– etwa bei der automatischen Ablehnung eines Online-Kreditantrags[62] – sondern ein „grundsätzliches Verbot" beinhaltet.[63] Ebenso wie Art 9 Abs. 1 DS-GVO (vgl. Pkt. III. 2.) verfolgt das Verarbeitungsverbot nach Art. 22 Abs. 1 DS-GVO den Zweck, betroffene Personen vor besonderen Risiken für ihre Rechte und Freiheiten zu schützen, die mit der automatisierten Verarbeitung verbunden sind.[64] Mit Verweis auf Erwgr. 71 DS-GVO hebt der EuGH insbesondere die Schutzbedürftigkeit vor diskriminierenden Wirkungen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung hervor.[65] Angesichts des normativen Gleichlaufs der Schutzrichtungen von Art. 9 Abs. 1 und Art. 22 Abs. 2 DS-GVO ist zur Vermeidung von Wertungswidersprüchen ein einheitlicher Maßstab bei der Beurteilung des Durschlagens von Verstößen auf die Wirksamkeit des Vertrags anzulegen.

4. Verstöße gegen datenschutzrechtliche Strafnormen

Hauptanwendungsfall von § 134 BGB ist der Verstoß gegen Strafvorschriften.[66] Nach dem Urteil des BGH zur „Telekom Spitzelaffäre" führt ein Verstoß gegen die inhaltsgleiche Vorgängerregelung in § 44 iVm § 43 BDSG aA nach § 134 BGB zur Nichtigkeit eines Vertrags über die Auswertung von Verbindungsdaten aus Telefongesprächen durch einen Dienstleister.[67] Die Einordnung von Strafnormen als Verbotsnorm ist konsequent, nicht zuletzt weil die Missbilligung des wirtschaftlichen Erfolgs unmittelbar aus der Strafandrohung folgt.[68]

Auswirkungen auf M&A-Transaktionen können sich insbesondere bei der Veräußerung von GPS-Daten ergeben – zB bei der Übernahme einer Detektei nebst Kundendaten oder die Ver-

---

[62] ErwGr. 71 S. 1 DS-GVO.
[63] EuGH ECLI:EU:C:2023:957 Rn. 52 = NZA 2024, 45 Rn. 52.
[64] EuGH ECLI:EU:C:2023:957 Rn. 57 = NZA 2024, 45 Rn. 57.
[65] EuGH ECLI:EU:C:2023:957 Rn. 59 = NZA 2024, 45 Rn. 59.
[66] MüKoBGB/Armbrüster § 134 Rn. 67.
[67] BGH NJW 2013, 401 Rn. 20 ff.
[68] Vgl. zum Ganzen Staudinger/Fischinger/Hengstberger BGB § 134 Rn. 442 ff.

äußerung von Werbesegmenten. Insofern hat der BGH die verdeckte Erhebung von GPS-Daten zur Erstellung persönlicher Bewegungsprofile durch eine Detektei als Straftrat nach § 44 Abs. 1 iVm § 43 Abs. 2 Nr. 1 BDSG aF eingeordnet.[69] Werden Nutzerprofile mit GPS-Daten bei der Verwendung von nativen Apps aus mobilen Endgeräten erhoben und Betroffene nicht auf die Erfassung von GPS-Daten hingewiesen, ist aufgrund des Eindringens in befriedetes Besitztum in das Endgerät wie dem Anbringen eines GPS-Peilsenders an einem PKW[70] von einer qualitativ schwerwiegenden Beeinträchtigung der Privatsphäre auszugehen. Auch der EuGH hat in der Rechtssache „Child Focus" den besonderen Schutz von Standortdaten im Unionsrecht mit Blick auf die Vielzahl von Aspekten des Privatlebens der Betroffenen, einschließlich sensibler Informationen wie sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie den Gesundheitszustand anerkannt.[71]

IV. Folgen nichtiger M&A-Verträge

Soweit Verträge auf einer datenschutzrechtlich unzulässigen Übertragung personenbezogener Daten beruhen, die aufgrund des Verbotscharakters der verletzten Datenschutzvorschrift die Nichtigkeit des Vertrags nach § 134 BGB zur Folge haben, sind Regressansprüche aus Leistungskondiktion bei bereits erfolgter Zahlung regelmäßig nach § 817 S. 2 BGB gesperrt.[72] Dies gilt insbesondere dann, wenn beiden Vertragsparteien ein Verstoß gegen eine datenschutzrechtliche Verbotsnorm zur Last fällt.[73] Etwas anderes kann allenfalls gelten, wenn eine Vertragspartei bewusst über die Konformität mit den in Rede stehenden Datenschutzvorschriften – zB durch Vorlage von gefälschten Auditberichten –

---

[69] BGH NJW 2013, 2530 Rn. 33 ff.

[70] BGH NJW 2013, 2530 Rn. 93.

[71] EuGH ECLI:EU:C:2020:791 Rn. 117 = EuZW 2021, 209 Rn. 117 mAnm Sandhu.

[72] BGH NJW 2013, 401 Rn. 26.

[73] Vgl. OLG Frankfurt a.M. NJW-RR 2018, 887 Rn. 47 zu § 28 Abs. 3 BDSG aF.

getäuscht wurde. Für die Beurteilung einer Kondiktionssperre ist eine Bewertung im konkreten Einzelfall notwendig.

Vor diesem Hintergrund ist im Vorfeld der Erfüllung von Zahlungsverpflichtungen besonderes Augenmerk auf die Einhaltung der datenschutzrechtlichen Rechenschafts- und Dokumentationspflichten nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO zu legen, die in der EuGH-Rechtsprechung eine erhebliche Aufwertung erfahren haben (vgl. Pkt. V.1.).

V. Konsequenzen für M&A-Transaktionen

1. Risikofaktoren

Bei Assets-Deals können sich die Anforderungen an die Einhaltung der datenschutzrechtlichen Rechenschafts- und Dokumentationspflichten nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO risikoschärfend auswirken.

Der EuGH bestätigte, dass Verantwortlichen aus Art. 5 Abs. 2 und 24 Abs. 1 DS-GVO nicht nur die Pflicht zur Rechenschaft, sondern auch Pflichten zur Compliance, dh. zur Vorbeugung von Datenschutzverstößen erwachsen, weshalb sie präventiv wirksame Compliance-Management-Systeme etablieren, unterhalten und dokumentieren müssen.[74] Diese Compliance-Pflicht hat Konsequenzen für die Beurteilung von Verstößen gegen datenschutzrechtliche Verbotsnormen (vgl. Pkt. III.). Denn ohne Nachweis der Datenschutzkonformität etwa mit Art. 9 Abs. 1 oder Art. 22 Abs. 1 DS-GVO ist im Zweifel eine Verletzung der Verbotsnormen anzunehmen. Zwar trägt nach den allgemeinen Maßstäben der Anspruchsteller die Beweislast für die tatbestandlichen Voraussetzungen eines Verstoßes gegen ein Verbotsgesetz.[75]

Die nationalen Beweislastregelungen werden jedoch von den vorrangig anwendbaren Wertungen der DS-GVO als unmittelbar

---

[74] EuGH ECLI:EU:C:2022:833 Rn. 81 = ZD 2023, 28 Rn. 81.

[75] BGH NJW-RR 2002, 159 (160); NJW 1983, 2018 (2019); MüKoBGB/Armbrüster § 134 Rn. 197.

geltendes Unionsrecht überlagert. So obliegt den Verantwortlichen, dh beiden Parteien einer Transaktion, die Beweislast für die Rechtmäßigkeit der Datenverarbeitung. Bereits aus der Rechtssache C-175/20 („Valsts ieņēmumu dienests") ließ sich eine eindeutige Signalwirkung für den Umfang der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO entnehmen, die bislang in Deutschland stiefmütterlich behandelt wurde.[76] Der EuGH ordnet die Rechenschaftspflicht als prozessuale Beweislastumkehr zu Lasten des oder der Verantwortlichen ein.[77] Diese Beweislastverteilung erstreckt sich nach Ansicht des Gerichtshofs nicht nur auf den Kanon der Datenschutzgrundätze aus Art. 5 Abs. 1 DS-GVO, sondern auch auf die Einhaltung aller konkretisierenden Vorschriften, etwa Art. 25 Abs. 2 DS-GVO (Privacy by Default). Auch das BVerwG stellte fest, dass Art. 5 Abs. 2 DS-GVO nicht nur Rechenschaftspflichten des Verantwortlichen gegenüber der Behörde, sondern generell die Beweislast hinsichtlich der Einhaltung der Grundsätze aus Art. 5 Abs. 1 DS-GVO regele.[78] In der Folge hat der EuGH die Beweislastumkehr aus Art. 5 Abs. 2 DS-GVO zulasten von Verantwortlichen explizit auf die Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 lit. a) DS-GVO iVm Art. 6 Abs. 1 DS-GVO erstreckt[79] und auch gegenüber privaten Stellen anerkannt.[80]

Beide Entscheidungen bedingen ein straffes Arbeitsprogramm für Verantwortliche. Die abstrakten rechtlichen Vorgaben zu Compliance (Prävention), Nachweispflichten (Dokumentation) und Beweislastumkehr (Prozessrisiko) haben massive Auswirkungen auf Rückstellungen, Unternehmensbewertungen, Versicherbarkeit, Forschung & Entwicklung sowie die Haftung von Führungskräften. Abhilfe kann der Aufbau entsprechender Strukturen (z.B. Informationssicherheits- und Datenschutzmanagement) sowie deren sorgfältige Überwachung und kontinuierliche

---

[76] Vgl. zur Entwicklung im Datenschutzrecht Hense ZD 2022, 413 (414).

[77] EuGH ECLI:EU:C:2022:124 Rn. 77, 81 = ZD 2022, 271 Rn. 77, 81 ff.

[78] BVerwG NVwZ 2022, 1205 Rn. 47 ff.

[79] EuGH ECLI:EU:C:2023:373 Rn. 53 f. = ZD 2023, 606 Rn. 53 f.

[80] EuGH ECLI:EU:C:2023:537 Rn. 95, 152 = GRUR 2023, 1131 Rn. 95, 152.

Verbesserung nach dem PDCA-Zyklus schaffen (vgl. hierzu DSK, Standard-Datenschutzmodell, Version 3.0, S. 61 ff.).

Als maßgeblicher Risikofaktor bleibt festzuhalten: Was im Zuge eines Asset-Deals nicht ausreichend dokumentiert ist, kann zu schwer kalkulierbaren Nichtigkeitsfolgen und Prozessrisiken führen.

2. Mitigationsmaßnahmen für Due Diligence

Der Befund zur Qualifikation von Art. 9 Abs. 1 und Art. 22 Abs. 1 DS-GVO (vgl. III. 2.,3.) als Verbotsnormen iSv § 134 BGB nötigt zu tauglichen Mitigationsmaßnahmen in der Phase der Due Diligence bei der Prüfung der Assets.

Im Wesentlichen ist der Fokus auf zwei Gesichtspunkte zu legen. Einerseits ist die Prüfung ausreichender Dokumentationen zur Erfüllung der datenschutzrechtlichen Rechenschaftspflichten notwendig. Hierzu zählt neben der Evaluierung von Verfahrensverzeichnissen (Art. 30 DS-GVO), datenschutzrechtlichen Verträgen (Art. 26 und Art. 28 DS-GVO), Einwilligungserklärungen (Art. 9 Abs. 2 lit. a) iVm Art. 7 Abs. 1 DS-GVO) und etwaigen Auditberichten insbesondere die Beurteilung der Ergebnisse von Datenschutz-Folgenabschätzungen (DSFA). Nach Art. 35 Abs. 3 DS-GVO ist eine DSFA stets erforderlich bei automatisierten Verarbeitungen iSv Art. 22 Abs. 1 DS-GVO zur systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen sowie der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO. Dabei ist die Einhaltung einer validen Methodik – etwa einer Kombination von ISO/IEC 29134:2023 und dem Standard-Datenschutzmodell (Version 3.0) der Datenschutzkonferenz – unerlässlich für die Konformität mit den Anforderungen aus Art. 35 DS-GVO.

Andererseits sollte eine technische Prüfung der Datenbestände bei Transaktionen von Assets erfolgen. Dies gilt insbesondere im Bereich des Online-Marketing, bei dem die betreffenden Transaktionen Datensätze mit möglichen Ableitungen zu besonderen Kategorien personenbezogener Daten etwa in Nutzersegmenten enthalten können. Empfehlenswert ist die Durchführung eines sog. „data sensitivity audit" zur Analyse, ob in vorhandenen Da-

tenbanken und Datensätzen Art. 9-Daten enthalten sind.[81] Hierfür werden sich automatisierte Prozesse mithilfe von Machine Learning-Modellen etablieren. Kann man für diese sensiblen Daten keine Ausnahme aus Art. 9 Abs. 2 DS-GVO belasten, ist zu evaluieren, ob die Art. 9-Daten zu entfernen sind. Anderenfalls droht das Risiko einer vollständigen Rechtswidrigkeit des gesamten Datensatzes mit entsprechender Nichtigkeitsfolge der Transaktion.

VI. Fazit

Daten sind nicht per-se ein Asset. Selbstredend mag die Monetarisierung personenbezogener Daten attraktiv sein. Gleichzeitig ist es notwendig, bereits während der Due Diligence relevante datenschutzrechtliche Risiken frühzeitig zu identifizieren und zu eliminieren oder im Rahmen der Verhandlungen kaufpreismindernd zu berücksichtigen. Wenngleich die Bedeutung von Asset-Deals im Vergleich zu Share-Deals, denen in der Regel keine Nichtigkeitsfolgen drohen, noch gering ist, wird die Anzahl der Verwertung von Daten bei Unternehmenstransaktionen oder bei Veräußerungen im Zuge von Insolvenzverfahren und damit das Risiko für die Wirksamkeit entsprechender Verträge zunehmen.

Zur Vermeidung von Nichtigkeitsfolgen ist eine Akzentuierung der datenschutzrechtlichen Compliance während der Due Diligence ein probates Mittel, um dem Risiko von Verstößen gegen Verbotsnormen wie Art. 9 Abs. 1 und Art. 22 Abs. 1 DS-GVO nachhaltig entgegenzutreten.

---

[81] Herbrich jurisPR-ITR 17/2023 Anm 3.

Teil III: W&I-Insurances