschaft“) hätte im Zeitpunkt des Verstoßes Pflicht und Möglichkeit gehabt, Verstöße zu verhindern. Es ist nicht ganz ausgeschlossen, dass alternativ (oder sogar daneben) auf den Zeitpunkt der „Bebußung“ (Verhängung der Geldbuße) abgestellt wird. Zumindest ist dies dann der Fall, wenn der Datenschutzverstoß über den Eignerwechsel hinaus andauert.

In einer Entscheidung des Europäischen Gerichts vom Juli 2018 betreffend Kartellrechtsverstöße wurden die parallele (gesamtschuldnerische) Haftung von Mutter- und Tochtergesellschaft bestätigt. Im Unternehmenskaufvertrag müsste also – neben Freistellungsansprüchen des Käufers gegenüber dem Verkäufer für den Fall, dass auch der Käufer für vergangene Verstöße in eine Mithaft genommen wird – die Verantwortung für „historische“ Datenschutzverstöße auf den Verkäufer konzentriert werden. Wird das Zielunternehmen auf die Geldbuße in Anspruch genommen, muss der Verkäufer diese übernehmen; wird der Verkäufer in Anspruch genommen, darf er keinen Innenregress gegenüber dem Zielunternehmen haben.

Praxistipp:

Bei der Verhandlung des SPA sollte ein Augenmerk auf die „Datenschutztauglichkeit“ der operativen Compliance-Garantie(n) gelegt werden. Dies betrifft sowohl den Garantietatbestand, also wann ein Garantiefall vorliegt, als auch die Rechtsfolgenseite, also welche Schäden ersetzt bzw. Freistellungen verlangt werden können. Dabei ist auch zu berücksichtigen, dass das Zielunternehmen bei einer großen Verkäufer-Unternehmensgruppe mit „exorbitanten“ Bußgeldern für zurückliegende Datenschutzverstöße belastet werden kann, weil der Gesamt-Gruppenumsatz für die Bemessung der Geldbuße maßgeblich ist.

Eine technische und rechtliche Datenschutz-Due-Diligence ist im Rahmen eines Erwerbs ebenfalls anzuraten, um die Übernahme von Altrisiken – unabhängig von der in einer entsprechenden (Compliance-)Garantie liegenden Versicherung durch den Verkäufer – zu minimieren.

Experten-Kontakt

Dr. Axel-Michael Wagner
Rechtsanwalt

E-Mail: a.wagner@psp.eu

Über PSP

Peters, Schönberger & Partner (PSP) zählt mit einer 40-jährigen, erfolgreichen Unternehmenshistorie zu den renommiertesten mittelständischen Kanzleien in Deutschland. Als Steuerberater, Wirtschaftsprüfer und Rechtsanwälte unterstützen wir Sie bei wichtigen Entscheidungen und begleiten Sie bei deren Umsetzung. Zu unseren Mandanten zählen mittelständische Unternehmen, Familienunternehmen, vermögende Privatpersonen und Private Equity-Gesellschaften, die den Wunsch nach einer interdisziplinären und individuellen Beratung haben. Sie finden in uns einen professionellen, verlässlichen und durchsetzungsstarken Partner, der mit Leidenschaft Ihre rechtlichen und steuerlichen Interessen vertritt und auch die klassischen Aufgaben der Wirtschaftsprüfer übernimmt. Das PSP-Family Office unterstützt Sie zudem bei der Vermögensstrukturierung und verfügt über ausgewiesene Expertise in Nachfolge-, Stiftungs- und Immobilienfragen.

PSP MÜNCHEN

PETERS, SCHÖNBERGER & PARTNER
RECHTSANWÄLTE
WIRTSCHAFTSPRÜFER
STEUERBERATER
www.psp.eu