

2. Datenschutzrechtliche Rahmenbedingungen

2.1. Einzelne Grundbegriffe

2.1.1. Personenbezogene Daten

Personenbezogene Daten sind nach Art 4 Z 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Es geht nach der DSGVO darum, Daten mit Bezug zu einem Menschen, soweit diese eine Person identifizieren oder identifizierbar machen, zu schützen. Wenn daher im Datenraum offengelegte Informationen ein Identifikationsmerkmal von Mitarbeitern, Lieferanten oder Kunden beinhalten (zB Name oder Geburtsdatum) oder wenn der Inhalt der Information oder der Kontext eine eindeutige Identifikation erlauben, aber auch, wenn diese Information zwar für sich genommen nicht ausreicht, um eine Person zuzuordnen, dies aber gelingt, sobald die Information mit weiteren Informationen verknüpft wird,²³ wären die Regelungen der DSGVO zu beachten. Hervorzuheben ist, ob des häufig anzutreffenden Arguments, doch nur Daten aus der beruflichen Sphäre der Betroffenen zu verarbeiten, dass es rechtlich völlig belanglos ist, dass aus der Sicht des Verantwortlichen weniger „heikle“ Daten Gegenstand sind oder aus welcher Sphäre die Informationen stammen (zB Intim-, Privat- oder Familiensphäre), da die Auswirkungen oder die Intensität der Beeinträchtigung auf die betroffene Person nach dem Verarbeitungszweck und Kontext, in dem die Verarbeitung erfolgt, unterschiedlich sein können.²⁴

Daraus folgt, dass nur dann, wenn kein Personenbezug hergestellt werden kann, die Offenlegung von Unterlagen im Datenraum völlig frei ist. Das wäre lediglich bei anonymen oder anonymisierten Daten der Fall. Soweit Daten nicht *a priori* anonym sind (spricht sich nicht auf eine identifizierte oder identifizierbare natür-

²³ Vgl Klar/Kühling in Kühling/Buchner (Hrsg), DS-GVO/BDSG² (2018) Art 4 Nr 1 Rz 18 f.

²⁴ Vgl dazu ausführlich Karg in Simitis/Hornung/Spiecker (Hrsg), Datenschutzrecht (2019) Art 4 Nr 1 Rz 22 ff.

2.1.2. Verarbeitung

Die DSGVO definiert in Art 4 Z 2 den Terminus „*Verarbeitung*“ zunächst abstrakt als „*jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten*“ und nennt im Weiteren beispielhaft Tätigkeiten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten. Daneben kennt die DSGVO auch noch den Begriff der Verarbeitungstätigkeit, die Anknüpfungspunkt des Verzeichnisses von Verarbeitungstätigkeiten nach Art 30 DSGVO⁴⁸ (im Folgenden kurz auch „*Verarbeitungsverzeichnis*“) ist. Die Verarbeitungstätigkeit ist nicht legaldefiniert und der unterschiedlichen Terminologie sollte auch nicht zu viel Bedeutung beigemessen werden. So nimmt auch die Mehrheit der Literaturmeinungen an, dass Verarbeitung und Verarbeitungstätigkeit synonym verwendet werden können.⁴⁹

Hervorzuheben ist, dass dem Begriff des Übermittels gegenüber der Regelung im DSG 2000 keine eigene Bedeutung mehr zukommt. Vielmehr ist dieser ein Unterfall der Offenlegung. Offenlegung ist ein Oberbegriff für alle Vorgänge, durch die der Verantwortliche personenbezogene Daten anderen Stellen in der Weise zugänglich macht, dass diese Kenntnis vom Informationsgehalt der betreffenden Daten erlangen können. Unerheblich für das Vorliegen eines rechtfertigungsbedürftigen Vorgangs ist, ob die Daten an einen Dritten, einen Auftragsverarbeiter oder auch nur an Personen, die unter der Verantwortung des Verantwortlichen arbeiten, weitergegeben werden.⁵⁰ Von der Offenlegung werden damit drei Aktivitäten erfasst:

- (i) das Übermitteln, worunter die gezielte Weitergabe von Daten an einen anderen zu verstehen ist,
- (ii) die Verbreitung als Gegenstück zur Übermittlung, weil darunter die ungezielte Weitergabe an einen unbestimmten Empfängerkreis verstanden wird,
- (iii) und zuletzt die Bereitstellung als eher passive Form des Offenlegens, die es anderen möglich macht, durch eigenes Tätigwerden auf die Daten zuzugreifen (zB durch die Ermöglichung der Abfrage einer Datenbank, einer Website oder eines Internet-Forums).

Auf Basis der Datenschutz-RL wurde noch davon ausgegangen, dass die bloße Bereithaltung zum Abruf noch keine Übermittlung bedeutet; diese sollte erst dann vorliegen,

48 Art 30 Abs 1 DSGVO: „*Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.*“

49 Vgl zB *Bertermann in Ehmann/Selmayr* (Hrsg), DS-GVO² (2018) Art 30 Rz 7; *Hartung in Kühling/Buchner*, DSGVO, Art 30 Rz 15; *Petri* trifft eine Unterscheidung dahin, dass eine Verarbeitungstätigkeit eine gewisse zeitliche Kontinuität aufweist, während eine Verarbeitung eher punktuell geschieht (in *Simitis/Hornung/Spiecker* [Hrsg], Datenschutzrecht [2019] Art 30 Rz 16).

50 Vgl *Herbst in Kühling/Buchner* (Hrsg), DS-GVO/BDSC² (2018) Art 4 Nr 2 Rz 29.

Sowohl das Fehlen einer Vereinbarung als auch die Nichterfüllung dieser Anforderungen ist gemäß Art 83 Abs 4 lit a DSGVO bußgeldbewehrt, weshalb unbedingt zu empfehlen ist, die Rollenverteilung zwischen Verkäufer und Interessenten *ab initio* zu definieren und die rechtlichen Folgen daraus abzuleiten. Im weiteren Verlauf der Vorbereitung des M&A-Deals wäre dann noch, bevor der Datenraum öffnet, die Unterfertigung einer solchen Vereinbarung angezeigt. Es wird sich dabei in den meisten Sachverhaltskonstellationen um die sehr ähnliche oder gar idente Aufgabenverteilung zwischen dem Verkäufer auf der einen Seite und den Käufern auf der anderen Seite handeln, weshalb sich empfiehlt, eine Vereinbarung nach Art 26 DSGVO schon zu Beginn des Aufeinandertreffens der Parteien – wie auch die Geheimhaltungsvereinbarungen oder Absichtserklärungen – als vom Verkäufer vorformulierten Standardvertrag zu unterfertigen.¹⁸⁴ Einzelheiten, die sich innerhalb der Interessenten unterscheiden, könnten in einem Sideletter dazu angepasst werden.

Als nächster Schritt muss jede Transaktionspartei die ihr zugewiesenen Aufgaben vorbereiten und umsetzen (zB Information nach Art 13 und 14 DSGVO). Erst wenn diese Vorbereitungshandlungen geleistet wurden, dürfte die Datenverarbeitung initiiert werden. Hervorzuheben ist zuletzt an der Stelle, dass die Annahme der gemeinsamen Verantwortung nicht von einer Rechtsgrundlage für die Übermittlung entbindet.¹⁸⁵ Es muss vielmehr jede beteiligte Partei nichtsdestotrotz für sich eine Rechtsgrundlage der Verarbeitung (wie bereits erörtert zum einen für die Offenlegung der Daten im Datenraum und zum anderen für die Bewertung und Verarbeitung im Due-Diligence-Bericht) definieren.¹⁸⁶

3.2.5. Der Verantwortliche bei der Prüfung der Dokumente in der zweiten Due-Diligence-Phase

Den Datenempfänger treffen als weiteren Verantwortlichen selbstredend, wie bereits erwähnt, dieselben Verpflichtungen wie den originären Verantwortlichen. Die beschriebene Informationsasymmetrie in einer Akquisitionssituation verlangt, dass der Interessent Details zum Kaufgegenstand anfragt, die ihm die Bewertung der wirtschaftlichen Lage, der Rechtsverhältnisse und der Risiken daraus ermöglichen, um eine Kaufentscheidung treffen und eine Kaufpreiskalkulation vornehmen zu können. Die Interessen von Käufer und Verkäufer verhalten sich damit zueinander reziprok, weshalb zur Vermeidung von Wiederholungen auf die Ausführungen unter den Punkten 3.2.2. und 3.2.3.3. hinsichtlich der Rechtsgrundlage des Art 6 Abs 1 lit f DSGVO verwiesen werden kann. Genau diese Ge-

184 Vgl *Tribess/Spitz*, Datenschutz im M&A Prozess, GWR 2019, 261 (262), die die Unterfertigung eines eigenen Dokuments nicht als notwendig erachten und die Aufnahme der relevanten Bestimmungen in die Geheimhaltungsvereinbarung oder den Letter of Intent vorschlagen.

185 Vgl EuGH 29.7.2019, C-40/17, *Fashion ID*.

186 Vgl dazu Punkt 3.2.2.

3.2.7.1. Risiken in einem VDR

Art 32 Abs 1 DSGVO verlangt sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter, dass diese jeweils unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete TOM treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Als Maßnahmen nennt die DSGVO beispielhaft:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, und
- d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung.

Die Maßnahmen müssen im Sinne dieses risikobasierten Ansatzes den speziell in einem Datenraum drohenden Risiken gerecht werden. Zur Beurteilung, welche Maßnahmen zu treffen sind, ist somit eine Risikoanalyse vorzunehmen.²¹⁷ In einer Risikoanalyse wird versucht, die Informationssicherheitsrisiken zu erkennen und zu bewerten und so das Gesamtrisiko zu ermitteln. Ziel ist es, in weiterer Folge dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.²¹⁸

In der ersten Due-Diligence-Phase besteht das größte Risiko darin, dass fremden Personen Zugang zu Daten gewährt wird und die Weiterverarbeitung nur begrenzt kontrolliert werden kann. Soweit es um die heute beinahe anachronistisch anmutenden Datenräume in Hotelzimmern oder anderen Räumlichkeiten, wie den Besprechungszimmern einer Anwaltskanzlei, geht, ist das Risiko noch eher vernachlässigbar, wenn Unterlagen nicht vervielfältigt werden dürfen (zB durch Kopie oder Fotografie). Die Digitalisierung hat jedoch auch vor Unternehmenstransaktionen nicht Halt gemacht, weshalb physische Datenräume aus dem M&A-Alltag beinahe verschwunden sind und durch virtuelle Datenräume (VDR) ersetzt werden. Dabei werden verkäuferseitige Dokumente eingescannt und auf der Website eines entsprechenden Anbieters online zur Verfügung gestellt.²¹⁹

217 Vgl *Jahnel*, Datensicherheit und Datengeheimnis, in *Jahnel/Sieglwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 90.

218 *Bundeskanzleramt/Informationssicherheitsbüro*, Österreichisches Informationssicherheitshandbuch (2019) 94 (<https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf>, zuletzt abgefragt 29.2.2020).

219 Vgl *Hasenauer/Stingl*, Due Diligence – Praxisleitfaden für Transaktionen (2015) 59.

3.2.8. Auftragsverarbeitung im Datenraum

3.2.8.1. Anforderungen an die Auftragsverarbeitung

Art 28 Abs 1 DSGVO regelt das Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter; Art 4 Z 8 DSGVO determiniert den Begriff des Auftragsverarbeiters. Wie bereits oben ausgeführt, geht es darum, dass der Auftragsverarbeiter als quasi verlängerter Arm im Auftrag des Verantwortlichen tätig wird. Damit eine solche Auslagerung der Verarbeitungstätigkeit nicht zu einem Unterschreiten des Datenschutzstandards, der beim Verantwortlichen gälte, führt, regelt Art 28 DSGVO verschiedene Anforderungen an eine solche Konstellation.

So hat sich der Verantwortliche nach Art 28 Abs 1 DSGVO davon zu überzeugen, dass der Auftragsverarbeiter Garantien dafür bietet, dass geeignete TOM so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Außerdem darf ein Auftragsverarbeiter nur herangezogen werden, wenn dieser bereit ist, eine schriftliche Vereinbarung gemäß Art 28 Abs 3 DSGVO abzuschließen. Zur Schriftform ist zu erklären, dass nach herrschender Meinung nicht erforderlich ist, dass ein elektronisch abgefasster Auftragsverarbeitungsvertrag mit einer (die Unterschrift ersetzenden) qualifizierten elektronischen Signatur versehen sein muss, insoweit wird kein Unterschriftserfordernis angenommen.²⁴³ Es sollte nach dieser überzeugenden Rechtsansicht genügen, dass Auftragsverarbeitervereinbarungen der Datenraumanbieter, die häufig standardisiert (ähnlich den allgemeinen Geschäftsbedingungen oder Nutzungsbedingungen) zur Verfügung gestellt werden und nicht individuell verhandelbar sind, bei der Beauftragung durch Anklicken einer Tickbox akzeptiert werden. Zu achten ist allerdings darauf, dass – wie auch bei allen anderen Vertragsformblättern – der Leistungsgegenstand unter Umständen erst definiert werden muss. So proklamiert Art 28 Abs 2 DSGVO, dass Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Betroffenenkategorien festzulegen sind. Es ist daher entsprechend detailgetreu die Zweckbestimmung der beauftragten Datenverarbeitung zu beschreiben.²⁴⁴ Diese kann aber naturgemäß je nach Target und Art der Transaktion – abhängig auch vom Inhalt der Due-Diligence-Daten und daher der Branche und der Geschäftstätigkeiten des Unternehmens – divergieren, weshalb dafür keine standardisierten Floskeln übernommen werden sollten, sondern die Beschreibung individuell vorzunehmen ist.

243 Vgl *Fritz*, Der Auftragsverarbeiter im Fokus der DS-GVO, in *Jahnel* (Hrsg), Datenschutzrecht-Jahrbuch 2017 (2017) 9 (24) mwN; *Hartung* in *Kühling/Buchner* (Hrsg), DS-GVO/BDSG² (2018) Art 28 Rz 95, der dies mit der Pflicht zur autonomen Auslegung des Begriffs der Schriftform in einem Unionsrechtsakt begründet. AA etwa *Spanberger* in *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg), Datenschutzgrundverordnung (2017) Art 28 Anm 21, der die Schriftform gemäß § 886 ABGB auslegt.

244 Vgl *Hartung* in *Kühling/Buchner* (Hrsg), DS-GVO/BDSG² (2018) Art 28 Rz 65.

4. Datenverarbeitung nach Signing und/oder Closing

4.1. Zulässigkeit der Übermittlung von Daten im Rahmen des Signing/Closing

Nach dem Ende der zweiten Phase der Due Diligence und wenn sich der Verkäufer mit einem Interessenten über den Kaufpreis und die sonstigen Konditionen des Unternehmenskaufvertrags einig geworden ist, wird die Transition der Geschäftsunterlagen, Dokumente und sonstigen relevanten Daten beginnen, soweit dies Gegenstand des Kaufvertrags ist. Dazu zählen naturgemäß auch personenbezogene Daten und in diesem Stadium kann mit etwa einer pseudonymisierten Liste der Arbeitnehmer das Auslangen nicht mehr gefunden werden. Als Zweck der Übermittlung im Rahmen des Signing und/oder Closing einer M&A-Transaktion ist nämlich im Gegensatz zum Zweck der Due Diligence nicht die Erlangung von Informationen durch Kaufinteressenten zur Bewertung des Kaufgegenstands, sondern die Weitergabe der Informationen an den einzelnen Rechtsnachfolger zur Fortführung des Unternehmens und zur fortgesetzten Erfüllung der übertragenen Vertragsverhältnisse sowie zur Aufrechterhaltung der Geschäftsbeziehungen zu konstatieren. Zu beschreiben ist unter dem Zweck für diese Verarbeitungstätigkeit der Kaufgegenstand (etwa das ganze Unternehmen oder nur ein Teilbetrieb) und außerdem, ob es sich bei der rechtlichen Ausgestaltung der Struktur um eine Gesamt- oder Einzelrechtsnachfolge handelt. Dies ist deshalb wichtig (siehe dazu Punkte 4.3. und 4.4.), da die Rechtsgrundlage im Sinne des Art 6 Abs 1 DSGVO und, soweit lit f anwendbar ist, die Argumentation des berechtigten Interesses an der Verarbeitung davon abgeleitet sind, ebenso wie sich die Beurteilung der Verhältnismäßigkeit der Verarbeitung der Daten nach Maßgabe der Datenschutzgrundsätze des Art 5 DSGVO danach richtet.

4.2. Unternehmenserwerb durch Umstrukturierungen

Als erste Ausgestaltung einer Unternehmenstransaktion, die für die datenschutzrechtliche Beurteilung der Zulässigkeit der Weitergabe von Daten relevant ist, soll die Umgründung eines Unternehmens erwähnt werden. Der Begriff Umgründung bezeichnet Vorgänge, bei denen sich der Rechtsträger eines Unternehmens ändert, sein Vermögen jedoch grundsätzlich unverändert fortbesteht. Egal ob Spaltung (§ 1 SpaltG), Verschmelzung (§ 219 AktG) oder übertragende Umwandlung (§ 1 UmwG) – diese Umgründungsformen gehen in Österreich mit einer

Soweit jedoch der Vertragspartner vom Altgläubiger und/oder Neugläubiger rechtzeitig über die Vermögensübernahme samt Vertragsverhältnissen informiert wird und dieser damit die Möglichkeit bekommt, einen Wechsel des Vertragspartners durch Beendigung des Vertragsverhältnisses (soweit dies die Kündigungsmöglichkeiten erlauben oder durch den Wechsel des Vertragspartners ein außerordentlicher Kündigungsgrund realisiert würde) zu verhindern, können bei Nichtäußerung eines Widerspruchs solche Umstände argumentiert werden,³¹⁰ die schutzwürdige Interessen des Betroffenen offenbar nicht verletzen. Wenn Kunden nämlich eine Übertragung ihrer Vertragsverhältnisse wünschen, darf man regelmäßig auch unterstellen, dass die Kunden entweder konkludent dem Übergang ihrer Daten zustimmen oder hiergegen keine Einwände haben, da sie an der Fortsetzung des Vertragsverhältnisses interessiert sind.³¹¹

Die für die Berufung auf Art 6 Abs 1 lit f DSGVO notwendige Möglichkeit zum Widerspruch räumt nicht zuletzt ohnedies § 38 UGB ein; so kann der Vertragspartner nach § 38 Abs 2 UGB der Übernahme seines Vertragsverhältnisses binnen dreier Monate nach Mitteilung davon sowohl gegenüber dem Veräußerer als auch gegenüber dem Erwerber widersprechen, wobei die Vertragsbeziehung dann mit dem Veräußerer weiter bestehen würde. Die Wendung in Abs 2 des § 38 UGB letzter Satz „*im Falle eines wirksamen Widerspruchs besteht das Vertragsverhältnis mit dem Veräußerer fort*“ bedeutet daher, dass der Vertrag durch einen erklärten Widerspruch rückwirkend auf den Veräußerer zurückfällt.³¹²

Im Informationsschreiben an den Vertragspartner, das vom Verkäufer des Vermögens versendet wird, könnte dies folgendermaßen beschrieben sein:

Informationsschreiben

[...] Damit der Vertrieb unverändert fortgeführt werden kann und insbesondere Ihre Verträge und Ihre sonstigen Geschäftsbeziehungen zu uns aufrechterhalten sowie die Bestellungen für Sie in gleicher Art und Weise abgewickelt werden können, müssen Ihre Daten aus Ihrer Geschäftsbeziehung mit uns [*das sind: Auflistung der Datenarten*] weitergegeben werden. Wenn Sie eine solche Fortführung der Geschäftsbeziehungen mit unserem Rechtsnachfolger ablehnen und keine weitere Kontaktaufnahme wünschen, bitten wir Sie, uns dies bis zum 1.1.2022 durch ein kurzes E-Mail unter abc@datenschutz.at mitzuteilen.

Wir führen für die Verarbeitung der Daten unsere berechtigten Interessen und die des Erwerbers nach Art 6 Abs 1 lit f DSGVO ins Treffen, die darin bestehen, dass der Verkauf des Teilbetriebs die Übertragung der Kunden-

310 Vgl Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24.5.2019, wonach bei laufenden Verträgen die zivilrechtliche Genehmigung genügt und ansonsten das Opt-out-Modell (Widerspruchslösung) befürwortet wird.

311 Vgl Schröder in *Forgó/Helfrich/Schneider* (Hrsg), *Betrieblicher Datenschutz*³ (2019) 670, Rz 38.

312 *Dehn* in *Torggler* (Hrsg), *UGB*³ (2019), § 38 UGB Rz 56.

4.4.2. Veräußerung von Kundendatenbanken innerhalb eines Betriebs

Wenn kein aufrechtes Vertragsverhältnis besteht und nur Kundendaten übertragen werden – und zwar insoweit, als Kundendaten zu bereits beendeten Vertragsbeziehungen oder Kundendaten ohne jede Beziehung zu den früheren Vertragsverhältnissen, um sie für ähnliche oder ganz andere Zwecke zu vermarkten, veräußert werden sollen³¹⁷ –, kommt die Rechtsgrundlage des Art 6 Abs 1 lit b DSGVO nicht in Betracht. Art 6 Abs 1 lit b DSGVO stellt für die Zulässigkeit der Datenverarbeitung nämlich auf die Erfüllung eines Vertrags mit dem Betroffenen ab. An einer solchen vertraglichen Grundlage fehlt es jedoch in den vorliegenden Sachverhaltskonstellationen. Als Rechtsgrundlage kommt neben der stets möglichen Rechtsgrundlage der Einwilligung des Betroffenen das Vorliegen berechtigter Interessen gemäß Art 6 Abs 1 lit f DSGVO in Betracht.

Ob der Veräußerer zur Weitergabe der Daten durch seine berechtigten Interessen oder die des Erwerbers legitimiert ist, hängt insgesamt von der Ausgestaltung des Deals ab und ist vor allem davon abhängig, welche Kategorien von Kundendaten in welchem Umfang zu welchem Zweck übertragen werden sollen. Im Rahmen der bei diesem Erlaubnistatbestand gebotenen Interessenabwägung sind die berechtigten Interessen des Verkäufers und des Erwerbers mit den schutzwürdigen Interessen der betroffenen Kunden im Einzelfall abzuwägen.

4.4.2.1. Altdaten

Soweit nun kein aufrechter Vertrag mit dem Kunden, dessen Daten weitergegeben werden, besteht, muss ein anderer Tatbestand des Art 6 DSGVO als Rechtsgrundlage der Übermittlung argumentiert werden. Prinzipiell kann eine Datenverarbeitung auch dann stattfinden, wenn diese zur Wahrung der berechtigten Interessen des Verkäufers als Verantwortlichen erforderlich ist, allerdings nur dann, wenn nicht die Interessen oder Grundrechte der betroffenen Personen überwiegen (Art 6 Abs 1 lit f DSGVO). Art 6 Abs 1 lit f DSGVO ist ein Auffangtatbestand, der im Gegensatz zur früheren Rechtslage in Österreich³¹⁸ keine Anwendungsfälle – auch nicht beispielhaft – vorgibt. Um diesem Tatbestand Konturen zu verleihen,

³¹⁷ Vgl. Schröder in *Forgó/Helfrich/Schneider* (Hrsg.), *Betrieblicher Datenschutz*³ (2019) 670 Rz 39.

³¹⁸ § 8 Abs 3 DS-G 2000 BGBl I 1999/165 idF BGBl I 2015/132: „Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten, 1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder 2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder 3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder 4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist oder 5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder 6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat oder 7. im Katastrophenfall, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist; im letztgenannten Fall gilt § 48a Abs. 3.“

8. Praxistipps

8.1. Checkliste zur Abgrenzung der Rollen in komplexen Datenverarbeitungsstrukturen

Fragen zur Qualifikation als Auftragsverarbeiter gemäß Art 28 DSGVO ⁴⁷²		
Ist das wesentliche Element der Dienstleistung auf die Verarbeitung personenbezogener Daten für die Zwecke eines Verantwortlichen (Datenverarbeitung ist der zentrale Gegenstand der Beauftragung) gerichtet?	Ja	Nein
Ist die Datenverarbeitung lediglich eine Nebentätigkeit zur Erfüllung des Auftrags (zB Post- und Transportdienstleistungen)?	Ja	Nein
Besteht ein eigenes Interesse des Dienstleisters an den Daten?	Ja	Nein
Legt das „beauftragende“ Unternehmen (Auftraggeber) die Zwecke und Mittel der Verarbeitung im Wesentlichen selbst fest?	Ja	Nein
Bestimmt der Auftraggeber über das technische Tool?	Ja	Nein
Legt der Auftraggeber den Umfang der Datenverarbeitung (Inhalt, Datenkategorien, Zweck, Übermittlungsempfänger) fest?	Ja	Nein
Hat der Dienstleister ausschließlich eine (technische) Hilfs- oder Unterstützungsfunktion?	Ja	Nein
Trifft der Dienstleister Entscheidungen, legt er Dinge fest oder beschließt er eigenständig?	Ja	Nein
Spricht der Auftraggeber nur Empfehlungen mangels fachlicher Kenntnisse aus, die der Dienstleister dann eigenverantwortlich umsetzt?	Ja	Nein

472 Vgl. dazu *Bitkom*, Begleitende Hinweise zu der Anlage Auftragsverarbeitung, 17 ff (<https://www.bitkom.org/sites/default/files/file/import/170515-LF-Auftragsverarbeitung-online.pdf>, zuletzt abgefragt 10.11.2019).

10. Ausfolgung und Löschung der Daten

- 10.1. Mit Schließung des VDR oder früher nach Aufforderung durch den Verantwortlichen A – spätestens mit Beendigung des Hauptvertrags – hat der Auftragsverarbeiter B sämtliche in seinen Besitz gelangten Daten, Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, einschließlich Sicherungskopien, dem Verantwortlichen A auszuhändigen oder nach Weisung des Verantwortlichen A datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- 10.2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter B entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. [Schlussbestimmungen]

8.4. Musterbestimmungen für eine Vereinbarung über eine gemeinsame Verantwortlichkeit

Vereinbarung über eine gemeinsame Verantwortlichkeit gemäß Art 26 DSGVO

abgeschlossen zwischen Verantwortlichem A, Datenschutz-Straße 11, 1220 Wien (im Folgenden auch der „**Verantwortliche A**“ oder nur „**A**“) und Verantwortlichem B, Datenraum-Gasse 1, 1010 Wien (im Folgenden auch der „**Verantwortliche B**“ oder nur „**B**“) wie folgt:

Präambel

[Beschreibung von A und B; Beschreibung Funktion des Datenraums und der Transaktion laut zB einem Letter of Intent]

Mit der vorliegenden Vereinbarung legen Verantwortlicher A und Verantwortlicher B für die Bereiche, in denen sie aufgrund ihrer jeweiligen tatsächlichen Funktionen und Beziehungen *[zB nach Maßgabe des Letter of Intent vom 2.2.2020]* gemäß Art 26 Abs 1 Satz 2 DSGVO in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß Art 13 und 14 DSGVO nachkommt.

Dies vorausgeschickt, vereinbaren der Verantwortliche A und der Verantwortliche B (im Folgenden gemeinsam auch die „**Vertragsparteien**“ oder einzeln eine „**Vertragspartei**“) wie folgt: