Datenhändler – juristisch unbekannte Wesen?

Zur datenschutz- und strafrechtlichen Verantwortung der Datenvermittlung

Stand 06.03.2025

Thilo Weichert
weichert@netzwerk-datenschutzexpertise.de
Waisenhofstraße 41, 24103 Kiel
Karin Schuler
schuler@netzwerk-datenschutzexpertise.de
Kronprinzenstraße 76, 53173 Bonn
www.netzwerk-datenschutzexpertise.de

Inhalt

Personenbezogene Daten sind schon seit Langem Handelsware. Das Datenschutzrecht nimmt sich dieses Umstands nur mit Verzögerung an. Bisher ist weitgehend ungeklärt, wie die persönlichkeitsrechtlichen Beeinträchtigungen, die von Datenhändlern ausgehen, rechtlich eingehegt werden können.

1 Datenhändler als Phänomen

Das Anliegen des Datenschutzrechts ist es, die durch die Digitalisierung und Kommerzialisierung verursachten Beeinträchtigungen des allgemeinen Persönlichkeitsrechts und der Privatsphäre normativ in den Griff zu bekommen. Gegenüber Datenhändlern, die große Mengen personenbezogener illegal erlangter Daten vermitteln, ist das bis heute nicht gelungen.

1.1 Datenschutz steht in einem größeren Zusammenhang

Das Datenschutzrecht machte in seiner über 50jährigen Geschichte eine Vielzahl von Metamorphosen durch. Seine Ursprünge hat es im öffentlichen Recht und in der Abwehr übermäßiger hoheitlicher digitaler Eingriffe. Der Umstand der Verdatung von Verbraucherinnen und Verbrauchern zur zielgerichteten Adressierung von Werbung und zur Prüfung von deren Kreditwürdigkeit machte den Datenschutz zum zivilrechtlichen Abwehrrecht. Dieses richtete sich zunächst gegen Adresshändler und Auskunfteien, später auch gegen Handelsunternehmen. Dass Datenschutz zugleich Verbraucherschutz ist, wurde erst sehr viel später, in den 10er Jahren dieses Jahrhunderts rechtlich anerkannt. Die Entwicklung des Datenschutzes zum Beschäftigtenschutz hat demgegenüber ihre Ursprünge schon in den 70er Jahren des letzten Jahrhunderts. Doch diese Entwicklung blieb zäh, sowohl individualrechtlich als auch kollektivrechtlich, und sie ist bis heute nicht ausgereift. Die Verteidigung des Persönlichkeitsrechts gegen Internet-Plattformen, gegen Hatespeech und Fakenews hat eine 30jährige Geschichte. Lösungen sind jedoch auch hier allenfalls ansatzweise in Sicht. Die Schnittstellen zwischen Datenschutz und Informations-, Meinungsäußerungs- und Medienrecht verursachen bei der Rechtsanwendung seit Jahren Verunsicherung. Auch als Bestandteil des Wettbewerbsrechts kämpft der Datenschutz noch heute um Anerkennung. Die massive Digitalisierung aller Lebensbereiche führt zwangsläufig dazu, dass weitere **rechtliche Anpassungen** nötig sind, die durch Veränderung des normativen Rahmens oder durch dessen angepasste Auslegung erfolgen können.

Eine solche Anpassung erfolgte durch die Feststellung des Europäischen Gerichtshofs (EuGH), dass Internetplattformen eine eigenständige **Datenschutzverantwortlichkeit** zukommt. Dies hatte zur Folge, dass nicht auf Hilfskonstruktionen wie deren polizeirechtliche Behandlung als Störer zurückgegriffen werden musste.[1] Eine offene Flanke besteht bis heute darin, dass die persönlichkeitsrechtliche Relevanz von Software-Produkten keine eigenständige Würdigung gefunden hat. Die Produkthersteller werden rechtlich allenfalls als weisungsabhängige Auftragsverarbeiter behandelt, obgleich sie es meist selbst sind, die in heutigen Systemen die Art der Datenverarbeitung bestimmen und sie den formal verantwortlichen Kunden ohne deren Einflussmöglichkeit vorgeben.

[1] EuGH 05.06.2018 – C-210/16, NJW 2018, 2537.

Erst mit der KI-Verordnung[2] zeichnet sich die Anerkennung von Softwareprodukt-Anbietern als eigenständige Player auf dem Feld persönlichkeitsrelevanter Digitalisierung ab.

Noch überhaupt nicht vom Datenschutzrecht erfasst ist das **Phänomen der Datenhändler**. Diese vermitteln zumeist massenhaft personenbezogene Datensätze, ohne dass es eine klare Handhabe zu geben scheint, dass der mit dem Handel für die Betroffenen verursachte persönlichkeitsrechtliche Schaden durch das Datenschutzrecht verhindert werden kann.

1.2 Datenhändler in der Praxis

Im Juli 2024 veröffentlichte netzpolitik.org eine Recherche zum Datenhandel. Das Nachrichtenportal beschaffte sich unentgeltlich bei einem US-Datenhändler die Kostprobe von Datensätzen mit 3,6 Milliarden **Handy-Standortangaben** aus Deutschland. Diese stammten aus zwei Monaten von Ende 2023 und enthielten ca. 11 Millionen Advertising IDs (MAID) von Handynutzenden. Mit dieser ID konnte nachvollzogen werden, wo sich Handys entlang bewegten: im Büro, zu Hause, in der Natur; auf der Straße, in einer Entzugsklinik, in einem Gefängnis oder in einem Swinger-Klub. Vermittelt wurde diese Datenkostprobe von dem Online-Marktplatz Datarade, einem Start-up in Berlin. Gehandelt wurden dabei die Daten der US-Firma Datastream Group, die im monatlichen Abonnement die Standortdaten nach eigenen Angaben aus bis zu 163 Ländern anbietet – etwa für personalisierte Werbung. Die Datastream-Group firmiert inzwischen unter dem Namen Datasys. Zusätzliche Recherchen von netzpolitik.org und weiteren Medien ergaben, dass die Daten von Datastream von der litauischen Werbefirma „Eskimi.com“ in Vilnius bzw. das mit Eskimi eng verbundene Unternehmen Redmob stammten.[3] Die per MAID pseudonymisierten Bewegungsprofile waren kinderleicht konkreten Personen zuzuordnen, z. B. indem regelmäßige Standorte mit im Internet verfügbaren Telefonbuchangaben abgeglichen wurden.[4] So ließen sich z. B. Angehörige von Sicherheitsbehörden identifizieren.[5] Datarade vermittelt auch medizinische Informationen und Bonitätsauskünfte. Die genaue Herkunft der Daten ist oft unklar.[6]

Im Rahmen einer ähnlichen Recherche eines niederländischen Radios wird Datarade zitiert (übersetzt): „Als Plattform fungieren wir **nur als Vermittler**. Wir selbst verkaufen keine Datensätze. Datenhändler können ihre Datensätze auf unserer Plattform zum Verkauf anbieten, um mit Interessenten in Kontakt zu treten. Selbstverständlich lassen wir nur legale Inhalte auf unserer Plattform zu, wie es auch in unseren Allgemeinen Geschäftsbedingungen steht. … Datarade hält es für wichtig, gegen Rechtsverstöße vorzugehen.“[7] Und in einem englischsprachigen Blogbeitrag meint Datarade

[2] Verordnung über künstliche Intelligenz v. 13.06.2024, ABl. EU L v. 12.07.2024.
[3] Meineck/Dachwitz,Databroker Files: Diese EU-Firma soll Standortdaten aus Deutschland verkauft haben, 12.02.2025, https://netzpolitik.org/2025/databroker-files-diese-eu-firma-soll-standortdaten-aus-deutschland-verkauft-haben/.
[4] Meineck/Dachwitz, Databroker Files: Firma verschleudert 3.6 Milliarden Standortdaten von Menschen in Deutschland, 16.07.2024, https://netzpolitik.org/2024/databroker-files-firma-verschleudert-36-milliarden-standorte-von-menschen-in-deutschland/.
[5] Meineck/Dachwitz, Wie Datenhändler Deutschlands Sicherheit gefährden, 16.07.2024, https://netzpolitik.org/2024/databroker-files-wie-datenhaendler-deutschlands-sicherheit-gefaehrden/.
[6] Krempl, Sicherheitsrisiko: So einfach können Handy-Nutzer heimlich verfolgt werden, 12.01.2024, Kurzlink: https://heise.de/-9596230.
[7] Nachweis bei Meineck/Dachwitz, Databroker Files (Fn. 3); Originalzitat bei van den Berg, Nederlandse telefoons online stiekem te volgen: ‘Extreem veiligheidsrisico’, 10.01.2024,

(übersetzt): „So müssen Datenanbieter beispielsweise beweisen, dass sie Daten im Einklang mit der DSGVO […] beschaffen und dass sie alle PII (persönlich identifizierbare Informationen) aggregieren, um Datenschutz zu gewährleisten. Erst wenn ein Anbieter geprüft und zugelassen ist, kann er mit dem Verkauf von Daten über einen Datenmarktplatz beginnen.“[8]

Bei der Analyse der von netzpolitik.org erlangten Daten zeigte sich, dass die Daten offenbar aus **unterschiedlichen Quellen**, also von verschiedenen Apps stammten. Die Qualität der Daten erwies sich regelmäßig als hoch. Auch wenn diese nicht immer für jeden Einzelfall gewährleistet war.

Die **Nutzungsmöglichkeiten** der im Rahmen der Medienrecherche erlangten Daten ist auch jenseits des Einsatzes für Werbezwecke groß: Sie eignen sich zum Stalking, also dem beharrlichen Belästigen von Menschen, oder zum Doxing, dem Einschüchtern einer Person durch Veröffentlichung privater Informationen. ES ist zudem offenbar Praxis, dass Geheimdienste sich über den Weg des Datenhandels nachrichtendienstlich relevante Informationen beschaffen. Dies geschieht unter dem Kürzel ADInt (advertising based intelligence).[9] Auch Gefahrenabwehr- und Strafverfolgungsbehörden können Zugriff auf die vermittelten Daten nehmen. Die New York Times bekam 2019 die Standortdaten von mehr als 12 Millionen Smartphone-Nutzern zugespielt, die u. a. von Wetter-Apps und Kartendiensten erfasst worden waren. 2021 wurden der Zeitung weitere rund 100.000 Ortsinformationen vom Tag des Sturms auf das Kapitol am 06.01. über tausende Trump-Anhänger, Randalierer und Passanten mit MAIDs zugetragen. Zuvor war bekannt geworden, dass US-Behörden Bewegungsprofile, etwa von der Firma Anomaly Six, kaufen und ohne Richtergenehmigung nutzen.[10]

Anfang 2025 gab netzpolitik.org bekannt, dass es eine weitere über den Handel vermittelte Anzahl von Datensätzen erlangen konnte. Die Zusammenstellung stammte vom US-Datenhändler Datastream Group, bezog sich auf einen einzigen Tag im Juli 2024 und enthielt 380 Millionen Standortdaten aus 137 Ländern, die mit rund 40.000 verschiedenen Apps verknüpft waren. Deren Nutzende dürften nicht ansatzweise ahnen, was mit ihren Daten geschieht. Zu den **deutschen Datenlieferanten** mit metergenauen Standortdaten gehören die populären Apps Wetter Online, Focus Online, Kleinanzeigen und FlightRadar24. Über andere Apps wie web.de und gmx.de, Tinder, Grindr und Candy Crush Saga sowie Upday des Axel-Springer-Konzerns wurden die Nutzenden offenbar (nur) per IP-Adresse geortet, so dass eine Ortsunschärfe der Standortdaten im Kilometer-Bereich besteht.[11] Kurz zuvor war bekannt geworden, dass einer der bekanntesten US-Databroker, Gravy Analytics, offenbar Ziel eines

https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico. .

[8] Kelly, Ultimate Guide to The Data Marketplace in 2024, 29.11.2024, https://datarade.ai/company/blog/data-marketplaces.

[9] Meineck/Dachwitz, Wie Datenhändler Deutschlands Sicherheit gefährden (Fn. 5); Sosna, "Fundgrube Internet" - vom tatsächlich möglichen und rechtlich zulässigen Sammeln der Nachrichtendienste im Netz, Zeitschrift für das Gesamte Sicherheitsrecht 2024, 53 ff.; Wetzling/Ruckerbauer, Informationsbeschaffung mit der Kreditkarte, 28.05.2024, https://www.interface-eu.org/publications/nachrichtendienstliche-datenkaeufe; Meineck/Dachwitz, ADINT – gefährliche Spionage per Online-Werbung, 19.07.2024, https://netzpolitik.org/2024/databroker-files-adint-gefaehrliche-spionage-per-online-werbung/.

[10] Krempl, Sicherheitsrisiko (Fn. 6).

[11] Meineck/Dachwitz, Neuer Datensatz enthüllt 40.000 Apps hinter Standort-Tracking, 15.01.2025, https://netzpolitik.org/2025/databroker-files-neuer-datensatz-enthuellt-40-000-apps-hinter-standort-tracking/.

Hackerangriffs war und gigantische Mengen durch populäre Handy-Apps gesammelte Standortdaten verloren gingen.[12]

Ein weiteres Beispiel für einen Datenhändler ist Xandr, der einen der größten Datenmarktplätze der Werbewelt betreibt. **Xandr** wurde 2022 durch Microsoft vom US-Telekommunikationsanbieter AT&T für angeblich über eine Milliarde Dollar übernommen und 2023 in Microsoft Monetize (Supply-Side-Plattform), Microsoft Invest (Demand-Side-Plattform) und Microsoft Curate (Marktplatz für Daten plus Inventar) aufgeteilt und umbenannt.[13] Eine öffentlich zugängliche Angebotsliste von Xandr, datiert vom Mai 2021, enthielt 651.463 unterschiedliche Merkmalskategorien aus teilweise höchst sensitiven Bereichen wie Gesundheit, Politik, Finanzen, persönlichen Charakteristiken, Beschäftigung, Interessen, Ethnie, Religion und Demografie (Alter, Geschlecht, Wohnort).[14]

Gemäß eigenen Angaben hatte Xandr 2022 alle 1.294 **Auskunftsersuchen** nach Art. 15 DSGVO abgelehnt, ebenso wie alle 660 **Löschanträge**. Xandr begründete sich jeweils damit, man habe die Identität der Antragstellenden nicht verifizieren können.[15]

1.3 Hilflose Aufsicht

Offensichtlich sind die oben dargestellten Datenverkäufe datenschutzrechtlich unzulässig. Sie beruhen zumeist auf der Behauptung, die Betroffenen hätten eine **Einwilligung** für den Datenverkauf erteilt. Für eine wirksame Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7 DSGVO) muss die Voraussetzung erfüllt sein, dass der Betroffene über Daten, Zwecke und Empfänger informiert ist, bevor er seine Erklärung abgibt.[16] Weder die Empfänger noch die von diesen verfolgten Zwecke sind aber bei den dargestellten Vermittlungen zum Zeitpunkt der Datenerhebung festgelegt. Es kommt hinzu, dass der Weg von der Datenerhebung bis zur Datennutzung zumeist über mehrere Stationen erfolgt, bei denen die Datensätze oft kombiniert oder angereichert werden. Dies führt dazu, dass, selbst wenn man das Kleingeschriebene von App-Nutzungsbedingungen und die Einwilligungserklärungen durch App-Nutzung generell akzeptieren würde, die konkreten „Einwilligungen“ unwirksam sind.

Genauso wenig kommt als Legitimation der Rückgriff auf ein „**berechtigtes Interesse**“ (Art. 6 Abs. 1 lit. f DSGVO) in Frage. Dem stehen in jedem Fall überwiegende „Interessen oder Grundrechte und Grundfreiheiten“ der Betroffenen entgegen.[17]

---

[12] Meineck/Dachwitz, Hacker wollen Bestände von US-Databroker veröffentlichen, 09.01.2025, https://netzpolitik.org/2025/gigantisches-daten-leak-droht-hacker-wollen-bestaende-von-us-databroker-veroeffentlichen/.

[13] Microsoft nimmt Abschied von der Marke Xandr, 20.06.2023, https://www.adzine.de/2023/06/microsoft-nimmt-abschied-von-der-marke-xandr/.

[14] Dachwitz, Das sind 650.000 Kategorien, in die uns die Online-Werbeindustrie einsortiert, FIfF-Kommunikation 3/2023, 59 ff. = 08.03.2023, https://netzpolitik.org/2023/microsofts-datenmarktplatz-xandr-das-sind-650-000-kategorien-in-die-uns-die-online-werbeindustrie-einsortiert/.

[15] Biselli, Xandr verweigert jede Datenauskunft, 09.07.2024, https://netzpolitik.org/2024/beschwerde-von-noyb-xandr-verweigert-jede-datenauskunft/.

[16] Vgl. ErwGr 32 DSGVO; EuGH 01.10.2019 – C-673/17 Rn. 58, NJW 2019, 3433 (Planet 49); EuGH 11.11.2020 – C-61/19 Rn. 37, NJW 2021, 841 (ANSPDCP); Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2024, Art. 4 Rn. 114.

[17] EuGH 04.07.2023 – C-252/21 Rn. 117, NJW 2023, 2997 (Meta Platforms), Ehmann in Simitis/Hornung/Spiecker, Datenschutzrecht, 2. Aufl. 2025, Art. 6 Anhang 3 Rn. 41.

Die Leiterin der für Datarade zuständigen **Datenschutzaufsichtsbehörde**, die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) Meike Kamp meinte, sie habe keine Handhabe gegen das Unternehmen auf der Grundlage der DSGVO, da der Marktplatz selbst keine Daten verarbeite, sondern lediglich den Kontakt zwischen Käufer und Verkäufer herstelle. Und auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Louisa Specht-Riemenschneider erklärte, dass sich die DSGVO auf die Verarbeitung von Daten beziehe, nicht auf die Vermittlung durch Datenhändler und sprach von einer „Rechtsschutzlücke". Der Gesetzgeber sei gefordert.[18]

Die Frage steht im Raum, ob der Handel mit Daten tatsächlich keine Verarbeitung im Sinne des Datenschutzrechts darstellt und ob mit dem Datenschutzrecht gegen die Vermittlungen unzulässiger Datenübermittlungen somit tatsächlich nicht vorgegangen werden kann.

2 Datenhandel nach DSGVO

Die Frage, ob **Datenschutzrecht anwendbar** ist, hängt davon ab, ob es sich bei den vermittelten Daten um personenbezogene Daten handelt und ob deren Vermittlung durch die Beteiligten als Datenverarbeitung im Sinne der DSGVO zu verstehen und zu verantworten ist.

2.1 Personenbezug

Personenbezogene Daten sind „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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann" (Art. 4 Nr. 1 DSGVO).

„Einer **Pseudonymisierung** unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. 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, wie beispielsweise das Aussondern. 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" (ErwGr 26 S. 2-4 DSGVO). Es ist nicht erforderlich, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden.[19] Die zeitlich zugeordnete IP-Adresse beim einem Online-Medienanbieter ist

[18] Meineck/Dachwitz, Databroker Files (Fn. 3).
[19] EuGH 19.10.2016 – C-582/14 Rn. 43, NJW 2016, 3579 (Breyer).

personenbezogen.[20] Das Gleiche gilt für den beim Real-Time-Bidding für Online-Werbezwecke genutzten TC-String.[21]

Standortdaten von Mobilgeräten sind personenbezogene Daten, auch wenn keine direkte Zuordnung dieser Daten zu einem Namen erfolgt, wenn sie z. B. über **Mobile Advertising-IDs (MAID)** erschlossen werden. Wie einfach insofern Zuordnungen jeweils zu einer natürlichen Person möglich sind, hat netzpolitik.org anhand vieler Beispiele nachgewiesen. Als die New York Times 2019 die Standortdaten von mehr als 12 Millionen Smartphone-Nutzern zugespielt bekam, die durch Apps erfasst worden waren, gelang es Auswertern beispielsweise, die Wege von US-Präsident Donald Trump nachzuzeichnen.[22]

Der Umstand, dass sich unter gehandelten Daten auch solche befinden, deren **Korrektheit fraglich** ist, ändert nichts daran, dass es sich bei diesen Daten um personenbezogene Daten im Sinne der DSGVO handelt.

2.2 Verarbeitung

Eine Datenübermittlung von einem Verkäufer an einen Käufer eines Datensatzes ist eine Offenlegung und damit eine Verarbeitung i. S. v. Art. 4 Nr. 2 DSGVO. Der Verarbeitungsbegriff umfasst auch die „Organisation“, die „Anpassung oder Veränderung“, die „Verwendung“ oder jede Form der „Bereitstellung“ von personenbezogenen Daten.

Das Ergebnis aus Ziffer 2.1 sowie die Feststellung, dass Handel und Verkauf dieser Daten eine Verarbeitung im Sinne von Art. 4 Abs. 1 Ziffer 2 darstellen, führt dazu, dass die DSGVO für den Gesamtvorgang des Datenhandels anwendbar ist.[23]

2.3 Verantwortlichkeit

Bisher scheinen deutsche Datenschutzbehörden davon auszugehen, dass Datenhändler weder Verantwortliche noch Auftragsverarbeiter i. S. v. Art. Art. 4 r. 7 u. 8 DSGVO sind (s. o. 1.3). **Verantwortlicher** ist die Person oder Stelle, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

Ursprünglich hatten Datenschutzaufsichtsbehörden zumeist ein eher enges Verständnis von Verantwortlichkeit bei ihrer Rechtsanwendung. Dies wurde vom EuGH korrigiert.[24] Die vom EuGH vorgenommene weite Definition des Verantwortlichen zielt darauf ab, „einen **wirksamen und umfassenden Schutz** der betroffenen Personen zu gewährleisten“.[25]

Im Interesse eines wirksamen und umfassenden Datenschutzes hat der EuGH in vielen Fällen einer Datenkooperation eine gemeinsame Verantwortlichkeit angenommen, wobei die verschiedenen

[20] EuGH 19.10.2016 – C-582/14 (Fn. 19) Rn. 49.
[21] EuGH 07.03.2024 – C-604/22 Rn. 50, K&R 2024, 256 (IAB Europe).
[22] Krempl, Sicherheitsrisiko (Fn. 6).
[23] Zur Vagheit der personenbezogenen Zuordnung EuGH 04.10.2024 – C-21/23 Rn. 88, NJW 2025, 33 (Lindenapothke).
[24] So zur Verantwortlichkeit von Nutzern von Facebook-Accounts EuGH 05.06.2018 – C-210/16 (Fn. 1).
[25] EuGH 10.07.2018 – C-25/17 Rn. 66, NJW 2019, 290 (Zeugen Jehovas).

Akteure in verschiedenen Phasen der Verarbeitung in unterschiedlichem Ausmaß einbezogen sein können und nicht zwangsläufig gleichwertig verantwortlich sein müssen.[26] Relevant ist, dass eine Stelle **aus Eigeninteresse Einfluss** auf die Verarbeitung der Daten nimmt und damit an der Entscheidung über die Zwecke und Mittel der Verarbeitung mitwirkt.[27] Nach Art. 26 Abs. 1 DSGVO handelt es sich um „gemeinsam Verantwortliche“, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen.[28]

Die **Mitwirkung an der Entscheidung** über die Zwecke und Mittel kann verschiedene Formen haben und sich sowohl aus einer gemeinsamen Entscheidung von zwei oder mehr Einrichtungen als auch aus übereinstimmenden Entscheidungen solcher Einrichtungen ergeben. Die Entscheidungen müssen sich in einer Weise ergänzen, dass sich jede von ihnen konkret auf die Entscheidung über die Verarbeitungszwecke und -mittel auswirkt. Es ist nicht einmal erforderlich, dass zwischen den Verantwortlichen eine förmliche Vereinbarung über die Zwecke und Mittel der Verarbeitung besteht.[29] Im Fall einer Verarbeitungskette besteht die gemeinsame Verantwortlichkeit nur für die Verarbeitungsschritte, für die eine gemeinsame Entscheidung vorliegt.[30]

Für die Annahme eines Verantwortlichen kommt es nicht darauf an, ob die Stelle tatsächlich im Besitz der Daten ist.[31] So ist z. B. IAB (Interactive Advertising Bureau) Europe gemeinsam mit den Internetwerbeanbietern gemeinsam verantwortlich, weil es die Rahmenbedingungen für das **Real Time Bidding** bei dem Versteigern von Internetwerbung festlegt, die als Grundlage des Ausspielens personenbeziehbarer Werbung dienen.[32]

Beim **Datenhandel** kommt es also für die Annahme einer gemeinsamen Verantwortung darauf an, dass der Datenhändler damit ein Eigeninteresse verfolgt und bei der Vermittlung über die Zwecke und Mittel mitentscheidet. Ein Eigeninteresse besteht schon darin, dass sich der Datenhändler die Vermittlung vergüten lässt. Ein Vermittler entscheidet auch über die Zwecke und Mittel mit, da er bei der Vermittlung dem Käufer bestimmte Zwecke, etwa die Werbenutzung, vorgibt. Dies gilt erst recht, wenn der Vermittler es dem Käufer freistellt, für welche Zwecke dieser eine Weiterverarbeitung vornimmt. Angesichts der gemeinsamen Verantwortlichkeit ist der Vermittler verpflichtet, sich hinreichend darüber zu vergewissern, dass der Käufer seine Verarbeitung auf zulässige Zwecke beschränkt. Hinsichtlich der Mittel besteht dadurch eine Mitverantwortung des Vermittlers, dass er die Rahmenbedingungen benennt, wie die Übermittlung der vermittelten Daten erfolgen soll. Für die Beurteilung kommt es nicht darauf an, ob der Vermittler selbst einen Zugriff auf die vermittelten Daten hat oder nicht.

Die Verantwortlichkeit des Datenhändlers bezieht sich somit auf die **Datenübermittlung**. Diese würde es ohne die Vermittlung nicht geben. Dass dieses Ergebnis vom DSGVO-Gesetzgeber beabsichtigt war,

[26] EuGH 05.06.2018 – C-210/16 (Fn. 1) Rn. 28; EuGH 10.07.2018 – C-25/17 (Fn. 25) Rn. 66.
[27] EuGH 10.07.2018 – C-25/17 (Fn. 25) Rn. 68.
[28] EuGH 05.12. 2023 – C-683/21 Rn. 40, NJW 2024, 348 (NZÖG Litauen); EuGH 07.03.2024 – C-604/22 (Fn. 21) Rn. 57.
[29] EuGH 05.12. 2023 – C-683/21 (Fn. 25) Rn. 43 f.
[30] EuGH 07.03.2024 – C-604/22 (Fn.21) Rn. 73; EuGH 29.07.2019 –C-40/17 Rn. 74, NJW 2019, 2755 (Fashion ID).
[31] EuGH 05.06.2018 – C-210/16 (Fn. 1) Rn. 38, EuGH 10.07.2018 – C-25/17 (Fn. 25) Rn. 69; EuGH 07.03.2024 – C-604/22 (Fn.21) Rn. 69.
[32] EuGH 07.03.2024 – C-604/22 (Fn. 21) Rn. 77; zum Real Time Bidding Weichert, DANA 3/2019, 120 ff.

zeigt sich in der Verwendung des in Art. 4 Nr. 2 DSGVO umfassenden Verarbeitungsbegriffs in Art. 4 Nr. 2 DSGVO, der schon die „Verbreitung“ und die „Bereitstellung“ erfasst.[33]

Der Datenhändler teilt seine Verantwortlichkeit mit dem Verkäufer und dem Käufer. Alle drei Beteiligten entscheiden mit dem Abschluss des Datenverkaufs über die Zwecke und Mittel der Datenübermittlung. Der Verantwortlichkeit des Datenhändlers tut es keinen Abbruch, wenn sowohl der Verkäufer wie auch der Käufer ihre Sitze **außerhalb der EU und des Europäischen Wirtschaftsraums** (EWR) haben, oder wenn dies für einen von ihnen gilt. Der Vermittlungsprozess begründet eine Zuständigkeit gemäß der DSGVO und eröffnet die sich hieraus ergebenden rechtlichen Konsequenzen.

Keine gemeinsame Verantwortlichkeit besteht bzgl. der **Weiterverarbeitung** der Daten durch den Käufer. Dieser trägt die alleinige Verantwortung dafür, dass er möglicherweise entgegen der beim Datenhandel festgelegten zulässigen Zwecke die Daten für unzulässige Zwecke verwendet.

Wird ein Datenhändler nur für einen Datenverkäufer tätig, so kann statt einer gemeinsamen Verantwortlichkeit eine **Auftragsverarbeitung** (Art. 4 Nr. 8 DSGVO) für den Verkäufer gegeben sein, vorausgesetzt, dieser handelt ausschließlich auf Weisung des Verkäufers und bestimmt nicht mit bei der Festlegung der Zwecke der vermittelten Daten (Art. 28 DSGVO).

2.4 Konsequenzen der gemeinsamen Verantwortlichkeit

Angesichts des Umstands, dass Datenhändler auch Verantwortliche für eine Datenverarbeitung sind, unterliegen sie sämtlichen DSGVO-Verpflichtungen. Sie haben Untersuchungen der zuständigen Datenschutzaufsicht zu dulden und alle Informationen bereitzustellen, die für deren Aufgabenerfüllung nötig sind (Art. 58 Abs. 1 DSGVO). Datenhändler haben also gegenüber der Aufsicht umfassend **Auskunft zu erteilen**, welche Daten von welchen Verkäufern zum Verkauf bereitgestellt werden und welche Käufer welche Daten erworben haben.

3 Strafrechtliche Verantwortung

Die unter 1.2 dargestellte Praxis weist auf eine hohe kriminelle Energie hin. Bei den geschilderten Formen des Datenhandels handelt es sich um Straftaten.

3.1 Datenschutzstrafrecht

Regelmäßig ist der Tatbestand des § 42 Abs. 1 BDSG erfüllt, wonach mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft wird, „wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen ohne hierzu berechtigt zu sein, 1. einem Dritten übermittelt oder 2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt“. Bei Datenhändlern liegt in jedem Fall ein **gewerbsmäßiges Vorgehen** vor, da die

[33] S. o. 2.2; Roßnagel in Simitis/Hornung/Spiecker (Fn. 17), Art. 4 Nr. 2 Rn. 26.

Datenhändler durch wiederholtes Vermitteln eine fortdauernde Einnahmequelle von einiger Dauer und einigem Umfang in Anspruch nehmen.[34]

Voraussetzung für die Strafbarkeit ist, dass die unzulässige Datenvermittlung **wissentlich** erfolgt. Es genügt bedingter Vorsatz.[35] Bedingter Vorsatz ist, wenn der Täter die Tatbestandsverwirklichung für möglich hält. Der Umstand, dass Datenschutzbehörden über die Medien erklärt haben, dass sie ein Vorgehen gegen den unzulässigen Datenhandel nicht für möglich ansehen, schließt die Vorsätzlichkeit nicht aus. Selbst wenn dem Datenhändler die Einsicht in das Unrecht fehlt, handelt er nicht schuldlos, da der Irrtum vermeidbar ist (§ 17 StGB).

Antragsberechtigt sind u. a. die **Aufsichtsbehörden**. Da von den beteiligten Verantwortlichen an den Deals kein Antrag zu erwarten ist und auch nicht von den Betroffenen, die i. d. R. von ihrer Betroffenheit keine Kenntnis erlangen, sollten die Aufsichtsbehörden nach Ausermittlung des Sachverhaltes erwägen, einen solchen Antrag zu stellen, um eine hinreichende Sanktionierung zu erreichen.

3.2 Datenhehlerei

Die Vermittlung von illegal erlangten Datenbeständen dürfte zudem regelmäßig den Straftatbestand der Datenhehlerei erfüllen (§ 202d Abs. 1 StGB). Danach wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer nicht allgemein zugängliche Daten, „die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder **einem anderen verschafft**, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen“.

Schutzgut dieser Strafrechtsnorm ist zumindest auch die individuelle Privat- und Intimsphäre, insbesondere wenn insofern schwerwiegende Beeinträchtigungen erfolgen. Das Persönlichkeitsrecht generell soll von § 202d StGB jedoch nicht geschützt sein.[36]

Fraglich ist, ob eine Datenhehlerei auch dann besteht, wenn ein über die Daten **Verfügungsberechtigter** unter Verstoß gegen den Datenschutz und damit unzulässigerweise, aber zunächst rechtmäßig erlangte Daten verkauft. Dies kann z. B. gegeben sein, wenn ein App-Anbieter berechtigterweise Standortdaten aus dem Mobilgerät eines Betroffenen erhebt, weil dies für die Erbringung des Dienstes erforderlich ist. Dies ist dagegen nicht der Fall, wenn sich ein App-Anbieter für die Erhebung von Standortdaten auf eine unwirksame „Einwilligung“ beruft. Es spricht vieles dafür, dass es hierauf nicht ankommt. Es kann keinen Unterschied machen, ob jemand in einer Kette eines illegalen Datenhandels, z. B. als App-Anbieter, ganz am Anfang steht, oder erst an zweiter oder späterer Stelle. Bei einem Datenverkauf unzulässig verarbeiteter Daten wird die Verfügungsmacht des Betroffenen verletzt, also z. B. die des Handynutzers im Fall des Verkaufs von Mobilfunk-

[34] Burchard in Simitis/Hornung/Spiecker (Fn. 17), § 42 Rn. 15.
[35] Burchard in Simitis/Hornung/Spiecker (Fn. 17), § 42 Rn. 20.
[36] Kargl in Kindhäuser/Neumann/Paeffgen/Saliger (NK), StGB Band 3, 6. Aufl. 2023, § 202a Rn. 7 i. V. m. § 202d Rn. 7.; Hoyer in Wolter/Hoyer, SK-StGB Band IV, 10. Aufl. 2024, § 202d Rn. 1.

Standortdaten. Diese Betroffenen haben ein schutzwürdiges Interesse an der Nichtverwendung der Daten.[37]

Voraussetzung für die Anwendbarkeit des § 202d StGB ist eine **rechtswidrige Vortat**. Der Zweck dieser Norm ist es nicht, jede Weitervermittlung von durch einen Datenschutzverstoß als Vortat erlangten Daten zu sanktionieren. Vielmehr muss es sich bei der „Vortat" um eine Straftat handeln (§ 11 Abs. 1 Nr. 5 StGB). Diese muss objektiv vorliegen. Es spielt keine Rolle, ob der Täter der Vortat schuldhaft gehandelt hat oder ob ein Strafantrag vorliegt. In Betracht kommen auch Straftaten nach dem BDSG. Wurde bei der Datenbeschaffung z. B. gegen § 42 BDSG verstoßen, so ist auch die Weitervermittlung nach § 202d StGB strafbar.[38] Erst recht gilt dies für Verstöße gegen die berufliche Schweigepflicht (§ 203 StGB) als Vortat.

Die **Tatbestandshandlung** ist äußerst weit, indem das „sich oder einem anderen Verschaffen", das „Überlassen, „Verbreiten" oder „sonst Zugänglich-Machen" sanktioniert wird. Es kommt also auch aus strafrechtlicher Sicht nicht darauf an, dass der Datenhehler selbst und alleine über die Daten Verfügungsmacht hat.[39]

Die Verfolgung des § 202d StGB erfolgt – ebenso wie bei § 42 BDSG und § 203 StGB – bei Vorliegen eines Strafantrags. Anders als bei § 42 BDSG und § 203 StGB genügt aber auch, wenn kein Strafantrag vorliegt, „dass die Strafverfolgungsbehörde wegen des **besonderen öffentlichen Interesses** an der Strafverfolgung ein Einschreiten vom Amts wegen für geboten hält" (§ 205 Abs. 1 S. 2 StGB). Bei den unter 1.2 dargestellten Sachverhalten, bei denen es sich um massenhaft vermittelte unzulässige Datenbestände handelte, besteht ein solches besonderes öffentliches Interesse.

Hinsichtlich der **subjektiven Seite** genügt Eventualvorsatz. Es genügt das Bewusstsein, dass die Daten aus einer irgendwie rechtswidrigen Tat stammen.[40] So ist z. B. beim massenhaften Verkauf von Standortdaten allgemein bekannt, dass es sich hierbei um unzulässig weiterverarbeitete Daten aus Telekommunikationsvorgängen handelt. Für die Bereicherungsabsicht genügt es, wenn die Datenvermittlung gegen ein Honorar erfolgt oder erfolgen soll.[41]

4 Ergebnis

Die Annahme, illegale Datenhändler könnten daten- und strafrechtlich nicht zur Verantwortung gezogen werden, ist falsch. Die Aufsichtsbehörden sind aufgefordert, diesem sich immer stärker verbreitenden Unwesen entgegen zu stellen, ohne die Verantwortung auf den Gesetzgeber zu verschieben. Dabei sollten sie nicht nur die Datenhändler als „Hehler" selbst ins Visier nehmen, sondern ebenso Verkäufer und Käufer der datenschutzwidrig verkauften Datensätze. Aber auch die

[37] Hilgendorf in Leipziger Kommentar StGB (LK, Hrsg. Cirener/Radtke/Rissing-van Saan-Rönnau/Schluckebier), 13. Aufl. 2023 Band 10, § 202d Rn. 3; Kargl in Kindhäuser/Neumann/Paeffgen/Saliger (Fn. 36), § 202d Rn. 13.
[38] Kargl in Kindhäuser/Neumann/Paeffgen/Saliger (Fn. 36), § 202d Rn. 14.
[39] Hilgendorf in LK-StGB (Fn. 37), § 202d Rn. 23; Hoyer in SK-StGB (Fn. 36), § 202c Rn. 8 i. V. m. § 202Rn. 8; a. A. Kargl in Kindhäuser/Neumann/Paeffgen/Saliger (Fn. 36), § 202d Rn. 18.
[40] Kargl in Kindhäuser/Neumann/Paeffgen/Saliger (Fn. 36), § 202d Rn. 21.
[41] Kargl in Kindhäuser/Neumann/Paeffgen/Saliger (Fn. 36), § 202d Rn. 22.

Staatsanwaltschaften sollten sich diesem Phänomen annehmen, zumal es sich hierbei um höchst gesellschaftsschädliche Kriminalität handelt.

Abkürzungen

ABl. EU	Amtsblatt der EU
Abs.	Absatz
Art.	Artikel
Aufl.	Auflage
BDSG	Bundesdatenschutzgesetz
BVerfG	Bundesverfassungsgericht
ca.	circa
DANA	DatenschutzNachrichten
DSGVO	Europäische Datenschutz-Grundverordnung
ErwGr	Erwägungsgrund
EuGH	Europäischer Gerichtshof
ff.	fort-/folgende
Fn.	Fußnote
i. d. R	in der Regel
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
K&R	Kommunikation und Recht (Zeitschrift)
lit.	Buchstabe
MAID	Mobile Advertising Identifier
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
Rn.	Randnummer
S.	Satz/Seite
s. o.	siehe oben
StGB	Strafgesetzbuch
u. a.	unter anderem/und andere
v.	von
z. B.	zum Beispiel