Rechtsprechung

OLG Celle: Mangel einer an sich einwandfreien Standardsoftwarelösung

BGB §§ 133, 157, 305c, 323, 346, 433, 434, 437, 440

Verpflichtet sich der Verkäufer eines Softwarelizenzvertrages ein auf die Anforderungen des Käufers zugeschnittenes Produkt (hier zur Registrierkassenfunktion im Geschäftsbetrieb des Käufers) zu liefern, so ist er verpflichtet, abzuklären, ob sich mit der von ihm angebotenen (Standard-)Software angesichts der vorhandenen Hard- und Software-Komponenten des Käufers die vertraglich vorausgesetzte Funktion erreichen lässt. *(nicht amtl.)*

OLG Celle, Beschl. v. 26.8.2019 – 20 U 35/18
(LG Hannover, Urt. v. 22.11.2018 – 9 O 9/18)

Aus den Gründen:

(...) II. (...) Der Senat bleibt bei seiner Auffassung, dass die Klägerin keinen Anspruch gegen den Beklagten auf Zahlung der Kosten für den Erwerb der Softwarelizenz (§ 433 Abs. 2 Alt. 1 BGB) hat, weil der Beklagte durch Rücktrittserklärung vom 19.8.2017 wirksam vom Kaufvertrag zurückgetreten ist (§ 434 Abs. 1 Nr. 1, § 437 Nr. 2, § 440 Satz 1, § 323 Abs. 1, § 346, § 349 BGB)

Im Einzelnen.

1. Ohne Erfolg macht die Klägerin geltend, das von ihr abgegebene, auf die „Anforderungen [des Beklagten] zugeschnittene" Angebot auf Abschluss eines Softwarelizenzvertrages (...) sei so zu verstehen, dass die im Angebot aufgelisteten Module für die Anforderungen des Geschäftsbetriebs des Beklagten ausgewählt worden seien. Eine über den Verkauf einer Standardsoftware hinausgehende Verpflichtung sei daraus nicht herzuleiten (...).

Der Senat teilt diese Ansicht nicht. Die Formulierung des ersichtlich für mehrfache Verwendung konzipierten Angebotsschreibens ist unklar. Zweifel bei der Auslegung gehen insofern zu Lasten der Klägerin (§ 305c Abs. 2 BGB). Das Angebot ist (...) aus Sicht eines objektiven Empfängers unter Berücksichtigung von Treu und Glauben (§ 133, § 157 BGB) so zu verstehen, dass die Klägerin eine Software anbietet, die auf die konkrete Situation des Beklagten und dessen Verwendung zugeschnitten ist. Die Klägerin war daher beim Verkauf ihrer Software verpflichtet, abzuklären, ob sich mit ihrer Software bei der bestehenden Hard- und Software des Beklagten die von beiden Seiten nach dem Vertrag vorausgesetzte Verwendung (§ 434 Abs. 1 Satz 2 Nr. 1 BGB), die vorgeschriebene Registrierkassenfunktion, erreichen lässt. Zumindest hätte sie den Beklagten darauf hinweisen müssen, dass er mit dem bestehenden System und der Software das Ziel nicht erreichen kann.

2. Deshalb kann auch dahinstehen, ob der Vortrag der Klägerin, dass die gelieferte Software mit dem Betriebssystem des Beklagten kompatibel und nur die Signatureinheit des Beklagten nicht mit der Software des Beklagten vereinbar sei, in zweiter Instanz noch berücksichtigungsfähig ist (...). Die Klägerin hat den geschuldeten Hinweis unterlassen, dass der Beklagte mit ihrer Software und seiner Ausgangssituation nicht das Ziel „gesetzlich vorgeschriebene Registrierkassenfunktion" erreichen kann. (...)

3. Auch dem Einwand der Klägerin, der Beklagte habe nicht vom Vertrag zurücktreten können, weil der Klägerin angesichts der Hard- und Software-Voraussetzungen des Beklagten eine Nacherfüllung unmöglich gewesen sei, folgt der Senat nicht. Die Klägerin hätte zumindest darauf hinweisen können und müssen, dass das Gesamtsystem mit den angebotenen und bestehenden Komponenten nicht den Vertragszweck erfüllt und – anschließend daran – gegebenenfalls die Rückabwicklung des Vertrags akzeptieren müssen. (...)

Eingesandt von RA Jan-Malte Böttchern, Bremen

Daten und Sicherheit

Aufsätze

Gerrit Hornung / Carolin Gilga*

Einmal öffentlich – für immer schutzlos?

Die Zulässigkeit der Verarbeitung öffentlicher personenbezogener Daten

Die Veröffentlichung von privaten Informationen im Internet ist heutzutage gang und gäbe. Täglich kreieren Millionen Nutzer sozialer Medien neue Beiträge über sich und andere, Blogger berichten über neuste Trends und aktuellste Neuigkeiten werden auf Nachrichten-Webseiten zur Verfügung gestellt. Hierdurch nimmt auch die Menge der online verfügbaren personenbezogenen Daten Tag für Tag rasant zu. Mangels ausdrücklicher Rege-

* Der Text ist im Zusammenhang mit dem BMBF-Projekt „Echtzeit-Lagebild für effizientes Migrationsmanagement zur Gewährleistung humanitärer Sicherheit (HUMAN+)", FKZ 13N14722, entstanden.

lung ist für die DSGVO bisher weithin unklar, wie derartige öffentliche Informationen datenschutzrechtlich einzuordnen sind. Der Beitrag untersucht den Begriff des öffentlichen personenbezogenen Datums und analysiert, welchen Einfluss das Kriterium der Öffentlichkeit auf die Zulässigkeit der Verarbeitung nimmt.

I. Privilegierte Verarbeitung – auch nach der DSGVO?

1 Im Internet existieren vielfältige Möglichkeiten, um Inhalte mit anderen zu teilen. Fotos, persönliche Erlebnisse, politische Meinungen u.v.m. werden in sozialen Netzwerken, auf Blogs und anderen Webseiten veröffentlicht.[1] Dabei richten sich diese Inhalte oftmals nicht an eine begrenzte Anzahl von Personen, sondern werden bewusst einem möglichst großen, unbestimmten Adressatenkreis zur Verfügung gestellt. Hierdurch entstehen täglich große Mengen – nicht nur, aber häufig – personenbezogener Daten, die *frei* im Internet *zugänglich* sind. Faktisch sind die Erhebung und weitere Verarbeitung dieser Daten häufig einfach zu bewerkstelligen. Es stellt sich aber die Frage, unter welchen Voraussetzungen dies zulässig ist.

2 Die DSGVO sieht nur an einer einzigen Stelle eine Bestimmung zu *offensichtlich* durch die betroffene Person *öffentlich gemachten* Daten vor: Art. 9 Abs. 2 lit. e DSGVO hebt in diesem Fall das grundsätzliche Verarbeitungsverbot auf, wenn es sich um besondere Kategorien personenbezogener Daten handelt. Dies entspricht der alten Rechtslage in Art. 8 Abs. 1 lit. e DSRL,[2] der z.B. durch §§ 13 Abs. 2 Nr. 4, 28 Abs. 6 Nr. 2 BDSG a.F. umgesetzt worden war. Demgegenüber enthält die DSGVO *keine allgemeine Norm* zur Verarbeitung *öffentlicher Daten*, während nach altem deutschen Recht die Verarbeitung von Daten aus allgemein zugänglichen Quellen – über die DSRL hinaus, bzw. als nationale Ausformung ihrer Abwägungsklauseln – „privilegiert", d.h. erleichtert zulässig war.[3] Auch im deutschen Recht existieren nur noch rudimentäre Bestimmungen zu öffentlichen Daten.[4]

3 Dies führt zu der Frage, ob die Verordnung zumindest dogmatisch eine dem BDSG a.F. ähnliche Kategorie öffentlicher Daten kennt (III.), welche Daten wegen ihrer Öffentlichkeit hierzu zu zählen sind (IV.), welche Bestimmungen auf sie anzuwenden sind und ob die Verarbeitung dieser Daten weiterhin privilegiert ist (V.).

II. Relevanz und Risiken öffentlich zugänglicher Daten

4 Im Zuge der stetig anwachsenden Menge frei zugänglicher (personenbezogener) Daten im Internet werden immer mehr Technologien und Geschäftsmodelle entwickelt, die aus ihnen einen Mehrwert generieren. Damit geht ein gesteigertes Interesse an der Verwendung dieser Daten einher. Dieses kann sich auf die übergreifende Analyse globaler Trends oder auf konkrete Personen und Ereignisse beziehen. Für Unternehmen können derartige Analysen z.B. im Rahmen von Markt-, Meinungs- und Trendforschung einen Wettbewerbsvorteil bedeuten[5] oder Produktbeobachtungen erleichtern.[6] Wichtige Erkenntnisse können sich für die sozialwissenschaftliche Forschung ergeben.[7] Auch in *Bewerbungsprozessen* möchten Recruiter oftmals auf öffentliche Daten zugreifen, um sich ein besseres Bild von Bewerbern zu verschaffen.[8] *Öffentliche Stellen* können öffentliche Informationen u.a. verwenden, um die Strafverfolgung effizienter zu gestalten, staatliche Handlungen und Entscheidungen genauer zu adressieren, Krisensituationen durch breitere Informationsgrundlagen besser zu meistern[9] oder Stimmungsbilder in der Bevölkerung aufzufangen.[10] In Betracht kommt auch eine Verwendung der Daten für Amtsermittlungen von Steuerbehörden oder Sozialleistungsträgern.[11] Für den einzelnen Internetnutzer ergibt sich zudem die Möglichkeit, sein *Recht auf Informationsfreiheit* wahrzunehmen, indem er das Internet zur Information und Meinungsbildung verwendet.

5 Diesen Chancen stehen aus datenschutzrechtlicher Sicht allerdings *deutliche Risiken* gegenüber. Die betroffenen Personen wissen möglicherweise nichts von der Verfügbarkeit ihrer Daten und sind sich nicht immer über die potentiellen Auswirkungen einer Veröffentlichung bewusst. Angesichts der weiten Verbreitung im Netz kann es passieren, dass eine Löschung der Daten schwer oder unmöglich wird („das Internet vergisst nichts"),[12] Arbeitgeber oder Behörden gezielt auf Daten zugreifen oder beliebige Dritte diese zusammentragen und auswerten. Je nach Art der öffentlichen Daten, Interesse und Verarbeitungszweck des Verantwortlichen und Rechtsbeziehung zu der betroffenen Person kann dies erhebliche Auswirkungen haben.

6 Aus rechtlicher Sicht sind viele Problemstellungen nicht abschließend geklärt. Öffentlich gemachte personenbezogene Daten sind *weltweit verfügbar*, einheitliche weltweite *Regelungen* bestehen hingegen *nicht*. Ein gemeinsames Verständnis von zentralen Begrifflichkeiten sowie Vorgaben für den Umgang mit öffentlichen personenbezogenen Daten existieren nicht. So-

---

1 Zu den Rechtsfragen von sozialen Netzwerken s. näher *Hornung/Müller-Terpitz* (Hrsg.), Rechtshandbuch Social Media, 2015 (2. Aufl. 2020, i.E.).

2 RL 95/46/EG v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, ABl L 281/31.

3 S. §§ 10 Abs. 5 S. 2, 13 Abs. 2 Nr. 5, 14 Abs. 2 Nr. 5, 28 Abs. 1 S. 1 Nr. 3, Abs. 3 S. 2 Nr. 1, 29 Abs. 1 S. 1 Nr. 2, 30 Abs. 2 Nr. 2, 30a Abs. 1 S. 1 Nr. 2, Abs. 2, 33 Abs. 2 S. 1 Nr. 7 lit. a, Nr. 8 lit. a, Nr. 9, 35 Abs. 6, 43 Abs. 2 Nr. 1-4 BDSG a.F.

4 Die Strafvorschriften in § 42 Abs. 1 und Abs. 2 BDSG n.F. enthalten die (fehlende) Allgemeinzugänglichkeit als Tatbestandsmerkmal. Daneben existieren noch spezialgesetzliche Regelungen, die die Verarbeitung von Daten aus allgemein zugänglichen Quellen privilegieren, s. z.B. § 10 Abs. 2 S. 5 Nr. 4 KWG.

5 S. *Solmecke/Wahlers*, ZD 2012, 550; *Venzke-Caprarese*, DuD 2013, 775; *BVDW*, Social Media Monitoring in der Praxis, 2017, 16 ff.; zu den datenschutzrechtlichen Fragen der Markt- und Meinungsforschung nach der DSGVO s. *Hornung/Hofmann*, ZD-Beilage 4/2017.

6 *Klindt/Wende*, BB 2016, 1419 (auch zur Frage der Reichweite der Produktbeobachtungspflicht).

7 Zu den datenschutzrechtlichen Fragen *Golla/Hofmann/Bäcker*, DuD 2018, 89.

8 *Oberwetter*, BB 2008, 1562; *Forst*, ZSA 2010, 457, 428; *Kort*, NZA-Beilage 2016, 62, 69; *Bayreuther* in Hornung/Müller-Terpitz (Fn. 1), Kap. 8 Rz. 56 ff.

9 Dieses Szenario wurde im BMBF-Projekt „Echtzeit-Lagebild für effizientes Migrationsmanagement zur Gewährleistung humanitärer Sicherheit (HUMAN+)" beispielhaft für das Migrationsmanagement untersucht.

10 *Schulz/Hoffmann*, DuD 2012, 7; *Nebel* in Richter (Hrsg), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, 2015, S. 89, 95 ff.; *Martini*, VerwArch 2016, 307, 317 ff.

11 Näher *Bieresborn*, NZS 2016, 532.

12 S. zum Recht auf Vergessenwerden (nunmehr terminologisch in Art. 17 DSGVO verankert) und der Diskussion in Folge von EuGH v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317, AfP 2014, 245 = NJW 2014, 2257 – Google Spain, nunmehr *Becker*, Das Recht auf Vergessenwerden, 2019; ferner z.B. *Hornung/Hofmann*, JZ 2013, 163; *Trentmann*, CR 2017, 26.

wohl für den Verantwortlichen als auch für betroffene Personen kann dies zu großer Rechtsunsicherheit führen.

III. Öffentlichen Daten als dogmatische Kategorie

7 Will man auch unter der DSGVO eine dogmatische Kategorie der öffentlichen Daten bilden, so lässt sich entweder an der *Eigenschaft der Allgemeinzugänglichkeit* oder an der *Person* anknüpfen, die diese Eigenschaft hervorgerufen hat.

1. Keine gesetzliche Definition

8 Die erste Gruppe der *öffentlichen*, also *allgemein zugänglichen* Daten, ist weder in der Verordnung noch im BDSG definiert. In Anlehnung an die Definition des § 10 Abs. 5 S. 2 BDSG a.F. sowie nach dem Wortsinn des in Art. 9 Abs. 2 lit. e DSGVO verwendeten Begriffs „öffentlich" sollten darunter alle Daten verstanden werden, die einem *unbestimmten Personenkreis*, also einer nicht begrenzten Anzahl an Personen, frei zugänglich sind.[13] Diese Eigenschaft wird *objektiv* meist relativ leicht zu bestimmen sein, da für sie unerheblich ist, durch wen die Daten veröffentlicht wurden.

2. Veröffentlichung durch die betroffene Person

9 Der Begriff der *offensichtlich* durch die betroffene Person *öffentlich gemachten* Daten, wie er in Art. 9 Abs. 2 lit. e DSGVO verwendet wird, stellt eine *Unterform* der *öffentlichen Daten* dar und ist inhaltlich wesentlich enger gefasst. Anders als bei der reinen Allgemeinzugänglichkeit kann es deutlich schwerer sein festzustellen, durch wen ein Datum öffentlich gemacht wurde. Um diese Unsicherheit nicht zu Lasten der betroffenen Person ausgehen zu lassen, hat der europäische Gesetzgeber das *Merkmal der Offensichtlichkeit* aus der DSRL beibehalten. Bei seiner Beurteilung ist auf die Perspektive eines *außenstehenden Beobachters* abzustellen.[14] Besteht Unsicherheit bzgl. der Offensichtlichkeit, ist diese zu verneinen.[15] Liegt hingegen für den außenstehenden Beobachter Offensichtlichkeit vor, so ist der Tatbestand von Art. 9 Abs. 2 lit. e DSGVO auch dann erfüllt, wenn der beim Beobachter hervorgerufene Anschein nicht den tatsächlichen Gegebenheiten entspricht.[16] Wäre dem nicht so, liefe dies erheblich zu Lasten des Verantwortlichen. Würde bspw. nach bereits erfolgter Verarbeitung klar, dass das Kriterium der Öffentlichkeit nicht vorlag, könnte die Verarbeitung *rückwirkend als rechtswidrig* zu beurteilen sein. Dem Verantwortlichen drohten dann empfindliche Sanktionen (v.a. nach Art. 77 ff. DSGVO), ohne dass er sein Verhalten im Vorhinein darauf einrichten konnte.

3. Veröffentlichung durch Dritte

10 Das Kriterium der *offensichtlichen Veröffentlichung* durch die betroffene Person kann auch erfüllt sein, wenn die Veröffentlichung *durch einen Dritten* erfolgt, die betroffene Person sie aber veranlasst hat und dies für den außenstehenden Beobachter erkennbar ist.[17] Diese über den strengen Wortlaut hinausgehende Auslegung ist geboten, weil es teleologisch letztlich auf den autonomen Willen der betroffenen Person ankommen muss, und dieser in derartigen Fällen offensichtlich mit der Handlung des Dritten übereinstimmt. Dagegen ist eine bloße Duldung der Veröffentlichung nicht ausreichend.[18]

IV. Einordnung der Daten als (durch die betroffene Person) veröffentlicht

11 Insbesondere im Internet ist oftmals nicht eindeutig, ob es sich tatsächlich um *öffentliche* Daten handelt und ob diese ggf. auch *offensichtlich* durch die betroffene Person selbst *öffentlich gemacht* wurden. Nachfolgend werden daher typische Szenarien kurz vorgestellt und diesbezüglich analysiert.

1. Daten in sozialen Netzwerken

12 Für eine Nutzung sozialer Netzwerke wie *Facebook* oder *Instagram* ist typischerweise eine Anmeldung erforderlich. Dies schließt jedoch die Einordnung der Daten als *öffentlich* nicht aus.[19] Grund ist, dass prinzipiell jedermann Zugang zu den sozialen Netzwerken erhalten kann und der potentielle Empfängerkreis damit weder begrenzt noch für die betroffene Person vorhersehbar ist.[20] Die Eigenschaft der Öffentlichkeit bei Daten aus sozialen Medien muss deshalb im Einzelfall beurteilt werden.

a) Eindeutige Nutzereinstellungen

13 Die Nutzer sozialer Netzwerke haben im Regelfall die Möglichkeit, ihre Privatsphäreneinstellungen zu konfigurieren. Bei Facebook kann bspw. ausgewählt werden, ob Beiträge öffentlich, für Freunde oder nur für bestimmte Freunde zugänglich sind. Wählt der Nutzer die *Einstellung „öffentlich"*, so ist eine Veröffentlichung zweifelsfrei gegeben. Wird ein Beitrag nur für bestimmte Freunde zugänglich gemacht, ist der Adressatenkreis begrenzt und überschaubar. Somit sind die Daten jedenfalls dann nicht öffentlich, wenn es sich tatsächlich um einen begrenzten Kreis von „Freunden" im hergebrachten Sinn des Wortes handelt.[21]

b) Verfügbarkeit auch für „Freundesfreunde"

14 Problematischer ist hingegen der Umgang mit Beiträgen eines Nutzers, die gemäß der ausgewählten Privatsphäreneinstellung

---

13 Ebenso *Schulz* in Gola, DSGVO, 2. Aufl. 2018, Art. 9 Rz. 26; *Weichert* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 9 Rz. 78; *Schiff* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 9 Rz. 45; *Wedde* in Däubler et al., 2018, DSGVO BDSG, Art. 9 Rz. 84; *Greve* in Auernhammer, DSGVO BDSG, 6. Aufl. 2018, Art. 9 Rz. 25; *Kampert* in Sydow, DSGVO, 2. Aufl. 2018, Art. 9 Rz. 31; s.a. *Dallmann/Busse*, ZD 2019, 394, 395.

14 *Weichert* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 9 Rz. 80; *Albers/Veit* in BeckOK DSR, 30. Edition, Art. 9 DSGVO Rz. 66.

15 *Kampert* in Sydow, DSGVO, 2. Aufl. 2018, Art. 9 Rz. 33; *Weichert* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 9 Rz. 80.

16 *Weichert* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 9 Rz. 80.

17 *Greve* in Auernhammer, DSGVO BDSG, 6. Aufl. 2018, Art. 9 Rz. 25; *Korge* in Gierschmann et al., DSGVO, 2017, Art. 9 Rz. 30; *Wedde* in Däubler et al., DSGVO BDSG, 2018, Art. 9 Rz. 87.

18 *Petri* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 9 Rz. 59; a.A. *Greve* in Auernhammer, DSGVO BDSG, 6. Aufl. 2018, Art. 9 Rz. 25.

19 Dies regelte explizit § 10 Abs. 5 S. 2 BDSG a.F.

20 Ebenso zum BDSG a.F. *Wolf*, Big Data und Innere Sicherheit, 2015, 74 ff.; *Venzke-Caprarese*, DuD 2013, 775, 776.

21 In diesem Fall greift überdies rglm. die Ausnahme des Art. 2 Abs. 2 lit. c DSGVO; s. zum alten Recht *Hornung* in Hornung/Müller-Terpitz (Fn. 1), Kap. 4 Rz. 48.

auch für die Freunde eines Freundes sichtbar sind und deren Empfängerkreis daher entsprechend erweitert ist.[22] Zwar bleibt die Anzahl der Personen, denen der Beitrag zugänglich ist, nicht unbestimmt, sondern wird auf die „Freundesfreunde" begrenzt. Allerdings sind dem Nutzer nicht alle Personen bekannt, denen der Beitrag zusätzlich zugänglich wird.[23] Er begibt sich damit trotz des Wissens über entsprechende Konfigurationsmöglichkeiten in eine Situation, die für ihn einer *Veröffentlichung gleichkommt*. Die Daten sind damit im Regelfall als öffentlich einzustufen.

c) Umfangreiche Freundeslisten

15 Es wird ebenfalls vertreten, dass Daten als öffentlich einzustufen sind, wenn ein Nutzer eine so umfangreiche Freundesliste hat, dass der Adressatenkreis für ihn *nicht mehr überschaubar* ist.[24] Diese Ansicht ist grundsätzlich nachvollziehbar, da sie ebenfalls an das allgemeine Kriterium des unbestimmten Personenkreises anknüpft. Bei sozialen Netzwerken führen jedoch auch sehr große Freundeslisten regelmäßig gerade nicht zur Unbestimmtheit des Adressatenkreises. Auch bei mehreren hundert Adressaten hat der Nutzer diese bewusst ausgewählt, so dass nicht unterstellt werden sollte, die Adressaten seien für ihn nicht überschaubar. Hierfür sprechen auch *teleologische Gründe*, da bei einer vorschnellen Annahme einer entsprechenden Öffentlichkeit erleichterte Voraussetzungen für die Verarbeitung gelten und die betroffene Person hierdurch potentiell erhebliche Nachteile hat.[25] Die Daten sind damit als *nicht-öffentlich* zu bewerten. Eine Grenze dürfte erst erreicht werden, wenn ein Nutzer *wahllos und umfangreich Freundesanfragen* versendet und annimmt, weil er in diesem Fall aktiv die Öffentlichkeit sucht. Wann die Schwelle der Wahllosigkeit erreicht ist, lässt sich allerdings kaum abstrakt bestimmen, sondern bedarf – so sehr der Praxis mit einer generellen Kontaktzahl geholfen wäre – einer Würdigung des konkreten Einzelfalls.

d) Erkennbarkeit der veröffentlichenden Person

16 Für einen außenstehenden Beobachter ist bei veröffentlichten Beiträgen i.d.R. erkennbar, wer die Daten veröffentlicht hat und ob es sich dabei um die betroffene Person handelte oder nicht. Angesichts der derzeitigen technischen Ausgestaltung bleiben bei einer solchen Feststellung zwar oftmals Restzweifel bestehen. So wird in den AGB vieler sozialer Netzwerke wie z.B. Facebook eine (rechtlich zweifelhafte) *Klarnamenpflicht* vorgeben.[26] Allerdings wird diese nicht systematisch durchgesetzt. Es ist deshalb – schon angesichts des Fehlens verbreiteter sicherer Verfahren des Identitätsmanagements im Internet[27] – rein faktisch relativ leicht möglich, dass sich Personen *unter falschem Namen* registrieren. Allerdings lässt sich auch bei analogen Medien nicht immer zweifelsfrei erkennen, wer die Informationen tatsächlich veröffentlicht hat. Es muss folglich ausreichend sein, wenn alle zur Verfügung stehenden Informationen für die Veröffentlichung durch die betroffene Person sprechen und der außenstehende Beobachter damit zum Ergebnis gelangt, dass die Veröffentlichung durch diese erfolgt ist (s.o. Rz. 7 ff.).

17 Überdies muss hinsichtlich falscher Nutzernamen unterschieden werden. Meldet sich ein Nutzer nämlich mittels eines selbst gewählten, fiktiven *Pseudonyms* an (dies dürfte die Mehrzahl der Fälle betreffen), veröffentlicht unter diesem aber *eigene personenbezogene Daten*, so bleibt Art. 9 Abs. 1 lit. e DSGVO im Falle von sensiblen Informationen anwendbar, weil die Norm nicht an eine identifizierte betroffene Person, sondern an den frei verantwortlichen Akt der Veröffentlichung anknüpft. Nur wenn als Pseudonym eine existierende andere Person gewählt und im Wege des Identitätsdiebstahls deren Daten veröffentlicht werden, ist dies anders zu bewerten. Da derartige Fälle indes selten vorkommen, kann allein wegen dieser Möglichkeit das Tatbestandsmerkmal der *Offensichtlichkeit nicht entfallen*, solange es keine Indizien für eine Identitätstäuschung gibt.

e) Spätere Entfernung

18 Werden die Daten nach einer Veröffentlichung wieder entfernt, so ändert dies nichts daran, dass sie *zunächst* durch die betroffene Person *öffentlich gemacht* wurden. Dies lässt sich allenfalls bei Diensten anders bewerten, die wie *SnapChat* von Anfang an erkennbar darauf angelegt sind, die Daten nur für eine (ggf.: sehr) begrenzte Zeitspanne verfügbar zu machen. Allerdings kann durch das Löschen der Daten eine veränderte Bewertung durch die betroffene Person erkennbar werden, die Anlass dafür sein kann, eine ggf. im Rahmen von Art. 6 DSGVO erforderlich Abwägung (s.u. Rz. 42 ff. und Rz. 58 ff.) zu ihren Gunsten ausfallen zu lassen.[28]

2. Daten in Blogs und auf anderen Webseiten

19 Neben den sozialen Netzwerken besitzen Blogs eine zentrale Bedeutung im Internet. Blogautoren schreiben meist über spezifische Themenbereiche und geben ihre Meinungen oder Erfahrungen wieder. Daneben sind auch einfache, nicht regelmäßig aktualisierte Webseiten ein probates Mittel, um Informationen breit im Internet zu kommunizieren. Wird der Zu-

---

22 Bspw. wenn der Nutzer einen Freund auf einem Beitrag verlinkt und in seinen Einstellungen nicht konfiguriert hat, dass dessen Freunde den Beitrag nicht einsehen können – s. https://www.facebook.com/help/211513702214269?helpref=faq_content.

23 Zwar besteht die Option, die betreffenden Freundeslisten einzusehen oder diese beim Freund zu erfragen. In der Praxis dürfte dies allerdings kaum je geschehen.

24 *Weichert* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 9 Rz. 78; wohl auch *Petri* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 9 Rz. 58.

25 S.u. Rz. 38, Rz. 42. Teleologisch ist der Fall damit gerade umgekehrt zu bewerten wie das nur scheinbar identische Problem, wann eine Veröffentlichung in sozialen Medien dazu führt, dass eine Verarbeitung nicht mehr in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt (Art. 2 Abs. 2 lit. c DSGVO); s. dazu EuGH v. 6.11.2003 – C-101/01, ECLI:EU:C:2003:596, AfP 2004, 248 = CR 2004, 286 = MMR 2004, 95. Dort eröffnet ein weiter Begriff der Öffentlichkeit nämlich den Anwendungsbereich und damit einen stärkeren Schutz der betroffenen Person.

26 S. https://de-de.facebook.com/legal/terms/update unter Punkt 3.1; zur rechtlichen Problematik *Schnabel/Freund*, CR 2010, 718; *Caspar*, ZRP 2015, 233.

27 Dazu mit interdisziplinären Perspektiven die Beiträge in *Engemann/Hornung* (Hrsg.), Der digitale Bürger und seine Identität, 2016.

28 Die hier diskutierte Situation ist also von derjenigen zu unterscheiden, die oftmals unter dem Stichwort eines „Rechts auf Vergessenwerden" diskutiert wird. Dabei haben typischerweise Dritte Daten über die betroffene Person im Internet veröffentlicht, und diese wendet sich nunmehr (wegen anfänglicher Rechtswidrigkeit oder aufgrund einer veränderten Rechtslage nach Ablauf einer gewissen Zeit) gegen eine weitere Abrufbarkeit der Daten auf einer Webseite und/oder gegen die Auffindbarkeit in den Suchergebnissen einer Suchmaschine.

gang zu einem Blog oder einer sonstigen Webseite – wie i.a.R. – nicht auf einen bestimmten Adressatenkreis beschränkt, sind die Daten als *öffentlich* einzustufen. Bestehen dagegen Zugangsbeschränkungen wie Passwörter oder handelt es sich um einen Microblogging-Dienst, der wie *Twitter* Privatsphäreneinstellungen ermöglicht, so ist die *Öffentlichkeit* wie bei sozialen Netzwerken zu bewerten (s. Rz. 12 ff.).

20 Bei Blogs und vielen Webseiten ist es für einen außenstehenden Beobachter meist *offensichtlich erkennbar*, ob die Daten von der betroffenen Person selbst oder durch einen Dritten eingestellt wurden. Soweit – wie in vielen, aber bei weitem nicht allen Blogs – aus der eigenen Lebenswelt berichtet wird, werden die Daten *offensichtlich selbst* öffentlich gemacht. Dasselbe ist bei Eigenberichten auf anderen Webseiten der Fall, wenn die Autoren erkennbar sind. Enthält ein Blog dagegen im Einzelfall oder sogar von seiner ganzen Zielrichtung her personenbezogene Daten Dritter, so bedarf es für die Klassifizierung dieser Daten als offensichtlich selbst öffentlich gemachte eines Willensaktes der betroffenen Personen, für den entsprechende offensichtliche Indizien vorliegen müssen. Bei allgemeinen Webseiten jenseits von Blogs wird dies – also die Veröffentlichung von Daten Dritter ohne derartige Indizien – sogar der typische Fall sein. Die personenbezogenen Daten sind dann im Regelfall zwar *öffentlich*, aber *nicht offensichtlich* durch die betroffene Person *öffentlich gemacht*.

3. Ergebnis

21 Anhand dieser Szenarien wird klar, dass eine Einordnung von Daten als öffentlich oder nicht-öffentlich *nicht immer ad hoc* stattfinden kann. Insbesondere bei sozialen Netzwerken ergibt sich ein großer Graubereich, innerhalb dessen die Einordnung Argumentationssache sein wird. Vor allem das Kriterium des begrenzten Adressatenkreises kann aufgrund seiner Abstraktheit nicht immer eindeutig auf jeden Sachverhalt angewendet werden. Es ist daher sinnvoll, auf die gewählte *Privatsphäreneinstellung* der betroffenen Person abzustellen, da sich hierin ihr *Wille zur Öffentlichkeit* widerspiegelt. Internetnutzer wissen heutzutage um die Möglichkeiten, ihre Privatsphäre zu schützen. Werden entsprechende Vorkehrungen nicht getroffen, ist – jedenfalls solange die Einstellungen leicht geändert werden können – davon auszugehen, dass die betroffene Person die Daten nicht nur einem begrenzten Publikum *zugänglich machen* möchte. Dies gilt umso mehr, als die Standardeinstellungen der sozialen Netzwerke i.d.R. keine allgemeine Zugänglichkeit der selbsterstellten Daten vorsehen, so dass (entsprechend Art. 25 Abs. 2 DSGVO) eine aktive Entscheidung der betroffenen Person anzunehmen ist.

V. Datenschutzrechtliche Zulässigkeit der (Weiter-) Verarbeitung

22 Im Rahmen der datenschutzrechtlichen Zulässigkeit ist systematisch zwischen der Verantwortlichkeit für die *Veröffentlichung* und der Verantwortlichkeit für den *Abruf* und die *Weiterverarbeitung* zu differenzieren. Für die datenschutzrechtliche Zulässigkeit des Abrufs und der Weiterverarbeitung ist sodann die *Grundrechtsrelevanz* öffentlicher und offensichtlich durch die betroffene Person öffentlich gemachter Daten von Bedeutung, die in Abwägungsfragen relevant wird. Schließlich ist hinsichtlich der Zulässigkeit der Verarbeitung selbst[29] zwischen verschiedenen *Datenarten* und verschiedenen *Verantwortlichen* zu unterscheiden.

1. Abgrenzung zur Verantwortlichkeit des Veröffentlichenden

23 Datenschutzrechtliche Zulässigkeitsfragen sind immer mit Blick auf einzelne Verantwortliche, betroffene Personen und Verarbeitungsschritte zu beantworten. Deshalb ist die *Zulässigkeit einer Veröffentlichung* von Daten durch einen Verantwortlichen von der *Zulässigkeit der weiteren Verarbeitung* durch einen anderen Verantwortlichen zu unterscheiden. Ob die Veröffentlichung zulässig oder unzulässig war, spielt zwar in bestimmten Konstellationen für die Zulässigkeit der Weiterverarbeitung eine Rolle (s.u. Rz. 42 ff.)), es besteht aber kein direkter Zusammenhang. Dasselbe gilt für verfahrensrechtliche (Nachberichts-)Pflichten, die denjenigen treffen können, der die Daten öffentlich gemacht hat.

a) Konstellationen und Zulässigkeitsfragen der Veröffentlichung

24 Für die Zulässigkeit der Veröffentlichung personenbezogener Daten sind verschiedene Konstellationen zu unterscheiden:

- Eigene Veröffentlichung: In der ersten Fallgruppe macht die *betroffene Person* Daten über sich *selbst öffentlich*. Hier ist weiter zu unterscheiden, ob dies auf einer eigenen, technisch selbst betriebenen Webpräsenz oder auf einer Plattform, beispielsweise in einem sozialen Netzwerk geschieht.
- Veröffentlichung durch Dritte: In der zweiten Fallgruppe *veröffentlichen Dritte* Daten über die betroffene Person. Dies können Privatpersonen (z.B. wiederum in sozialen Netzwerken) sein, Journalisten oder andere Akteure der Online-Berichterstattung, Arbeitgeber, staatliche Behörden und viele weitere Verantwortliche.

25 Betreibt die betroffene Person in der ersten Fallgruppe das Veröffentlichungsmedium selbst, so stellen sich keine datenschutzrechtlichen Zulässigkeitsfragen, weil ein Verantwortlicher nicht mit der betroffenen Person identisch sein kann; das Datenschutzrecht ist nicht anwendbar. Bei der Veröffentlichung in einem *sozialen Netzwerk* oder einer anderen Plattform verarbeitet der entsprechende Anbieter die personenbezogenen Daten und benötigt eine Erlaubnisnorm. Die Zulässigkeit wird sich regelmäßig auf den *Nutzungsvertrag* (Art. 6 Abs. 1 Unterabs. 1 lit. b DSGVO) oder eine bei Vertragsschluss zusätzlich abgegebene *Einwilligung* (Art. 6 Abs. 1 Unterabs. 1 lit. a DSGVO) stützen; die Reichweite dieser Zulässigkeitstatbestände ist im Einzelfall zu prüfen.

26 Die Zulässigkeitsfragen der zweiten Fallgruppe, also der *Veröffentlichung durch Dritte*, sind so heterogen, dass sie an dieser Stelle nur exemplarisch genannt und nicht beantwortet werden

29 Neben Zulässigkeitsregeln enthält die DSGVO viele weitere Pflichten. Diese unterscheiden nicht zwischen Verantwortlichen und sind deshalb bei der Verarbeitung öffentlicher Daten gleichermaßen zu beachten. Wenn es um öffentliche Daten geht, kann dies allerdings zu Herausforderungen führen, v.a. bei den Informationspflichten der Art. 12 ff. DSGVO. Dieser Aspekt wird hier ausgeklammert.

können. In Betracht kommen *alle Zulässigkeitstatbestände* des Art. 6 Abs. 1 Unterabs. 1 DSGVO, beispielsweise:

- Eine betroffene Person erteilt einem Journalisten die Einwilligung, in einem Online-Artikel namentlich genannt zu werden (lit. a).
- Die betroffene Person schließt einen Vertrag über den Betrieb einer individualisierten Webpräsenz mit einem Hostprovider (lit. b).
- Eine zuständige Behörde veröffentlicht auf Basis einer nationalen Rechtsvorschrift personenbezogene Daten über die betroffene Person, z.B. nach § 9 Abs. 1 InsO oder nach § 40 Abs. 1a LFGB (lit. c bzw. lit. e).
- Eine Behörde veröffentlicht einen Suchaufruf für eine betroffene Person, die sich in einer lebensbedrohlichen Situation befindet (lit. d, ggf. i.V.m. lit. e und nationalen Vorschriften).
- Ein Verbraucher veröffentlicht eine Bewertung eines Arztes in einem entsprechenden Bewertungsportal (lit. f).

27 Daneben können auch *nationale Rechtsgrundlagen* eine Veröffentlichung tragen, die im Rahmen von Öffnungsklauseln der DSGVO erlassen wurden. Dies betrifft (zumindest in bestimmten, im einzelnen umstrittenen Konstellationen) etwa die Veröffentlichung der Daten von Beschäftigten mit Außenkontakten im Rahmen von § 26 Abs. 1 Satz 1 BDSG.[30]

b) Nachberichtspflicht

28 Ist im konkreten Fall der Tatbestand der einschlägigen Verarbeitungsbefugnis nicht erfüllt, fällt er später weg oder liegt ein anderer Grund aus Art. 17 Abs. 1 DSGVO vor, so ist der Verantwortliche nach dieser Vorschrift zur *Löschung der Daten* verpflichtet. Dies betrifft auch die Entfernung von einer Webpräsenz oder aus einem anderen Veröffentlichungsmedium. Problematisch ist in dieser Konstellation allerdings oftmals, dass die Daten vor der Löschung von *beliebig vielen Dritten* abgerufen worden sein können und nun bei diesen potentiell weiterhin gespeichert und verarbeitet werden.

29 Um der betroffenen Person in diesen Fällen zumindest einen teilweisen ergänzenden Schutz zukommen zu lassen, verpflichtet der – im Gesetzgebungsverfahren stark umstrittene[31] – Art. 17 Abs. 2 DSGVO den Verantwortlichen dazu, *andere Verantwortliche*, die die durch ihn veröffentlichten Daten weiterhin verarbeiten, darüber zu *informieren*, dass die betroffene Person „von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat."[32] Geschuldet wird also nicht eine Löschung bei diesen Dritten, sondern deren Information.[33]

30 Der Gesetzgeber hat außerdem berücksichtigt, dass der erste Verantwortliche in sehr vielen Konstellationen erhebliche Probleme haben wird, die weiteren Verantwortlichen zu ermitteln; bei einer Veröffentlichung im Internet kann es sich grundsätzlich um beliebige Dritte handeln. Deshalb beschränkt Art. 17 Abs. 2 DSGVO die Informationspflicht. Sie erfasst nur „unter Berücksichtigung der *verfügbaren Technologie* und der *Implementierungskosten* angemessene Maßnahmen, auch technischer Art".

31 Diese Einschränkung ist einerseits zwingend, weil ansonsten vom ersten Verantwortlichen Unmögliches verlangt würde. Andererseits schränkt sie die *Wirkung der Pflicht* ganz erheblich *ein*. In bestimmten Sonderkonstellationen – vor allem bei der Veröffentlichung in großen, aber immer noch geschlossenen Nutzergruppen mit bekannten Nutzern – wird es zwar leicht möglich sein, entsprechende Informationen zu verteilen.[34] Für das frei zugängliche Internet existiert hingegen derzeit *keine „verfügbare Technologie"*, mit der man diejenigen, die öffentlich gemachte Daten abgerufen haben und jetzt weiterverarbeiten, identifizieren oder gar benachrichtigen könnte.[35]

32 Denkbar erscheinen lediglich Hilfsinstrumente wie die Information von *Suchmaschinenbetreibern*, bei denen man davon ausgehen kann, dass sie wegen der umfassenden Erhebung von Internetdaten auch die nunmehr gelöschten Daten erhoben haben und zumindest noch eine Zeitlang weiterverarbeiten. Eine Information dieser Betreiber kann auch technisch umgesetzt werden.[36] Für die vielen anderen Konstellationen des Abrufs aus dem Internet bleibt nur, auf eine – derzeit jedoch selbst konzeptionell nicht absehbare – technische Lösung zu hoffen.

33 Mit Blick auf die folgenden Ausführungen ist schließlich wichtig, dass auch eine *erfolgreiche Information* der weiteren Verantwortlichen, die die Daten abgerufen haben, *nicht dazu führt*, dass diese nunmehr aufgrund der Löschungsverpflichtung des ersten, veröffentlichenden Verantwortlichen nunmehr selbst zur Löschung verpflichtet wären.[37] Auch hier gilt, dass die *Verarbeitungsbefugnis* mit Blick auf den *jeweiligen Verantwortlichen* zu bestimmen ist. Die Information durch den ersten Verantwortlichen wird zwar regelmäßig Anlass für weitere Verantwortliche sein, ihre Verarbeitungsbefugnis und eine etwaige Löschungsverpflichtung zu prüfen.[38] Sie ist aber nicht selbst Grund für eine Löschung. Es kann mit anderen Worten ohne weiteres vorkommen, dass der erste Verantwortliche zur

---

30 S. näher *Seifert* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 88 Rz. 183 ff. m.w.N.

31 S. z.B. *Hornung* in Hill/Schliesky, Die Neubestimmung der Privatheit, 2014, 139 ff.; s.a. *Hornung/Hofmann*, JZ 2013, 163 ff.

32 Der Wortlaut ist insoweit missverständlich, als ein solches Verlangen gegenüber konkreten anderen Verantwortlichen in aller Regel nicht möglich sein wird, weil diese der betroffenen Person (noch) nicht bekannt sind. Es geht deshalb um ein entsprechend erweitertes Löschungsverlangen gegenüber dem Verantwortlichen, der die Daten veröffentlicht hat, s. *Dix* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 17 Rz. 26; ähnlich *Herbst* in Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 17 Rz. 52.

33 S. *Kamann/Braun*, in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 17 Rz. 47; *Kamlah* in Plath, DSGVO BDSG, Art. 17 Rz. 15; ein geleakter Entwurf der Kommission vom November 2011 hatte noch eine solche Rechtspflicht enthalten, s. *Hornung* in Hill/Schliesky, Die Neubestimmung der Privatheit, 2014, 141.

34 *Dix* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 17 Rz. 27.

35 S. z.B. *Härting*, BB 2012, 459, 464; *Hornung/Hofmann*, JZ 2013, 163, 168 f.; *Worms* in BeckOK DSR, 30. Edition, Art. 17 Rz. 74.

36 S. *Hornung/Hofmann*, JZ 2013, 163, 168 ff.

37 *Hornung/Hofmann*, JZ 2013, 163, 166; *Dix* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 17 Rz. 28.

38 S. *Hornung/Hofmann*, JZ 2013, 163, 167; *Kamlah* in Plath, DSGVO BDSG, 3. A. 2018, Art. 17 Rz. 15; *Paal/Pauly*, DSGVO BDSG, 2. Aufl. 2018, Art. 17 Rz. 32; *Schantz* in Schantz/Wolf, Das neue Datenschutzrecht, 2017, Rz. 1215; *Veil* in Gierschmann et al., DSGVO, 2017, Art. 17 Rz. 131; *Dix* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 17 Rz. 28.

Löschung auf seiner Webseite verpflichtet ist (beispielsweise nach Fristablauf, so im oben genannten Fall die Behörden gem. § 3 Abs. 1 InsIntBekV oder § 40 Abs. 4a LFGB), ein anderer Verantwortlicher die Daten aber weiter speichern und anderweitig verarbeiten darf (in diesem Beispiel etwa ein Journalist im Rahmen einer Langzeitrecherche über ein Unternehmen). Die im Folgenden erörterten Probleme der Zulässigkeit der Weiterverarbeitung sind deshalb *uneingeschränkt* auch dann *relevant*, wenn eine entsprechende Information erfolgt ist.

2. Grundrechtsrelevanz der Verarbeitung öffentlicher Daten

34 Eine wesentliche Weichenstellung für diese Zulässigkeitsproblematik liegt in der Frage, ob öffentliche Daten *grundrechtlich geschützt* werden. Dies ist sowohl für die staatliche Datenverarbeitung (Grundrechtseingriff) als auch für private Verantwortliche (mittelbare Drittwirkung; Einfluss auf die vielen Abwägungsklauseln der DSGVO)[39] relevant. Durch die Verordnung hat sich dieses Problem auf die europäische Ebene verlagert und betrifft nunmehr v.a. Art. 7 und 8 GRCh.[40] Jedenfalls im Anwendungsbereich der DSGVO kommt es damit nur noch in Randbereichen, v.a. bei den Öffnungsklauseln, auf die Rechtsprechung des BVerfG zu dieser Frage an.[41]

a) Grundrechtseingriff

35 Der EuGH wendet in Datenschutzfällen Art. 7 und 8 GRCh praktisch immer ohne Differenzierung *kumulativ* an. Will man unterscheiden, so ist für Art. 7 GRCh über Art. 52 Abs. 3 S. 1 GRCh die Auslegung von Art. 8 EMRK heranzuziehen. Für beide Normen kommt es darauf an, ob die Daten einen Bezug zum Privat- und Familienleben haben. Hierzu hat der EGMR entschieden, dass die systematische Erhebung und Speicherung von Informationen über eine betroffene Person auch dann in den *Schutzbereich* von Art. 8 EMRK fallen kann, wenn sie aus *öffentlichen Quellen* stammt.[42] Der Umfang des Schutzes ist allerdings davon abhängig, inwieweit das Individuum diesen auch berechtigt erwarten darf.[43] Dies kann in Fällen mit ausgeprägtem *Öffentlichkeitsbezug gemindert* sein oder ganz entfallen,[44] wobei der EGMR und die Literatur nicht immer klar erkennen lassen, ob bereits der Schutzbereich nicht eröffnet sein soll oder lediglich geringere Anforderungen an die Rechtfertigung des Eingriffs gestellt werden.

36 Angesichts der kumulativen Anwendung von Art. 7 und Art. 8 GRCh durch den EuGH ist diese Frage von *untergeordneter Relevanz*. Denn Art. 8 GRCh stellt im Unterschied zu Art. 7 GRCh nicht auf die Privatsphäre, sondern auf den Schutz personenbezogener Daten ab. Der Anwendungsbereich von *Art. 8 GRCh* entspricht insoweit dem der DSGVO (Daten einer identifizierten oder identifizierbaren Person)[45] und *erfasst* auch *öffentliche* personenbezogene Daten. Zwar hat sich der EuGH bisher nicht explizit zu dieser Frage geäußert.[46] Allerdings hat er in mehreren Fällen Art. 7 und Art. 8 GRCh im Rahmen von Abwägungsentscheidungen umstandslos auf Fälle angewendet, in denen die Daten öffentlich waren. Dies betrifft nicht nur Offline-Fälle wie die Videoüberwachung öffentlicher Räume,[47] sondern auch die Verarbeitung *öffentlicher Internetdaten*.[48] Daraus muss gefolgert werden, dass ein Datum nicht aufgrund seiner Öffentlichkeit aus dem Schutzbereich herausfällt. Stellt eine betroffene Person die Daten selbst öffentlich zur Verfügung, so kann darin ein *Grundrechtsverzicht* (oder gerade die Ausübung des Persönlichkeitsrechts) liegen. Inwieweit dies den Eingriff entfallen lässt, ist im Einzelfall zu prüfen.

b) Mittelbare Drittwirkung

37 *Öffentliche* personenbezogene Daten sind damit grundrechtlich *nicht schutzlos* gestellt. Eine Beschränkung des Schutzumfanges kommt je nach Intensität eines Öffentlichkeitsbezugs jedoch in Betracht. Soweit es um die *mittelbare Drittwirkung* im Verhältnis zwischen Privaten geht, ist dies v.a. im Hinblick auf das Grundrecht auf *Informationsfreiheit* nach Art. 11 GRCh zu befürworten. Demnach hat jede Person das Recht, sich anhand von verfügbaren Informationen eine Meinung zu bilden oder sich zu informieren.[49] Da öffentliche personenbezogene Daten frei verfügbar sind, ist es nur folgerichtig, diese zumindest grundsätzlich für die Informationsfreiheit zu öffnen. Daraus können Konflikte mit Persönlichkeitsrechten entstehen, wenn die Daten nicht durch die betroffene Person öffentlich gemacht wurden. Diese Konflikte sind im Wege *praktischer Konkordanz* zu lösen. Hierfür hat der EuGH z.B. in der Entscheidung *Goo-*

---

39 Dazu z.B. *Hornung/Spiecker gen. Döhmann* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 1 Rz. 25 ff.

40 Zum Datenschutz als europäischem Grundrecht umfassend *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, 2012; *Marsch*, Das europäische Datenschutzgrundrecht, 2018.

41 Danach ist die Kenntnisnahme öffentlich zugänglicher Informationen durch staatliche Stellen grundsätzlich kein Grundrechtseingriff, s. BVerfG v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 344 f = CR 2008, 306. Dies ändert sich jedoch, wenn es sich um ein gezieltes Zusammentragen, Speichern und Auswerten (ggf. unter Hinzuziehung weiterer Daten) handelt, s. ebd., 345; näher zur Rspr. *Johannes* in Roßnagel/Friedewald/Hansen (Hrsg.), Die Fortentwicklung des Datenschutzrechts, 2018, 155 ff.; zum Grundrechtseingriff *Martini*, VerwArch 2016, 307, 321 ff.; kritisch zur Rspr. z.B. *Desoi*, Big Data und allgemein zugängliche Daten im Krisenmanagement, 2018, 76 ff.

42 EGMR, Urt. v. 4.5.2000, Rs. 28341/95 (Rotaru/Rumänien), Rz. 43 f. (dort auch ohne Einsatz heimlicher Mittel der Datenbeschaffung); ähnlich für Videoüberwachung EGMR, Urt. 28.1.2003, Rs. 44647/98 (Peck/Vereinigtes Königreich) Rz. 59; allgemein für öffentliche Daten und die Überwachung mittels GPS EGMR, Urt. v. 2.9.2010, Rs. 35623/05 (Uzun/Deutschland), NJW 2011, 1333, Rz. 43 ff.; eher restriktive Übertragung dieser Rspr. auf Internetsachverhalte bei *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, 2017, 33 ff., 110.

43 S. für öffentliche Daten EGMR v. 24.6.2004 - 59320/00, AfP 2004, 348 = NJW 2004, 2647, 2648 Rz. 50 ff., 69, 78 - Fotoaufnahmen; Urt. v. 28.4.2003, Rs. 44647/98 (Peck/UK), Rz. 58 - Videoüberwachung; allgemein z.B. EGMR, Urt. v. 25.6.1997, Rs. 20605/92 - Halford/UK, Rz. 42 ff.; Urt. v. 25.12.2001, Rs. 44787/98 - P.G. and J.H./UK Rz. 57; Urt. v. 17.10.2003, Rs. 63737/00 - Perry/UK Rz. 36 ff.; Urt. v. 26.7.2007, Rs. 64209/01 - Peev/Bulgaria Rz. 37 ff.

44 *Bernsdorff* in Meyer, GRCh, 4. A. 2014, Art. 7 Rz. 19 m.w.N.; *Gersdorf* in BeckOK InfR, 23. Edition, Art. 7 Rz. 21.

45 Z.B. *Kühling/Raab* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Einf. Rz. 27.

46 Anders für die vorgelagerte Frage der Veröffentlichung personenbezogener Daten durch staatliche Stellen, die explizit als Grundrechtseingriff beurteilt wird, s. z.B. EuGH v. 9.11.2010 - C-92/09, C-93/09, ECLI:EU:C:2010:662, CR 2011, 271 = MMR 2011, 122 m. Anm. *Hornung*.

47 EuGH v. 11.12.2014 - C-212/13, ECLI:EU:C:2014:2428, CR 2015, 100 m. Anm. *Bretthauer* = NJW 2015, 463 -Ryneš.

48 EuGH - C-468, 469/10, EuZW 2012, 37 - ASNEF/FECEMD; EuGH v. 13.5.2014 - C-131/12, ECLI:EU:C:2014:317, AfP 2014, 245 = CR 2014, 460 = NJW 2014, 2257 - Google Spain.

49 *Bernsdorff* in Meyer, GRCh, 4. Aufl. 2014, Art. 11 Rz. 13 m.w.N.; *Kühling* in Heselhaus/Nowak, HB EU-Grundrechte, 2006, § 23 Rz. 20; *Jarass*, GRCh, 3. Aufl. 2016, Art. 11 Rz. 15.

gle Spain[50] und jüngeren Folgeentscheidungen[51] Leitlinien entwickelt, die noch weiter ausgearbeitet werden müssen.

3. Differenzierung zwischen Datenarten

38 Im Rahmen der DSGVO richtet sich die Zulässigkeit der Datenverarbeitung allgemein nach den Rechtmäßigkeitstatbeständen des Art. 6 Abs. 1 Unterabs. 1 DSGVO. Für die *„besonderen Kategorien* personenbezogener Daten" nach Art. 9 Abs. 1 DSGVO tritt eine Verschärfung hinzu, wonach die Verarbeitung unabhängig von Art. 6 Abs. 1 Unterabs. 1 DSGVO *prinzipiell verboten ist*, solange nicht einer der Tatbestände des Art. 9 Abs. 2 DSGVO eingreift. Art. 9 DSGVO ist für die Verarbeitung öffentlicher Daten von besonderer Bedeutung, da zum einen viele dieser Daten (z.B. im Internet) unter eine der genannten Kategorien fallen[52] und zum anderen einer mit Art. 9 Abs. 2 lit. e DSGVO einer der Ausnahmetatbestände hier *explizit einschlägig* ist. Schließlich ist das systematische Verhältnis zwischen Art. 6 und Art. 9 DSGVO nicht endgültig geklärt. Aus diesen Gründen wird Art. 9 DSGVO hier vor der allgemeinen Zulässigkeitsnorm des Art. 6 DSGVO behandelt.

39 Im Unterschied zu den öffentlichen Daten haben die offensichtlich durch die betroffene Person öffentlich gemachten personenbezogenen Daten Eingang in die Verordnung gefunden. Gemäß Art. 9 Abs. 2 lit. e DSGVO ist das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten allgemein[53] aufgehoben, wenn sich die Verarbeitung auf personenbezogene Daten bezieht, die die betroffene Person *offensichtlich selbst öffentlich gemacht* hat (dazu oben Rz. 11 ff.).

40 In der Literatur wird mitunter verkannt, dass das Verhältnis zwischen Art. 9 und Art. 6 DSGVO komplexer ist, als es auf den ersten Blick erscheint. So findet sich teilweise die pauschale Aussage, Art. 9 DSGVO verdränge Art. 6 Abs. 1-3 DSGVO[54] oder sei *lex specialis* zu ihnen.[55] Dies ist jedoch *nicht zutreffend*, sondern in den Ausnahmefällen des Art. 9 Abs. 2 DSGVO greifen zusätzlich die Anforderungen des Art. 6 DSGVO (s.u. Rz. 42 ff.).[56] Art. 9 Abs. 2 DSGVO lässt nämlich ausdrücklich nur das Verbot der Verarbeitung nach „Absatz 1" entfallen, trifft aber keine Aussage zur grundsätzlichen Rechtmäßigkeit der Verarbeitung. Auch nach EG 51 S. 5 DSGVO sind zusätzlich zu den speziellen Anforderungen des Art. 9 DSGVO die allgemeinen Bedingungen für die rechtmäßige Verarbeitung einzuhalten.[57] Würde dies anders gesehen, stünden sensible *offensichtlich* durch die betroffene Person *öffentlich gemachte* Daten unter einem geringeren Schutz als einfache durch die betroffene Person *öffentlich gemachte* Daten, da sich die Verarbeitung Letzterer an der Interessenabwägung des Art. 6 Abs. 1 Unterabs. 1 DSGVO messen lassen muss, selbst wenn diese *offensichtlich* durch die betroffene Person *öffentlich gemacht* wurden.[58] Dies entspräche nicht dem Sinn und Zweck der Verordnung.

41 Nur auf diesem Weg kann schließlich das wichtige Problem adressiert werden, dass Art. 9 Abs. 2 lit. e DSGVO das Verarbeitungsverbot dauerhaft entfallen lässt, die *Risiken einer Verarbeitung* der öffentlich gemachten Daten sich seit dem Öffentlichmachen aber *geändert haben* können. Hinter Art. 9 Abs. 2 lit. e DSGVO steht der Gedanke der freiverantwortlichen Entscheidung der betroffenen Person, ihre personenbezogenen Daten der Öffentlichkeit zu überantworten. Die nachvollziehbare Wertung des Gesetzgebers verknüpft – wie in anderen Rechts- und Lebensbereichen auch – Selbstbestimmung mit Verantwortung und mutet dem Einzelnen zu, mit den Folgen seiner Entscheidung zu leben. Allerdings kann diese Verknüpfung an Legitimation einbüßen, wenn die betroffene Person die *Folgen* ihrer Entscheidung *nicht vorhersehen* konnte, weil die öffentlich gemachten Daten unter anderen technischen Verarbeitungsbedingungen, anderen individuellen Lebensverhältnissen oder in den Händen anderer Verantwortlicher völlig *andere persönlichkeitsrechtliche Folgen* haben können.[59] Art. 9 Abs. 2 lit. e DSGVO hält hierfür keine Lösung parat – die einmal öffentlich gemachten Daten wären tatsächlich für immer schutzlos. Die Anwendung von Art. 6 Abs. 1 Unterabs. 1 DSGVO (insbesondere lit. f) ermöglicht hingegen zumindest in Ausnahmefällen (s.u. Rz. 50 ff.) eine *Beschränkung der Verarbeitungsbefugnis*.

---

50 EuGH v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317, AfP 2014, 245 = CR 2014, 460 = NJW 2014, 2257, Rz. 93 ff. – Google Spain.

51 EuGH v. 24.9.2019 – C-507/17, ECLI:EU:C:2019:772, NJW 2019, 3499 – Google LLC/CNIL; EuGH v. 24.9.2019 – C-136/17, ECLI:EU:C:2019:773, NJW 2019, 3503 – GC ua/CNIL.

52 Dies sind 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.

53 Daneben können auch die anderen Ausnahmetatbestände eine Verarbeitung öffentlicher oder veröffentlichter sensibler Daten erfassen, z.B. zu Forschungszwecken Art. 9 Abs. 2 lit. j. DSGVO i.V.m. § 27 Abs. 1 S. 1 BDSG, s. *Golla/Hofmann/Bäcker*, DuD 2018, 89, 93.

54 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 3 Rz. 58; *Kampert* in Sydow, DSGVO, 2. Aufl. 2018, Art. 9 Rz. 63; *Greve* in Auernhammer, DSGVO BDSG, 6. Aufl. 2018, Art. 9 Rz. 16; ähnlich *Laue/Nink/Kremer*, Das neue Datenschutzrecht, § 2 Rz. 58 („findet [...] keine Anwendung"); offengelassen, aber mit ähnlicher Tendenz *Korge* in Gierschmann et al., DSGVO, 2017, Art. 9 Rz. 3.

55 *Mester* in Taeger/Gabel, DSGVO BDSG, 2019, Art. 9 Rz. 2; *Schulz* in Gola, DSGVO, 2017, Art. 9 Rz. 1 (allerdings widersprüchlich, da in Rz. 23 für den Fall der Veröffentlichung nach lit. e und in Rz. 27 sogar allgemein die Anwendung von Art. 6 Abs. 1 DSGVO vertreten wurde); nunmehr offengelassen: 2. Aufl. 2018, Art. 9 Rz. 5.

56 *Wedde* in Däubler et al., DSGVO BDSG, 2018, Art. 9 Rz. 3; *Jaspers/Schwartmann/Mühlenbeck* in Schwartmann et al., DSGVO BDSG, 2018, Art. 9 Rz. 111; *Albers/Veit* in BeckOK DSR, 30. Edition, Art. 9 Rz. 24 f., 64; *Golla/Hofmann/Bäcker*, DuD 2018, 89, 92 f.; *Robrahn/Bremert*, ZD 2018, 291, 295; speziell für Art. 6 Abs. 4 DSGVO auch *Weichert* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 9 Rz. 4; a.A. zu diesem Punkt *Schiff* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 9 Rz. 10 f. (wo allerdings die Zweckänderung allein auf Art. 9 DSGVO gestützt und dabei übersehen wird, dass die kumulative Anwendung der Normen das Schutzniveau gerade erhöhen würde; s. dazu *Albers/Veit* in BeckOK DSR, 30. Edition, Art. 9 Rz. 24 f.).

57 S. den Verweis bei *Petri* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 9 Rz. 2.

58 Ebenso *Robrahn/Bremert*, ZD 2018, 291 (295).

59 Dementsprechend hat der EuGH (freilich für die Veröffentlichung durch Dritte) betont, dass auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten im Laufe der Zeit nicht mehr den Bestimmungen des Datenschutzrecht entsprechen kann, s. EuGH v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317, AfP 2014, 245 = CR 2014, 460 = NJW 2014, 2257, 2264 – Google Spain.

4. Differenzierung nach Verantwortlichen

a) Verarbeitung durch private Stellen

42 Damit ist sowohl innerhalb wie außerhalb des Anwendungsbereichs von Art. 9 DSGVO eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO für die Verarbeitung erforderlich.

aa) Fehlende Eignung der Einwilligung

43 Hierfür kommt eine Einwilligung der betroffenen Person i.S.v. Art. 6 Abs. 1 Unterabs. 1 lit. a DSGVO i.a.R. nicht in Betracht. Gemäß Art. 4 Nr. 11, EG 32 DSGVO hat die Einwilligung durch eine eindeutige bestätigende Handlung zu erfolgen, mit der in informierter Weise bekundet wird, dass die betroffene Person mit der Verarbeitung einverstanden ist. Aus der Tatsache der Veröffentlichung kann aber zum einen *nicht eindeutig entnommen* werden, dass die Person in die Weiterverarbeitung einwilligt. Zum anderen *fehlt* es an der *Informiertheit*, da die betroffene Person nicht wissen wird, welche Daten zu welchem Zweck durch wen verarbeitet werden. Eine pauschale Einwilligung für alle Verantwortlichen zu allen denkbaren Zwecken würde nicht i.S.v. Art. 4 Nr. 11 DSGVO „für den bestimmten Fall" erfolgen.

44 Ist die Veröffentlichung nicht durch die betroffene Person selbst und ohne deren offensichtliche Zustimmung erfolgt, kommt eine Einwilligung ohnehin nicht in Frage. Hier geht die Handlung gar nicht erst von der betroffenen Person aus. Der Verantwortliche hätte zwar die Möglichkeit, in jedem einzelnen Fall eine ausdrückliche und informierte Einwilligung einzuholen, dieses Vorgehen ist jedoch im (Geschäfts-) Alltag *wenig praktikabel*.

bb) Struktur der Abwägung nach Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO

45 Als Rechtsgrundlage für die Verarbeitung kommt deshalb hauptsächlich Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO in Betracht.[60] Demnach ist eine Verarbeitung zulässig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Um die Verarbeitung auf Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO stützen zu können, bedarf es somit *erstens* eines berechtigten Interesses des Verantwortlichen oder eines Dritten. *Zweitens* muss die Verarbeitung zur Wahrung dieses Interesses erforderlich sein. *Drittens* dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person die Interessen des Verantwortlichen nicht überwiegen.[61]

(1) Berechtigtes Interesse und Erforderlichkeit

46 Ein Interesse i.S.d. Norm kann jedes *wirtschaftliche* oder *ideelle Interesse* sein.[62] Das Interesse ist berechtigt, wenn es nicht gegen die Rechtsordnung der Mitgliedstaaten oder der Union verstößt.[63] EG 47, 48 DSGVO nennen einige berechtigte Interessen, die jedoch keinen Bezug zur Verarbeitung öffentlicher personenbezogener Daten haben. Auch ohne derartige Erwähnung wird es aber sehr viele Konstellationen geben, in denen z.B. aus Gründen der Berufs- oder Informationsfreiheit (Art. 15, 11 GRCh) berechtigte Interessen an der Verarbeitung derartiger Daten zu bejahen sind. Von den Grundrechten und Grundfreiheiten, auf die sich gegenläufig die betroffene Person berufen kann, ist wenigstens Art. 8 GRCh betroffen, in entsprechenden Fallkonstellationen zudem Art. 7 GRCh und Art. 8 EMRK. Aber auch die Beeinträchtigung weiterer Grundrechte ist denkbar,[64] etwa der Gleichheitsrechte.[65] Das Kriterium der Erforderlichkeit ist erfüllt, wenn die Datenverarbeitung geeignet ist, den Interessen des Verantwortlichen zu dienen und eine weniger datenintensive Verarbeitung nicht in Frage kommt.[66]

(2) Abwägung

47 Bei der Abwägung der widerstreitenden Interessen gilt die Faustformel: Je höher das Risiko der Verarbeitung und je schwerwiegender der Eingriff in die Rechte und Interessen der betroffenen Person, umso schwerer müssen die Interessen des Verantwortlichen wiegen, damit eine Verarbeitung als rechtmäßig beurteilt werden kann.[67] Die Verordnung gibt für die Abwägungsfaktoren und ihre Gewichtung ansonsten so gut wie keine Hinweise. EG 47 S. 1 HS 2, S. 3 und S. 4 DSGVO stellen auf die *vernünftigen Erwartungen* der betroffenen Person hinsichtlich der Verarbeitung ab.[68] Dabei bleibt aber unklar, ob sich diese Fälle auf Erwartungen aus einer Beziehung zum Verantwortlichen begründen sollen (so EG 47 S. 1 DSGVO) oder ganz allgemein zu berücksichtigen sind (in diese Richtung S. 4 und wohl auch S. 3).

48 Es verwundert deshalb nicht, dass in der Literatur eine große Bandbreite von Abwägungsfaktoren vorgeschlagen wird. Die Kriterien lassen sich in drei Gruppen systematisieren, nämlich Besonderheiten

---

60 In Sonderkonstellationen kann die Verarbeitung auch zur Vertragserfüllung (Art. 6 Abs. 1 Unterabs. 1 lit. b DSGVO) erforderlich sein. Dies wird insbesondere für die Erhebung von Bewerberdaten aus dem Internet diskutiert, deren Zulässigkeit str. ist (s. ablehnend *Däubler* in Däubler et al., DSGVO BDSG, 2018, § 26 Rz. 45–46; bejahend *Forst* in Auernhammer, 6. Aufl. 2018, § 26 Rz. 19; *Franzen* in ErfK, 19. A. 2019, § 26 Rz. 19; *Gola* in Gola/Heckmann, BDSG, 13. A. 2019, § 26 Rz. 61). Die Frage wird hier ausgeklammert.

61 *Heberlein*, Datenschutz im Social Web, 2017, 127; *Kramer* in Auernhammer, DSGVO BDSG, 6. Aufl. 2018, Art. 6 Rz. 45; *Assion/Nolte/Veil* in Gierschmann et al., DSGVO, 2017, Art. 6 Rz. 128.

62 *Schulz* in Gola, DSGVO, 2. Aufl. 2018, Art. 6 Rz. 57; *Albers/Veit* in BeckOK DSR, 30. Edition, Art. 6 DSGVO Rz. 49; *Frenzel* in Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 6 Rz. 28; *Reimer* in Sydow, DSGVO, 2. Aufl. 2018, Art. 6 Rz. 54; *Buchner/Petri* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 6 Rz. 146.

63 *Heberlein* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 6 Rz. 25; *Schwartmann/Klein* in Schwartmann et al., DSGVO BDSG, 2018, Art. 6 Rz. 116; *Robrahn/Bremert*, ZD 2018, 291, 292 f.; *Plath* in Plath, BDSG/DSGVO, 3. Aufl. 2018, Art. 6 Rz. 21.

64 Dies wird in EG 4 S. 3 festgehalten; näher *Hornung/Spiecker gen. Döhmann* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 1 Rz. 30 ff.

65 S. am Beispiel öffentlicher Daten *Desoi* (Fn. 41), 103 ff.

66 *Plath* in Plath, DSGVO, 3. Aufl. 2018, Art. 6 Rz. 23; *Robrahn/Bremert*, ZD 2018, 291, 292; *Kramer* in Auernhammer, DSGVO BDSG, 6. Aufl. 2018, Art. 6 Rz. 50.

67 Siehe *Herfurth*, ZD 2018, 514 ff., welcher sich eingehend mit den Kriterien für die Interessenabwägung auseinandersetzt und zur objektiven Bewertung ein sog. „3x5-Modell" vorschlägt.

68 Das englische „expectation" bzw. „expect" wird in der deutschen Fassung von EG 47 dreimal unterschiedlich übersetzt, nämlich als Erwartung (S. 1), absehen können (S. 3) und rechnen müssen (S. 4).

- der *verarbeiteten Daten* (Art, Menge, Quelle und Qualität der Daten),
- der *Akteure* (Verantwortliche und betroffene Personen, einschließlich Machtverhältnissen und vernünftigen Erwartungen) und
- der *Verarbeitung selbst* (Art, Dauer, Häufigkeit und Zwecke der Datenverarbeitung).[69]

49 Dabei spielen auch Vorkehrungen des Verantwortlichen eine Rolle, welche über die gesetzlichen Anforderungen hinausgehen und das bestehende Risiko der Verarbeitung verringern, die Transparenz für die betroffene Person erhöhen oder zusätzliche technische und organisatorische Maßnahmen vorsehen.[70] Der Verantwortliche hat hierdurch die Möglichkeit, zu seinen Gunsten auf die Abwägung einzuwirken.

cc) Abwägung bei öffentlichen Daten

50 Die genannten Abwägungsfaktoren können auch bei der Verarbeitung öffentlicher Daten von unterschiedlichem Gewicht sein. Übergreifend stellt sich allerdings die Frage, ob sich die Abwägung gerade wegen des öffentlichen Charakters der zu verarbeitenden Daten typisieren und sich daraus ein Argument gewinnen lässt, zumindest *prima facie* die Abwägung zugunsten der *berechtigten Interessen* des Verantwortlichen ausfallen zu lassen.

51 Im *Text der DSGVO* findet sich kein Anhaltspunkt für eine derartige Zweifelsregelung für die Abwägung. Demgegenüber hatte der Gesetzgeber des *BDSG a.F.* für öffentliche (d.h. *„allgemein zugängliche"*) Daten eine typisierte Abwägung vorgenommen. Während die Erhebung personenbezogener Daten zur Erfüllung eigener Geschäftszwecke bspw. allgemein nur dann auf berechtigte Interessen gestützt werden konnte, wenn kein Grund zu der Annahme bestand, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwog (§ 28 Abs. 1 S. 1 Nr. 2 BDSG a.F.), bestand bei allgemein zugänglichen Daten eine Vermutung für die Zulässigkeit der Erhebung, solange das schutzwürdige Interesse des Betroffenen nicht „offensichtlich" überwog. Bei Abweichungen im Detail folgten etliche weitere Vorschriften diesem Muster.[71]

52 An dieser wie an vergleichbaren Stellen gilt, dass gegenüber einer Übernahme derartiger früherer nationaler Regelungen in die Auslegung abstrakter Generalklauseln der DSGVO große Skepsis angebracht ist. Ein solches Vorgehen birgt die Gefahr, den Harmonisierungszweck der DSGVO (s. EG 9 f.) zu unterlaufen. Erforderlich ist eine autonome europäische Auslegung mit entsprechender Methodik.[72] Allerdings kann diese natürlich auch zu dem Ergebnis kommen, dass frühere nationale gesetzliche Typisierungen weiterhin als Auslegungsargumente für die DSGVO valide sind.

(1) Grundsätzliche Privilegierung der Verarbeitung

53 Diesem Kriterium hält die frühere deutsche *„Privilegierung"* der Verarbeitung öffentlicher Daten zumindest im Grundsatz stand: Auch auf Basis einer autonomen Auslegung ist es sinnvoll und angemessen, das Kriterium der Öffentlichkeit der Daten im Rahmen der Abwägung nach Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO zu berücksichtigen.[73]

54 Hierfür sprechen *erstens* grundrechtliche Überlegungen. Die in Art. 11 GRCh verankerte *Informationsfreiheit* schützt die Wahrnehmung öffentlich zugänglicher Informationen.[74] *Zweitens* muss Art. 9 Abs. 2 lit. e DSGVO im Wege des Erst-recht-Schlusses berücksichtigt werden: Wenn die eigene Veröffentlichung von Daten sogar die strengeren Anforderungen des Art. 9 Abs. 1 DSGVO überwindet, so ist dies auch im Rahmen der Abwägung nach Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO relevant.[75] *Drittens* steht hinter der Unterscheidung zwischen öffentlich zugänglichen und sonstigen Daten eine weitere Erwägung: Sind Daten nämlich einmal öffentlich, ändert sich zum einen die *Erwartung der Verantwortlichen*, die nun davon ausgehen, dass faktisch ohne Zugangshürden wahrnehmbare Daten zumindest grundsätzlich auch verarbeitbar sind. Zum anderen ändert sich zugleich die *Erwartung der betroffenen Personen*, die ihrerseits damit rechnen, dass andere die Daten wahrnehmen. Letzteres ist im Rahmen der Abwägung gemäß EG 47 DSGVO zu berücksichtigen, weil die betroffenen Personen jedenfalls faktisch keine Erwartung mehr haben können, dass die Daten vertraulich bleiben. Zu berücksichtigen ist allerdings, dass EG 47 DSGVO im Ergebnis keine faktische, sondern eine *normative Bewertung* der vernünftigen Erwartungen verlangt. Dies gilt insbesondere, weil die öffentliche Zugänglichmachung ihrerseits *rechtswidrig* sein kann[76] und ggf. sehr sensible Daten umfasst, wie sich an Hackerangriffen immer wieder zeigt. In derartigen Fällen kann es rasch dazu kommen, dass der Faktor der *Allgemeinzugänglichkeit* in den *Hintergrund* tritt und die Verarbeitung dennoch rechtswidrig ist.

(2) Differenzierung nach Veröffentlichung

55 Innerhalb der Gruppe der *öffentlichen* Daten ist deshalb (vor-) entscheidend danach zu differenzieren, wer die Daten *öffentlich gemacht* hat. Ist dies die betroffene *Person selbst*, so wird die

---

69 S. *Herfurth*, ZD 2018, 514 ff.; weitere Systematisierungen bei *Schulz* in Gola, DSGVO, 2. Aufl. 2018, Art. 6 Rz. 59 ff.; *Buchner/Petri* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 6 Rz. 149 ff.; *Robrahn/Bremert*, ZD 2018, 291, 294.

70 *Reimer* in Sydow, DSGVO, 2. Aufl. 2018, Art. 6 Rz. 62; *Schwartmann/Klein* in Schwartmann et al., 2018, Art. 6 Rz. 129; *Assion/Nolte/Veil* in Gierschmann et al., DSGVO, 2017, Art. 6 Rz. 143.

71 S. Fn. 3; zur Anwendung auf öffentliche Daten im Social Media Monitoring *Solmecke/Wahlers*, ZD 2012, 550, 552 f.; *Venzke-Caprarese*, DuD 2013, 775.

72 Methodisch zweifelhaft insoweit zur hiesigen Fragestellung *Born* in Taeger (Hrsg.), Recht 4.0, 2017, 13, 24 f.

73 Ebenso für die DSRL, aber ohne detailliertere Begründung und ohne die im Folgenden genannten Differenzierungen, EuGH – C-468, 469/10, EuZW 2012, 37 Rz. 44 f.; v. 4.5.2017 – C-13/16, ECLI:EU:C:2017:336, CR 2017, 504 Rz. 32; v. 11.12.2019 – C-708/18, ECLI:EU:C:2019:1064, ZD 2020, 148 Rz. 54 f.; für die DSGVO im Grundsatz *Schantz* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DSGVO, Rz. 131 m.w.N.; *Schulz* in Gola, DSGVO, 2. Aufl. 2018, Art. 6 Rz. 59; *Plath* in Plath, BDSG/DSGVO, 3. Aufl. 2018, Art. 6 Rz. 21; *Taeger* in Taeger/Gabel, DSGVO BDSG, 2019, Art. 6 Rz. 122; *Heberlein*, Datenschutz im Social Web, 2017, 129 f.; *Herfurth*, ZD 2018, 514, 516 f.; *Dallmann/Busse*, ZD 2019, 394, 395 f.

74 Dies gilt, obwohl die Norm anders als Art. 5 Abs. 1 S. 1, Alt. 2 GG sich nicht explizit auf allgemein zugängliche Quellen bezieht.

75 *Schantz* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DSGVO, Rz. 131; *Schwarz*, ZD 2018, 353, 355.

76 Dazu oben Rz. 23 ff.

Eingriffsintensität in aller Regel geringer sein.[77] Zentrales Argument hierfür ist, dass die Veröffentlichung der eigenen Daten zum Ausdruck bringt, dass deren Inhalt *nicht als privat genug* erachtet wird, um sie der Öffentlichkeit zu entziehen. Die betroffene Person verliert an Schutzwürdigkeit. Dies hat der Gesetzgeber durch Art. 9 Abs. 2 lit. e DSGVO normativ anerkannt (s.o. Rz. 38 ff.) und ist dementsprechend erst recht für „normale" personenbezogene Daten zu berücksichtigen. Im Ergebnis wird daher die Interessenabwägung bei durch die betroffene Person veröffentlichten Daten regelmäßig zugunsten des Verantwortlichen ausgehen und die Datenverarbeitung zulässig sein. Allerdings kann es durchaus Ausnahmen hiervon geben, wenn bspw. Daten nach sehr langer Zeit (ggf. in Kombination mit weiteren Daten) eine andere Persönlichkeitsrelevanz erhalten, die Daten nicht mehr aktuell sind, die betroffene Person bei ihrer Entscheidung noch minderjährig war oder es um *eingriffsintensive Formen und Zwecke* der Verarbeitung geht. Dies gilt beispielsweise für Weiterverarbeitungen von Daten, die aus heterogenen öffentlichen Quellen zu Profilen kombiniert werden und so in neue Aussagegehalte münden.[78] Zumindest in Kombination können derartige Faktoren die Abwägung zugunsten der betroffenen Person ausfallen lassen.[79]

56 Sollen *durch Dritte veröffentlichte* personenbezogene Daten verarbeitet werden, ist die Eingriffsintensität geringer als bei privat gehaltenen, aber höher als bei durch die betroffene Person veröffentlichten Daten. Diese hat in solchen Fällen nicht selbst über die Veröffentlichung entschieden, weswegen ihr Schutzinteresse höher ist. Auf Seite des Verantwortlichen ist das Recht auf *Informationsfreiheit* gem. Art. 11 GRCh hervorzuheben. Dieses umfasst *alle allgemein zugänglichen* Informationen,[80] d.h. nicht nur Daten, die durch die betroffene Person selbst veröffentlicht werden. Das Informationsfreiheitsrecht kann zwar zugunsten des Datenschutzrechts beschränkt werden,[81] so dass im Konfliktfall im Wege *praktischer Konkordanz* nach Lösungen gesucht werden muss, die sich in der einfachgesetzlichen Abwägung niederschlagen. Allerdings sind *öffentliche* personenbezogene Daten aufgrund ihrer allgemeinen Zugänglichkeit *weniger schützenswert* als private.[82] Im Ergebnis wird die Abwägung deshalb vielfach zugunsten des Verantwortlichen ausfallen, die Waagschale kann aber im Einzelfall durchaus leichter zugunsten der betroffenen Person ausfallen als bei *selbst veröffentlichten* Daten. Der Verantwortliche hat deshalb zu prüfen, ob die betroffene Person schwerwiegende Interessen vorweisen kann, die Daten sensibel oder missbrauchsanfällig sind, erkennbar rechtswidrig veröffentlicht wurden[83] oder von Kindern stammen. Insbesondere im Falle der (aus den Umständen oder z.B. einer Information nach Art. 17 Abs. 2 DSGVO)[84] *erkennbar rechtswidrigen Veröffentlichung* wird es außerdem häufig bereits an der Erforderlichkeit i.S.v. Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO fehlen. Sollte die betroffene Person subjektive, in ihrer Person liegende besondere Interessen an dem Unterlassen der Verarbeitung haben, kann sie dieser gem. Art. 21 DSGVO widersprechen.

57 Im Ergebnis ist die *Öffentlichkeit* der Daten zwar ein wichtiger, aber eben nur ein Abwägungsfaktor unter vielen anderen. Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO ist offen für relevante und grundrechtlich fundierte Abwägungsfaktoren wie die Öffentlichkeit. Es ist aber angesichts des völligen Fehlens textlicher Anhaltspunkte nicht möglich, diesem Faktor dieselbe Bedeutung zuzumessen wie nach dem BDSG a.F., wo die Öffentlichkeit vielfach zu einer grundsätzlichen Vermutung der Zulässigkeit der Verarbeitung führte und die Abwägung damit entscheidend beeinflusste. In diesem Sinne hat die Öffentlichkeit personenbezogener Daten ihre frühere überragende Bedeutung für die Zulässigkeit verloren und kann *einfacher* durch *andere Abwägungsfaktoren überspielt* werden als nach altem Recht.

b) Verarbeitung durch öffentliche Stellen

58 Öffentliche personenbezogene Daten können auch für öffentliche Stellen eine *wertvolle Informationsquelle* darstellen. Soweit dies allerdings den Bereich der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung betrifft, kommt nach Art. 2 Abs. 2 lit. d DSGVO die *JI-Richtlinie* zur Anwendung, die ihren Anwendungsbereich komplementär in ihrem Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 regelt.[85]

59 Eine *Privilegierung* der Verarbeitung von öffentlichen Daten sieht die Verordnung auch für Behörden *nicht vor*.[86] Solche Verarbeitungen müssen sich also im Anwendungsbereich der DSGVO auf eine allgemeine Rechtsgrundlage nach Art. 6 Abs. 1 Unterabs. 1 DSGVO stützen. Ebenso wie bei den privaten Stellen stellt die Einwilligung gem. Art. 6 Abs. 1 Unterabs. 1 lit. a DSGVO (jenseits der umstrittenen Frage des zulässigen Einsatzes gegenüber öffentlichen Stellen)[87] i.d.R. keine praktikable Lösung dar. Auch die Tatbestände des Art. 6 Abs. 1 Unterabs. 1 lit. c und d DSGVO kommen nur in seltenen Aus-

77 *Schulz* in Gola, DSGVO, 2. Aufl. 2018, Art. 6 Rz. 59; *Assion/Nolte/Veil* in Gierschmann et al., DSGVO, 2017, Art. 6 Rz. 136, 142; *Plath* in Plath, DSGVO BDSG, 3. A. 2018, Art. 6 Rz. 21.

78 S. für das Beispiel automatisierter Persönlichkeitsanalysen zu Zwecken von „Backgroundchecks" *Dallmann/Busse*, ZD 2019, 394, 397.

79 S. zu einzelnen Abwägungskriterien bei öffentlichen Daten auch *Desoi* (Fn. 41), 93 ff. Im Falle der Unzulässigkeit wird die wesentliche Herausforderung die Kontrollierbarkeit sein. Dieses Vollzugsproblem wird hier trotz seiner Bedeutung ausgeklammert. Jedenfalls sollte nicht argumentiert werden, aufgrund dieses Problems falle die materiell-rechtliche Abwägung zugunsten der Zulässigkeit der Verarbeitung aus.

80 *v. Coelln* in Stern/Sachs, GRCh, 2016, Art. 11 Rz. 22; *Cornils* in BeckOK InfR, 23. Edition, Art. 10 EMRK Rz. 20; *Kühling* in Heselhaus/Nowak, HB EU-Grundrechte, 2006, § 23 Rz. 20 m.w.N.

81 S. Art. 11 Abs. 1 GRCh i.V.m. Art. 52 Abs. 3 GRCh, Art. 10 Abs. 2 EMRK.

82 So auch EuGH – C-468, 469/10, EuZW 2012, 37 Rz. 44 f.; EuGH v. 4.5.2017 – C-13/16, ECLI:EU:C:2017:336, CR 2017, 504 Rz. 32; EuGH v. 11.12.2019 – C-708/18, ECLI:EU:C:2019:1064, ZD 2020, 148 Rz. 54 f.

83 S. dazu oben Rz. 23 ff.

84 S. oben Rz. 28 ff.

85 Zur Abgrenzung der Anwendungsbereiche s. *Hornung/Schindler/Schneider*, ZIS 2018, 566; s.a. *Bäcker* in Hill/Kugelmann/Martini (Hrsg.), Perspektiven der digitalen Lebenswelt, 2017, 63. Das jüngste Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 enthält z.B. keine Bestimmungen für öffentliche Daten. Der Bereich der Umsetzung der JI-Richtlinie und die Erhebung öffentlicher Daten zu Sicherheitszwecken allgemein werden hier ausgeklammert, s. dazu *Johannes* in Roßnagel/Friedewald/Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018, S. 151.

86 Anders noch § 13 Abs. 2 Nr. 4, und § 14 Abs. 2 Nr. 5 BDSG a.F.

87 S. *Heckmann/Paschke* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 7 Rz. 51 ff.; *Buchner/Kühling* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 7 Rz. 15; *Schantz* in Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rz. 511.

nahmefällen in Betracht.[88] Zudem findet die Interessenabwägung nach Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO gem. Unterabs. 2 für öffentlichen Stellen in Erfüllung ihrer Aufgaben keine Anwendung.

60 Folglich stellt Art. 6 Abs. 1 Unterabs. 1 lit. e DSGVO den zentralen Tatbestand für öffentliche Stellen dar. Demnach ist eine Verarbeitung zulässig, wenn sie für die Wahrnehmung einer *Aufgabe im öffentlichen Interesse* oder in *Ausübung öffentlicher Gewalt* erfolgt. Gemäß Art. 6 Abs. 3 S. 1 DSGVO muss diese Rechtsgrundlage im Unionsrecht oder dem Recht des Mitgliedstaates, dem der Verantwortliche unterliegt, festgelegt sein.

61 Art. 6 Abs. 2 DSGVO erlaubt den Mitgliedstaaten, spezifischere Bestimmungen zu Art. 6 Abs. 1 Unterabs. 1 lit. c und e DSGVO zu erlassen oder beizubehalten. Anders als unlängst durch das *BVerwG* entschieden,[89] kann eine solche spezifischere Bestimmung auch eine *Abwägungslösung* umfassen.[90] Im Rahmen einer derartigen Konkretisierung wäre es durchaus möglich, eine *erleichterte Zulässigkeit* der Verarbeitung öffentlicher Daten durch Behörden vorzusehen. Der deutsche Gesetzgeber hat diese Möglichkeit allerdings bisher weder im BDSG n.F. noch an anderer Stelle genutzt.

62 Ob öffentliche Stellen *allgemein zugängliche* personenbezogene Daten verarbeiten dürfen, richtet sich damit nach den jeweiligen spezialgesetzlichen Rechtsgrundlagen. Soweit diese bestimmte Datenarten oder Erhebungsformen auflisten, die im Falle der Erhebung öffentlicher Daten nicht einschlägig sind (z.B. eine Erhebung unmittelbar bei der betroffenen Person), kann dies zur Unzulässigkeit der Verarbeitung führen. Im Falle von *Generalklauseln* kommt demgegenüber auch die Verarbeitung öffentlicher Daten in Betracht.[91] Allerdings tragen derartige Generalklauseln unter verfassungsrechtlichen Bestimmtheitsgesichtspunkten typischerweise *keine schweren Grundrechtseingriffe*; dies gilt auch bei öffentlichen Daten.[92]

63 Bei der Anwendung der Normen wird es vielfach unter Erforderlichkeits- und Verhältnismäßigkeitsgesichtspunkten zu *Abwägungsentscheidungen* kommen, bei denen (strukturell vergleichbar zu Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO, s. Rz. 50 ff.) berücksichtigt werden kann, dass die *Eingriffsintensität* bei der Verarbeitung öffentlicher Daten (und noch mehr bei selbst veröffentlichten Daten) typischerweise *herabgesetzt* ist. Aufseiten des Verantwortlichen ist zwar zu berücksichtigen, dass sich öffentliche Stellen nicht auf das Recht auf Informationsfreiheit berufen können. Dies kann aber durchaus kompensiert werden, wenn mit der Verarbeitung der öffentlichen Daten *wichtige Allgemeinwohlziele* verfolgt werden.[93] Schließlich besteht im Falle der zentralen Regelung zum Beschäftigtendatenschutz in § 26 BDSG[94] sogar ein völliger Gleichlauf zwischen privaten und öffentlichen Verantwortlichen: Die Zulässigkeit der Erhebung öffentlicher Daten richtet sich in beiden Konstellationen nach der umstrittenen Frage der *Erforderlichkeit* für die Begründung des *Beschäftigungsverhältnisses*, die entsprechende Abwägungen verlangt.[95]

VI. Fazit

64 *Öffentlich zugängliche* Daten haben ein erhebliches *Nutzungspotential* für private und öffentliche Datenverarbeiter. Dies gilt auch und gerade, wenn es sich um personenbezogene Daten handelt. In diesem Fall sind aber datenschutzrechtliche Vorgaben einzuhalten, die zu umfangreichen Abwägungserfordernissen führen.

65 Auf europäischer Ebene hat der Gesetzgeber die Regelungen der DSRL praktisch unverändert in die DSGVO übernommen. Dies gilt sowohl für den Zulässigkeitstatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 2 lit. e DSGVO; zuvor Art. 8 Abs. 2 lit. e DSRL), also auch für die stets zu beachtenden Zulässigkeitstatbestände (v.a. Art. 6 Abs. 1 Unterabs. 1 lit. e, f DSGVO, zuvor Art. 7 lit. e, f DSRL). Unterschiede ergeben sich lediglich insofern, als die DSGVO nunmehr *Anhaltspunkte für Abwägungskriterien* enthält (z.B. die Schutzwürdigkeit von Kindern in Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO oder die vernünftigen Erwartungen der betroffenen Person in EG 47 S. 1 DSGVO). Der Sache nach konnten diese Gesichtspunkte allerdings auch nach altem Recht bereits berücksichtigt werden.

66 Aus deutscher Perspektive ist die Fortschreibung der europäischen Rechtslage allerdings eine *materielle Rechtsänderung*, da die Privilegierung der Verarbeitung öffentlicher Daten nicht mehr in der schematischen Weise wie nach dem BDSG a.F. erfolgen darf. Die *öffentliche Zugänglichkeit* der Daten ist damit zwar weiterhin ein wichtiger, aber eben *nur ein Gesichtspunkt* innerhalb der Abwägung. Im Vergleich zum BDSG a.F. ist der Ansatz der DSGVO damit in beide Richtungen flexibler: Zum einen ist bei *nicht-öffentlichen* Daten nicht *per se* eine strengere Abwägung erforderlich, zum anderen kann bei *öffentlichen* Daten der Gesichtspunkt der *Allgemeinzugänglichkeit* leichter durch andere Umstände *überwunden werden* und dann zur Unzulässigkeit der Verarbeitung führen.

67 Damit lässt sich festhalten, dass einmal veröffentlichte Daten nach der DSGVO nicht nur nicht schutzlos sind, sondern sogar (moderat) stärker geschützt werden als nach dem BDSG a.F. Angesichts der in heutiger Zeit zu beobachtenden erheblichen Risiken der langfristigen Beobachtbarkeit und Möglichkeiten der Profilbildung anhand öffentlich zugänglicher Internetdaten ist dies zu begrüßen.

---

88 Art. 6 Abs. 1 Unterabs. 1 lit. d DSGVO könnte z.B. die Recherche in öffentlichen Daten rechtfertigen, um eine vermisste und mutmaßlich gefährdete Person aufzufinden.

89 BVerwG, NVwZ 2019, 473, 475 Rz. 26.

90 S. instruktiv *Veil*, https://www.cr-online.de/blog/2019/01/22/verheddert-im-auslegungsdickicht-der-ds-gvo/; ferner *Will*, ZD 2019, 231, 234; *Schnabel*, DÖV 2019, 653, 656.

91 S. am Beispiel der Verarbeitungsbefugnisse für Sozialdaten nach dem SGB X a.F. *Bieresborn*, NZS 2016, 532, 533 ff.

92 S. für das Beispiel der umfangreichen Nutzung öffentlicher Daten zum Katastrophenschutz *Desoi* (Fn. 41), 200 ff.

93 Beispiele bei *Desoi* (Fn. 41), 139 ff.

94 Dieser erfasst nach § 26 Abs. 8 BDSG (v.a. Nr. 1 und 7) auch öffentliche Arbeitgeber und Dienstherrn.

95 S.o. Fn. 60.

Prof. Dr. Gerrit Hornung, LL.M.

Universitätsprofessor an der Universität Kassel, Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht; Direktor am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

IT-Recht, Datenschutzrecht, E-Government

gerrit.hornung@uni-kassel.de

https://www.uni-kassel.de/fb07/hornung

Carolin Gilga, LL.M.

Doktorandin und wissenschaftliche Mitarbeiterin am Lehrstuhl für Öffentliches Recht, IT-Recht und Umweltrecht im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel

Datenschutzrecht und Arbeitsrecht

c.gilga@uni-kassel.de

https://www.uni-kassel.de/fb07/institute/iwr/personen-fachgebiete/hornung-prof-dr/team/wissenschaftliche-mitarbeiter-innen/carolin-gilga.html

Stefan Papastefanou

„Database Reconstruction Theorem" und die Verletzung der Privatsphäre (Differential Privacy)

Chancen und Risiken bei der Anwendung von Machine-Learning Algorithmen am Beispiel von Covid-19 Statistiken und des Zensus 2021

Im Rahmen von großen Erhebungen wie dem Zensus 2021 ist es vorgesehen, die Klarnamen von den restlichen erhobenen Daten zu trennen und so eine Anonymisierung der Daten zu erreichen. Hierdurch und eine Generalisierung der Informationen bei der Veröffentlichung sollen datenschutzrechtliche Bedenken bei der Erhebung, Speicherung und späteren Veröffentlichung der Daten ausgeräumt werden. Dies zeigt, dass großes Vertrauen in die Anonymisierung gelegt wird. Die Pflichten der DSGVO finden keine Anwendung für anonymisierte Daten und für amtliche Statistiken ist die Anonymisierung sogar gesetzlich vorgeschrieben. Der Beitrag zeigt allerdings, welche Schwierigkeiten bei der Anonymisierung durch das „Database Reconstruction Theorem" entstehen.

Im Gegensatz zu den üblicherweise geäußerten Bedenken zur Re-Identifizierung durch Verknüpfung von verschiedenen Datensätzen, zeigt dieses Theorem auf, dass bereits jeder korrekte Datenwert, der im Rahmen einer Umfrage erfasst und später veröffentlicht wird, die informationelle Selbstbestimmung des Umfrageteilnehmers in einem gewissen Grad verletzt. Im Rahmen dieses Theorems wird jedoch ein wichtiger Beitrag für das Datenschutzrecht geleistet, indem auf eine Methode hingewiesen wird, mit der die Verletzung der Privatsphäre mathematisch quantifiziert werden kann. Auch wird auf moderne Möglichkeiten und Risiken der Differential Privacy unter dem Einsatz von Machine-Learning eingegangen. Abschließend können Empfehlungen für die Anwendung dieser Methoden in Bereichen der Statistik, welche gerade bei Patientendaten im Rahmen der Covid-2019 Pandemie besonders relevant sind, aber auch in anderen datenschutzrechtlich bedenklichen Ebenen der Privatwirtschaft gegeben werden.

I. Anonymisierung im Rahmen von nationalen Statistiken

Ein Zensus wird mit dem ambitionierten Ziel durchgeführt, jede einzelne Person in Deutschland zu erfassen und bestimmte Informationen über sie zu festzuhalten wie etwa Alter, Geschlecht, Wohnort etc.[1] Der Gedanke dahinter besteht in der demographischen Erfassung der Bevölkerung und deren Verteilung auf die jeweiligen Bundesländer und Landkreise zu bestimmen. Letzteres ist insbesondere relevant für die staatspolitische Verteilung von Stimmen, wobei hier in Deutschland regelmäßig keine großen Änderungen zu erwarten sind.[2] 1

Aktuell werden im Rahmen der Covid-19 Pandemie auch täglich neue Statistiken veröffentlicht, die Informationen zu den Fallzahlen, der Entwicklung und der Verteilung enthalten. Solche Statistiken sind von erheblicher Bedeutung für die politischen Entscheidungen, da einige Maßnahmen und deren Lockerung von der Zahl und Konzentration von Infizierten abhängen. Mithin ist bei der Ermittlung und der Veröffentlichung 2

1 Zensus 2021 Newsletter Nr. 1/2017, Statistisches Bundesamt, 1 ff.

2 Im Gegensatz etwa zu den USA, bei denen im diesjährigen Zensus erwartet wird, neue Stimmgewichte im Electoral College aufgrund von sich ändernden Bevölkerungszahlen in den jeweiligen Bundesstaaten zu bewirken.