März 2019
7. Jahrg.
84364

Seite 1–52

InTeR

Zeitschrift zum Innovations- und Technikrecht

1

dfv Mediengruppe · Frankfurt am Main

- Product security publications (Kategorie C) definieren, wie Base security standards oder Group security publications für einen bestimmten Produkttyp angewendet werden können. Sie legen fest, wie verschiedene Produkte sicher miteinander interagieren und wie sie einheitlich zu steuern und zu verwalten sind. Daher sollten Product security publications ihre Anforderungen so weit wie möglich unter Bezugnahme auf Base security standards und Group security publications definieren, zum Beispiel IEC 62351-3.
- Guidance security publications (Kategorie D) sollten keine Anforderungen enthalten. Sie erläutern, wie Base security standards und Group security publications oder Product security publications umgesetzt werden können. In einigen Fällen werden Guidance security publications jedoch nicht verwendet. Stattdessen findet eine Bereitstellung der notwendigen Leitlinien durch informative Anhänge innerhalb des relevanten Anforderungsstandards statt, zum Beispiel IEC TS 62443-2-2.
- Test security publications (Kategorie E) definieren Möglichkeiten, um festzustellen, ob die Anforderungen von Base security standards und Group security- oder Product security publications korrekt implementiert wurden. Test security publications haben deshalb typischerweise eine spezialisierte Zielgruppe. Sie können Referenzimplementierungen definieren oder identifizieren, die verwendet werden können, um die korrekte Umsetzung durch erfolgreiche Interoperation zu bestimmen, zum Beispiel ISO/IEC 27007.

III. Fazit

Die in den letzten Jahren zahlreichen und durchaus verschiedenen Ansätze, die global in den unterschiedlichsten Staaten zur Regulierung der Cybersicherheit und bisweilen auch des Datenschutzes verfolgt werden, legen nahe, dass es sich hierbei um ein hochaktuelles Thema handelt, dem eine erhebliche Bedeutung in den innen- wie außenpolitischen Strategien der jeweiligen Regierungen beigemessen wird. Die Konzepte, mit denen der steigenden Bedrohungslage im digitalen Raum begegnet wird, sind dabei unterschiedlich und gehen von punktuellen, themen- und branchenspezifischen Regelungen bis hin zu ganzheitlichen Regulierungsansätzen, die auch Datenschutz- und Zertifizierungsfragen in sektoren- und branchenübergreifender Hinsicht adressieren. Daneben sind es teils auch aktuelle technische Herausforderungen, die die Nationalstaaten zur Förderung der Cybersicherheitsregulierung bewegen, so zum Beispiel für Japan im Bereich des IoT[12]. Cybersicherheit wird man aber letztlich nicht nur als rechtliche, sondern auch als Aufgabe der internationalen Normung und Standardisierung zu betrachten haben:[13] So können einschlägige Normen nicht nur zur technischen Konkretisierung der rechtlichen Cybersicherheitsanforderungen beitragen, sondern auch die einheitliche Auslegung von (neu erlassenen) Rechtsvorschriften fördern.[14] Nicht zuletzt kann die Standardisierung das Mittel zur Durchführung einer staatenübergreifenden Cybersicherheitszertifizierung sein bzw. diese zumindest erleichtern. Insoweit ist es zu begrüßen, dass die Belange der Normung und Standardisierung voraussichtlich auch in der neuen EU Cybersecurity-Verordnung in angemessener Weise Berücksichtigung finden

12 Ein weiteres Beispiel für neue, technikbezogene Gesetzgebungsvorhaben in Asien ist der Entwurf für ein Datenschutzgesetz in Indien, dazu *Kipker,* ZD 2018, 253.
13 Siehe nur *Kipker/Müller,* InTeR 2018, 24.
14 *Kipker,* DuD 2016, 610..

Alexander Kratz*

Datenportabilität und „Walled Gardens“

Historische Rekonstruktion und praktische Gefahren des Art. 20 DSGVO

Dieser Beitrag stellt erstmals den historischen Zusammenhang dar, in dem die Idee der Datenportabilität entstand: Aus dem Idealismus eines „Open Web“ heraus sollte „Walled Gardens“ entgegengewirkt werden. Neu eingeführt wird die Perspektive der „komplementären Dienste“. Darauf aufbauend lassen sich einige Fragen klären, z. B. weshalb Datenportabilität gerade für soziale Netzwerke konzipiert wurde. Entgegen der wohl herrschenden Meinung soll aufgezeigt werden, dass Art. 20 keineswegs ein datenschutzrechtlicher „Fremdkörper“ ist.

I. Aktueller Stand der Diskussion

Es ist eine der großen Neuerungen, die die DSGVO gebracht hat: Das Recht auf Datenportabilität in Art. 20. In der Praxis könnte es noch sehr relevant werden. Insofern ist erstaunlich, wie schwer es nach wie vor fällt, Art. 20 einzuordnen: Im Datenschutzrecht sei Art. 20 etwa „systemfremd“,[1] eigentlich ein übertriebenes Wettbewerbsrecht[2] – oder vielleicht doch unspektakulär datenschutzrechtlich, weil nur ein erweitertes Auskunftsrecht.[3]

Diese Unsicherheit liegt auch daran, dass der historisch-ideologische Ursprung der Datenportabilität bisher noch nicht erkannt wurde: Der Datenportabilität liegt der Idealismus eines „Open Web“ zugrunde. Offensichtlich wurde dies bisher schlicht übersehen. Hier möchte dieser Aufsatz

* Mehr über den Autor erfahren Sie auf Seite III.
1 *Dehmel/Hullen,* ZD 2013, 147, 153; *Richter,* PinG 2017, 231.
2 *Hennemann,* PinG 2017, 5, 6; für den wettbewerbsrechtlichen Charakter bspw. auch *Herbst,* in: Kühling/Buchner DS-GVO BDSG, 2. Aufl. 2018, Art. 20 Rn. 4.
3 *Hennemann,* PinG 2017, 5, 8; in der Tendenz bspw. auch *v. Lewinski,* in: BeckOK Datenschutzrecht, Wolff/Brink, 24. Edition 2018, Art. 20 Rn. 7.

ansetzen. Er will so eine neue Grundlage für das Verständnis von Art. 20 schaffen. Zunächst sollen jedoch die bisherigen Erkenntnisse über den Telos von Art. 20 dargestellt werden, sie sind nach wie vor zutreffend und nötig als Vorverständnis für die darauf aufbauenden Überlegungen.

1. Zwei Ziele

Zusammengefasst dient Art. 20 nach bisherigem Stand der Diskussion zwei Zielen. Zum einen soll Art. 20 die Kontrolle des Betroffenen über die ihn betreffenden Daten stärken.[4] So steht es auch in Erwägungsgrund (EG) 68. Der Art.–29-Gruppe zufolge soll so ein „Ausbalancieren des Verhältnisses zwischen betroffenen Personen und Verantwortlichen“ erreicht werden.[5]

Konkreter geht es daneben darum, den sog. Lock-In-Effekt zu reduzieren.[6] Dieser Effekt sorgt dafür, dass der Nutzer eines Dienstes faktisch an diesen gebunden ist, weil die sog. Wechselkosten (engl. „switching costs“) zu hoch sind.[7] Der Lock-In-Effekt erschwert so den Anbieterwechsel und lähmt den Wettbewerb. Der Marktzugang für neue Anbieter wird behindert.[8]

Beispielsweise wird ein Nutzer kaum die Kalender-Plattform wechseln, wenn er darin dutzende Termine eingetragen hat und diese nicht exportieren kann. Sonst müsste er jeden einzelnen Termin manuell in die neue Plattform übertragen. Die Wechselkosten (in Form des Zeitaufwands) sind hoch; der Nutzer ist „locked in“.[9] Mit Art. 20 müssen die Termine direkt an die neue Plattform übermittelt werden können (Abs. 2) oder in maschinenlesbarer Form herausgegeben werden (Abs. 1). Der Markteintritt neuer, überlegener Kalender-Plattformen wird leichter, das Angebot besser, so die Idee jedenfalls.

Weiterhinhin ist zu erwähnen, dass der Gesetzgeber bei Art. 20 vor allem an soziale Netzwerke gedacht zu haben schien.[10] Diese wurden als einziges konkretes Anwendungsbeispiel im DSGVO-Entwurf der Kommission erwähnt (EG 55).[11] In der Endfassung der DSGVO (EG 68) ist dies nicht mehr der Fall. Weiterhin sollte wohl gerade datenschutzfreundlicheren Anbietern der Markteintritt erleichtert werden.[12] Generell ist der Anwendungsbereich von Art. 20 nicht auf spezielle Dienste beschränkt, sodass eine Vielzahl von Anwendungsfällen denkbar ist.[13]

2. Offene Fragen

Der so verstandene Art. 20 wird in der Literatur kritisch hinterfragt. Zum einen wird bezweifelt, dass Art. 20 wirklich ins Datenschutzrecht passt. Zwar betont die Art.–29-Gruppe seinen datenschutzrechtlichen Charakter.[14] Die Reduzierung des Lock-In-Effekts scheint aber ein eher wettbewerbs- bzw. verbraucherschutzrechtliches Ziel.[15] Im Datenschutzrecht wirke Art. 20 insofern „systemfremd“[16], als „Fremdkörper“[17]. Dies wurde auch bereits im Gesetzgebungsverfahren bemängelt.[18]

Andererseits ist Art. 20 auch nicht klassisch wettbewerbsrechtlich konzipiert. Schließlich setzt Art. 20 tatbestandsmäßig keine Marktmacht voraus. Hierdurch erfasst Art. 20 neben den anvisierten Marktführern auch beispielsweise die (klischeehafte) „start-up software company in a garage“.[19] Art. 20 könnte insofern als „überschießendes Wettbewerbsrecht“ bezeichnet werden.[20]

Bezüglich der sozialen Netzwerke wird infrage gestellt, ob Art. 20 hier wirklich den Anbieterwechsel erleichtert. Die Stärke der Marktführer scheint weniger auf den Lock-In-Effekt, als vielmehr auf direkte Netzwerkeffekte zurückzugehen. Ein Wechsel des sozialen Netzwerks ist reizlos, wenn die eigenen Kontakte beim ursprünglichen Anbieter bleiben.[21]

II. Neues historisches Verständnis

Das bisherige Verständnis ist in historischer Hinsicht unvollständig. Bisher wird lediglich der DSGVO-Gesetzgebungsprozess berücksichtigt. Dabei wurde „Data Portability“ bereits ab ca. 2007 in der US-amerikanischen IT-Branche teils leidenschaftlich gefordert. 2010 kündigte die EU-Kommission dann an, sich mit Datenportabilität befassen zu wollen,[22] was letztlich in Art. 20 mündete. Es liegt nahe, dass die US-amerikanische Debatte der EU-Kommission als Inspiration diente.

Bisher wurde die Geschichte vor 2010 von der deutschsprachigen juristischen Literatur noch nicht aufgegriffen.[23] Dies mag daran liegen, dass sie aus den Gesetzgebungsmaterialien kaum ersichtlich ist. Jedenfalls fehlt damit ein zentraler Baustein für das Verständnis von Art. 20. Um diesen zu ergänzen, soll die historische Entwicklung[24] kurz vorgestellt und anschließend die großen Linien dahinter herausgearbeitet werden.

1. Historischer Abriss

Soweit ersichtlich, wurde „Data Portability“ erstmals 2007 öffentlich gefordert. Einige Blogger und Software-Entwickler veröffentlichten in diesem Jahr die von ihnen so genannte „Bill of Rights for Users of the Social Web“. In ihr wurde vor allem mehr Kontrolle der Betroffenen über ihre

4 *Jülicher/Röttgen/v. Schönfeld,* ZD 2016, 358, 360 f.; *Paal/Hennemann,* NJW 2017, 1697, 1701.
5 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01 (deutsche Fassung), vom 5.4.2017 (Ausgangsfassung vom 13.12.2016), S. 4; der Europäische Datenschutzausschuss hat die Leitlinie inzwischen gebilligt: s. https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-data-portability_de (zuletzt abgerufen am 28.1.2019).
6 *Brüggemann,* K&R 2018, 1; Impact Assessment der EU-Kommission: SEC(2012) 72 final, S. 28; *Paal,* in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 20 Rn. 6.
7 *Sperlich,* DuD 2017, 377; *Swire/Lagos,* Maryland Law Review 2013, 335, 388.
8 *Hennemann,* PinG 2017, 5; *Schätzle,* PinG 2016, 71, 74.
9 Vgl. Impact Assessment (Fn. 6), S. 28.
10 *Schantz,* NJW 2016, 1841, 1845; *Wybitul/Fladung,* BB 2012, 509, 512.
11 Ebenso im Impact Assessment (Fn. 6), S. 106.
12 Impact Assessment (Fn. 6), S. 28; *Albrecht,* CR 2016, 88, 93.
13 *Hennemann,* PinG 2017, 5; *Benedikt,* RDV 2017, 189.
14 Art.–29-Gruppe (Fn. 5), S. 4.
15 *Paal,* in: Paal/Pauly (Fn. 6), Art. 20 Rn. 3; *Benedikt,* RDV 2017, 189.
16 *Hennemann,* PinG 2017, 5, 6; *Dehmel/Hullen,* ZD 2013, 147, 153.
17 *V. Lewinski,* in: BeckOK (Fn. 3), Art. 20 vor Rn. 1.
18 Rat der Europäischen Union, 2012/0011 (COD), Fn. 190.
19 *Swire/Lagos,* Maryland Law Review 2013, 335, 339.
20 *Hennemann,* PinG 2017, 5, 6.
21 *Skobel,* PinG 2018, 160, 164; *Brüggemann,* K&R 2018, 1; *Hennemann,* PinG 2017, 5, 6.
22 COM (2010) 609 final, S. 8.
23 Jeweils in einem Halbsatz erwähnt wurde zumindest abstrakt der Punkt des offenen Internet von: *Laue/Nink/Kremer,* Das neue Datenschutzrecht in der betrieblichen Praxis, 2016, § 4 Rn. 61; *Schürmann,* in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, Art. 20 Rn. 4.
24 In der englischsprachigen juristischen Literatur dargestellt in: *Van der Auwermeulen,* Computer Law & Security Review 2017, 58 ff.

Daten verlangt, insbesondere auch mehr Datenportabilität.[25]

Ende 2007 gründete sich die DataPortability Workgroup, ein loser Zusammenschluss von Software-Entwicklern.[26] Sie verfolgte das Ziel, das Teilen von personenbezogenen Daten zwischen verschiedenen Plattformen zu erleichtern.[27] Dafür sollten Nutzungsbedingungen standardisiert werden, technische Koordinierung sollte Datenex- bzw. -importe erleichtern.[28] Ab Anfang 2008 nahmen auch Vertreter von Facebook und Google an der DataPortability Workgroup teil.[29] Daneben gab es auch andere Initiativen wie „OpenID“, „OAuth“ und „Portable Contacts“.[30]

Dabei herrschte eine regelrechte Euphorie um „Data Portability“. So meinte ein Teilnehmer der DataPortability Workgroup: „We are on the cusp of the next phase of the web […]. We think we are about to see a major transformation, as things that have been powered inside ‚walled garden‘ social networks become part of the open web.“[31] Der damalige Chief of Engineering von Google erklärte, Google sei ein „enthusiastic embracer“ von Datenportabilität.[32] Ein Marktanalyst fasste zusammen: „[Data Portability] is the trend of 2008.“[33] 2012 sprach der Erfinder des World Wide Web und MIT-Professor *Berners-Lee* sogar davon, dass in Datenportabilität ein „tremendous potential to help humanity“ läge.[34]

In der Folgezeit verlief sich die Bewegung. Wohl angestoßen von ihr[35] begannen jedoch Unternehmen wie Facebook, Schnittstellen zu entwickeln, mit denen Nutzer ihre Daten an Apps weitergeben konnten. Bekanntestes Beispiel ist vielleicht die sog. „Login with Facebook“-Funktion.[36] Eine ähnliche Funktion ermöglichte allerdings auch dem Unternehmen Cambridge Analytica (mittelbar) den Zugriff auf die Daten von Millionen von Nutzern.[37] 2014 schränkte Facebook diese Schnittstellen ein.[38] Im Zuge des Cambridge-Analytica-Skandals erklärte *Mark Zuckerberg* in einem Interview zur Idee der Datenportabilität: „So I do think early on on the platform we had this very idealistic vision around how data portability would allow all these different new experiences, and I think the feedback that we've gotten from our community and from the world is that privacy and having the data locked down is more important to people than maybe making it easier to bring more data and have different kinds of experiences.“[39]

2. „Walled Gardens“ und „Open Web“

Zentrales Verständniselement ist zunächst der Bezug von Datenportabilität zu sog. „Walled Gardens“. Datenportabilität ist historisch betrachtet als Gegenmaßnahme hierzu zu sehen.[40] Mit einem „Walled Garden“ ist eine Plattform gemeint, auf der der Nutzer möglichst viel Zeit verbringen soll. Dafür wird sie vom Rest des Internet isoliert. Die vom Nutzer gesammelten Daten können nicht exportiert werden, Verknüpfungen mit dem Rest des Internet sind schwierig.[41] Letztlich bleibt dieser untechnische Begriff etwas vage. Als Datenportabilität erstmals gefordert wurde (ca. 2007), zeichnete sich ein Trend zu immer mehr solcher „Walled Gardens“ ab. „Data Portability“ sollte nun einem Aspekt des „Walled Garden“ entgegenwirken, dass nämlich Datenexporte hier meist nicht angeboten werden.

Dass „Walled Gardens“ bekämpft werden sollten, erklärt sich aus der Denkweise eines „Open Web“.[42] Hier liegt der ideologische Ursprung der Datenportabilität. Im Grundsatz ist damit gemeint, dass das Internet frei, nicht beschränkt, sein soll. Was das Internet so innovationskräftig machte, war die freie Verknüpfbarkeit, der freie, gleiche Zugang, die Möglichkeit für jeden, sich darin kreativ zu entfalten. Dies sollte erhalten bleiben.[43] Das Abkapseln im Sinne des „Walled Garden“ widerspricht diesem angestrebten Strukturprinzip. Hierauf wies auch das EU-Parlament 2011 hin.[44]

3. „Komplementäre Dienste“

In den Aussagen der DataPortability Workgroup-Teilnehmer fällt weiterhin auf, dass es meist um neue Dienste und Erfahrungen ging, die ermöglicht werden sollten.[45] Das (geringfügig exaltierte) „tremendous potential“ sollte darin liegen, dass die vorhandenen Daten von neuen, *andersartigen* Diensten ausgewertet werden können.[46] Dies ist insofern interessant, als Art. 20 aktuell eher mit der Vorstellung betrachtet wird, dass der Nutzer von einem Dienst zu einem *gleichartigen* Dienst wechselt (wie beispielsweise von einer Kalender-App zu einer anderen Kalender-App).[47]

Diese Erkenntnis kann sich noch als zentral für das Verständnis von Art. 20 erweisen. Um klarer zu unterscheiden, soll dies als Datenübertragung zu „komplementären“ bzw. „substitutiven Diensten“ bezeichnet werden. „Substitutiv“

25 *Van der Auwermeulen* (Fn. 24), S. 58; „Bill of rights“ abrufbar unter: https://www.zdnet.com/article/a-bill-of-rights-for-the-social-web/ (zuletzt abgerufen am 28.1.2019).
26 *Saad,* Medium vom 26.3.2018, https://medium.com/@chrissaad/do-not-deletefacebook-because-of-cambridge-analytica-e8a2eec44730 (zuletzt abgerufen am 28.1.2019).
27 *Allison,* Social networks may find that it does not pay to be possessive, Financial Times vom 22.1.2008, S. 13, online abrufbar über das „Financial Times Historical Archive“.
28 *Bizannes* (Mitbegründer der DataPortability Workgroup), Techcrunch.com vom 23.6.2010, https://techcrunch.com/2010/06/23/data-portability-policy/ (zuletzt abgerufen am 28.1.2019).
29 *Van der Auwermeulen* (Fn. 24), S. 58; Techcrunch.com vom 8.1.2008, https://techcrunch.com/2008/01/08/this-day-will-be-remembered-facebook-google-and-plaxo-join-the-dataportability-workgroup/ (zuletzt abgerufen am 28.1.2019).
30 *Saad* (Fn. 26).
31 *Allison* (Fn. 27).
32 *Allison* (Fn. 27).
33 *Allison* (Fn. 27).
34 *Katz,* The Guardian (Online) vom 18.4.2012, https://www.theguardian.com/technology/2012/apr/18/tim-berners-lee-google-facebook (zuletzt abgerufen am 28.1.2019); *Reisinger,* CNET vom 18.4.2012, https://www.cnet.com/news/tim-berners-lee-tell-facebook-google-you-want-your-data-back/ (zuletzt abgerufen am 28.1.2019).
35 So jedenfalls der Mitbegründer der DataPortability Workgroup: *Saad* (Fn. 26).
36 *Saad* (Fn. 26).
37 *Ingram,* Reuters vom 4.4.2018, https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM (zuletzt abgerufen am 28.1.2019).
38 *Thompson,* Wired (Online) vom 21.3.2018, https://www.wired.com/story/mark-zuckerberg-talks-to-wired-about-facebooks-privacy-problem/ (zuletzt abgerufen am 28.1.2019).
39 *Thompson* (Fn. 38).
40 *Saad* (Fn. 26); *Allison* (Fn. 27); *Bizannes* (Fn. 28).
41 *Berners-Lee,* Scientific American 2010, 80, 82 f., abrufbar unter: http://www.cs.virginia.edu/~robins/Long_Live_the_Web.pdf (zuletzt abgerufen am 28.1.2019); *Beuth,* Zeit (Online) vom 13.11.2011, http://www.zeit.de/digital/internet/2011-10/amazon-walled-garden (zuletzt abgerufen am 28.1.2019).
42 *Saad* (Fn. 26); *Katz* (Fn. 34); *Reisinger* (Fn. 34).
43 *Berners-Lee* (Fn. 41), S. 82.
44 Entschließung des Europäischen Parlaments, 2011/2025(INI), Fn. 10 zu Punkt 16; ohne dies zu vertiefen auch zitiert von: *Laue/Nink/Kremer* (Fn. 23), § 4 Rn. 61; *Schürmann,* in: Auernhammer (Fn. 23), Art. 20 Rn. 4.
45 *Saad* (Fn. 26); *Thompson* (Fn. 38).
46 *Reisinger* (Fn. 34).
47 Die Übertragung zu einem andersartigen Dienst findet sich bspw. bei *Brüggemann,* K&R 2018, 1 (am Beispiel Spotify → Netflix).

ist dabei die Übertragung zu einem gleichartigen, „komplementär“ die zu einem andersartigen Dienst.[48]

Diese Differenzierung ermöglicht künftig einen nuancierteren Blick in Auslegungsfragen. Außerdem wird sie dabei helfen, bisher offene Fragen zum Telos von Art. 20 zu beantworten. Dies soll weiter unten gezeigt werden. An dieser Stelle bleibt festzuhalten, dass die Übertragung zu „komplementären Diensten“ historisch betrachtet fast wichtiger erscheint als der Wechsel zu „substitutiven Diensten“. Dies könnte auch daran liegen, dass ökonomisch betrachtet von „komplementären Diensten“ ein besonders großer Mehrwert zu erhoffen ist.[49] Der Wortlaut des Art. 20 ermöglicht beides.

Ein Beispiel für einen komplementären Dienst erwähnt die Art.–29-Gruppe (ohne auf diesen abstrakten Aspekt einzugehen): So könnten die Daten von Supermarkt-Kundenkarten von einem anderen Anbieter benutzt werden, um eine „individuelle CO_2-Bilanz“ zu erstellen.[50] Ein weiteres Beispiel wäre, aufbauend auf der Transaktionshistorie von Bankkunden individuelle Finanzberatungsdienste anzubieten. Art. 20 könnte es nunmehr sogar ermöglichen, eigene Daten für einen guten Zweck zu „spenden“, beispielsweise die Daten eines Fitnesstrackers an eine medizinische Forschungseinrichtung.[51]

III. Weitergedacht

1. Anschlussfragen

Die Entstehungsgeschichte wirft erst einmal neue Fragen auf. So ist merkwürdig, dass die Debatte um Datenportabilität schon vor einigen Jahren zum Stehen gekommen scheint. Ist Datenportabilität also eine überholte Idee? Saß die EU-Kommission in ihrem DSGVO-Entwurf einem kurzlebigen Trend auf, der nun per Unionsrecht zwangs-verewigt wird? Außerdem überrascht, dass auch die großen Online-Marktführer Datenportabilität (zumindest teilweise) befürworten. So entstanden bereits komplementäre Dienste. Ist Art. 20 dann überhaupt notwendig, um komplementäre Dienste zu stärken?[52]

Dass die großen Online-Marktführer teilweise freiwillig Schnittstellen einrichten, dürfte mit ihrem wirtschaftlichen Eigeninteresse zusammenhängen: Der komplementäre Dienst steuert dem ursprünglichen Dienst neue Funktionen bei, auch dieser wird so für den Nutzer interessanter.[53] Zudem kann sich der ursprüngliche Dienst so auch den Zugriff auf die Daten sichern, die der Nutzer im komplementären Dienst hinterlässt.[54] Beides ist jedoch nicht der Fall, wenn der komplementäre Dienst lediglich die Daten des Vorherigen verwenden will, aber sonst nicht an ihn angeschlossen werden soll. Dies könnte die Beobachtung eines Experten 2009 erklären: „[Facebook is] doing everything they can to be open while remaining closed“.[55] Insofern scheint das Interesse der Online-Marktführer an Datenportabilität naturgemäß vorhanden, aber limitiert.

Dies könnte auch der Grund sein, weshalb die Debatte um Datenportabilität ca. 2012/2014 zum Stillstand kam. Die DataPortability Workgroup hatte Datenportabilität zu einem gewissen Grad erreicht. Für die Marktführer könnte der ökonomische Anreiz gefehlt haben, Datenportabilität darüber hinaus voranzutreiben.

Dies vorausgesetzt, wäre die EU-Kommission mit ihrem Entwurf 2012 auch nicht einem kurzlebigen Trend aufgesessen, als sie ein Recht auf Datenportabilität vorschlug. Im Gegenteil: Art. 20 könnte ermöglichen, die Datenportabilität über das Eigeninteresse der Online-Marktführer hinaus auszudehnen. Weitere neue komplementäre Dienste könnten so gefördert werden – gerade solche Dienste, die ihre eigenen Kundendaten nicht automatisch an den ursprünglichen Dienst weiterleiten.

Ein erstes Wiederaufleben hat die Datenportabilität mit dem Mitte 2018 veröffentlichten „Data Transfer Project“ erfahren, in dem unter anderem Google, Facebook und Twitter kooperieren wollen.[56] Möglicherweise wurde diese Arbeitsgruppe auch aufgrund von Art. 20 initiiert.[57]

2. Soziale Netzwerke

Plötzlich Sinn ergibt nun, weshalb die EU-Kommission soziale Netzwerke als Anwendungsfall für Art. 20 nannte. Dabei scheinen doch eigentlich eher Netzwerkeffekte als Wechselkosten einen Anbieterwechsel zu verhindern. Die historische Darstellung zeigt nun, dass bezüglich sozialer Netzwerke ursprünglich nicht der substitutive Anbieterwechsel im Vordergrund stand, sondern die Ermöglichung komplementärer Dienste. Die riesigen Datensammlungen der sozialen Netzwerke sollten für neue Geschäftsideen nutzbar gemacht werden: „[S]uddenly it would be possible for two people in a garage to create a website or application that can take advantage of [social networks] without having to invest in building up their own social network“.[58]

Diese Hoffnung könnte jedoch weitgehend enttäuscht werden. Der Großteil der in sozialen Netzwerken gespeicherten Daten bezieht sich nämlich auf mehrere Personen. Dies wirft die Frage auf, ob ein Betroffener mithilfe von Art. 20 inzident auch die Daten Dritter übertragen lassen darf. Dies könnte deren Recht auf informationelle Selbstbestimmung berühren (bzw. Art. 7, 8 GRCh).[59] Daher dürfen der Art.–29-Gruppe zufolge Daten beim neuen Anbieter nicht zu neuen Zwecken verarbeitet werden (vgl. Art. 20 Abs. 4).[60] Dies aber ist genau die Idee komplementärer Dienste. Komplementären Diensten dürften so regelmäßig alle Daten, die sich auf Dritte beziehen, verwehrt bleiben. Bei sozialen Netzwerken wäre dies besonders einschneidend.

3. Fehlende Marktmacht-Voraussetzung

Weiterhin war im Ausgangspunkt offengeblieben, weshalb Art. 20 keine Marktmacht voraussetzt. Dabei besitzt Art. 20

48 Angelehnt an die „substitute“/„complementary services“ im wirtschaftswissenschaftlichen Aufsatz von: *Engels,* Internet Policy Review, Volume 5, Issue 2, 2016, S. 1, 2.
49 *Reisinger* (Fn. 34); so auch *Engels* (Fn. 48), S. 8.
50 Art.–29-Gruppe (Fn. 5), S. 5.
51 *Tennison* (CEO des „Open Data Institute“), auf ihrem Blog, 26.12.2017, http://www.jenitennison.com/2017/12/26/data-portability.html (zuletzt abgerufen am 28.1.2019).
52 *Engels* (Fn. 48), S. 9.
53 *Engels* (Fn. 48), S. 8.
54 *Van der Auwermeulen* (Fn. 24), S. 59.
55 *Gelles,* Facebook accused of restricting its users, Financial Times vom 11.7.2009.
56 https://datatransferproject.dev/; https://datatransferproject.dev/dtp-overview.pdf. (zuletzt abgerufen am 28.1.2019).
57 Vgl. bspw. *Tung,* Siliconrepublic.com vom 11.5.2018, https://www.siliconrepublic.com/enterprise/data-transfer-project-explained (zuletzt abgerufen am 28.1.2019).
58 *Allison* (Fn. 27).
59 *Skobel,* PinG 2018, 164; *Brüggemann,* K&R 2018, 1, 3; *Jülicher/Röttgen/v. Schönfeld,* ZD 2016, 358, 359.
60 Art.–29-Gruppe (Fn. 5), S. 13.

doch einen scheinbar wettbewerbsrechtlichen Charakter (Stichwort „überschießendes Wettbewerbsrecht“; vgl. oben). Zunächst ist diesbezüglich anzumerken, dass der Datenportabilität das Bild eines „Open Web“ zugrunde liegt. Diesem angestrebten Strukturprinzip liefe zuwider, würden kleine und mittelgroße „Walled Gardens“ erlaubt bleiben. Dass Datenportabilität auch den Missbrauch speziell von Marktmacht unterbindet, war historisch betrachtet insofern nur Teil des Ziels.

Weiterhin mag eine Marktmacht-Voraussetzung zwar bei substitutiven Anbieterwechseln sinnvoll sein. Die Förderung komplementärer Dienste würde dadurch jedoch behindert: Die meisten Banken dürften keine Marktmacht im engeren Sinne haben, genauso wenig der Hersteller eines intelligenten Stromzählers oder der eines Fitnesstrackers. Deren Daten wären dann jedoch komplett von Art. 20 ausgenommen; komplementäre Dienste könnten hierauf nicht aufbauen.

Abgesehen davon könnten kleinere Unternehmen sowieso von besonders großem Aufwand durch Art. 20 verschont bleiben, weil Art. 20 teilweise nur greift, wenn die Datenübertragung „technisch machbar“ ist (Abs. 2). Ob eine Übertragung „technisch machbar“ ist, soll dabei auch in Abhängigkeit von der Größe des Unternehmens beurteilt werden.[61]

4. Einordnung ins Datenschutzrecht

Die dritte offene Frage war, weshalb Datenportabilität im Datenschutzrecht eingeordnet wurde. Auf manche wirkt Art. 20 hier als „Fremdkörper“ (s. o.). Tatsächlich wirkt das Recht auf Datenportabilität ungewohnt neben dem ihm ähnlichen, etwa 40 Jahre älteren Auskunftsrecht (Art. 15 DSGVO). Dieses war bereits in der ersten Fassung des BDSG von 1977 enthalten (§§ 26 Abs. 2, 34 Abs. 2). Datenportabilität reagiert hingegen auf „Walled Gardens“, mit dem Ziel eines „Open Web“ – und damit auf stark veränderte tatsächliche Umstände. Die oben aufgezeigte Entstehungsgeschichte konnte das gefühlt „Fremde“ in Art. 20 vielleicht insofern etwas vertrauter machen.

Allerdings bleibt insgesamt richtig, dass das Ziel von Art. 20 auch großteils außerhalb des Datenschutzrechts liegt: Art. 20 soll substitutive und komplementäre Dienste stärken (s. o.). Art. 20 hat also eine stark innovationsfördernde Zielrichtung.

Dennoch scheint die Einordnung ins Datenschutzrecht nachvollziehbar. Zunächst ist klar, dass das Datenschutzrecht bei der Umsetzung von Datenportabilität entscheidend berücksichtigt werden musste. Bei Datenportabilität i. S. v. Art. 20 geht es um die Übertragung bzw. den Zugang zu personenbezogenen Daten. Dieser Bereich ist durch das Datenschutzrecht stark reguliert.[62] Insbesondere der Zweckbindungsgrundsatz führt dazu, dass personenbezogene Daten nicht frei gehandelt bzw. anschließend beliebig weiterverarbeitet werden dürfen.[63] Ob eine davon abweichende Umsetzung der Datenportabilität mit Art. 7, 8 GRCh vereinbar gewesen wäre, ist fraglich. Jedenfalls hätte sie einen Bruch mit den jetzigen Prinzipien des Datenschutzrechts bedeutet.

Dass die Datenportabilität nun die Form eines subjektiven Rechts des Nutzers erhielt, entspricht den historischen Forderungen, beispielsweise in der „Bill of Rights for Users of the Social Web“ (vgl. oben).[64] Eine alternative, wettbewerbsrechtlichere Regelung wäre vielleicht gewesen, dem Unternehmen, das die Daten erhalten soll, ein Recht auf den Zugang hierzu zuzusprechen. Für nicht-personenbezogene Daten wird so beispielsweise zur Zeit erörtert, ob Daten nicht „essential facilities“ darstellen können und daher Zugang zu ihnen zu gewähren ist.[65] Aufgrund von Art. 7, 8 GRCh hätte für personenbezogene Daten dann wohl eine Einwilligung des Betroffenen vorgeschrieben werden müssen. Mit Art. 20 entschied sich der Gesetzgeber jedoch für die erste Variante. Dadurch wird die Position des Betroffenen gestärkt. Der Betroffene hat (zumindest theoretisch, s. unten) die selbstbestimmte Initiative bzgl. der Datenübertragung.

Insofern ist es weder als richtig noch als falsch zu qualifizieren, dass Art. 20 im Datenschutzrecht geregelt wurde, sondern schlicht eine gesetzgeberische Entscheidung zugunsten des Betroffenen. Diese Entscheidung entspricht dabei den historischen Forderungen nach Datenportabilität.

5. Art. 20 als Gefahr für den Datenschutz

Allerdings ist nicht gesagt, dass der Betroffene Art. 20 auch tatsächlich so informiert und selbstbestimmt wahrnehmen wird, wie man sich dies gedacht haben mag. Es wäre nicht das erste Mal im Datenschutzrecht, dass ein restriktiv konzipiertes Instrument faktisch entgleitet. Mahnendes Beispiel ist insofern die Einwilligung. Auch die Einwilligung sollte im Ausgangspunkt dem Betroffenen eine selbstbestimmte Kontrolle über seine Daten ermöglichen, sie sollte ein „genuiner Ausdruck des Rechts auf informationelle Selbstbestimmung“[66] sein. In der Praxis wurde die Einwilligung stattdessen zum „Schlüssel zu einem nahezu unbegrenzten […] Zugang“ zu Daten des Betroffenen.[67]

Es scheint durchaus denkbar, dass Art. 20 faktisch ähnlich funktionieren könnte. Wird der Betroffene bspw. schlicht gefragt, ob er „seine Daten“ übertragen lassen will (wozu er das Recht gem. Art. 20 hat), ähnelt dies schon dem Äußeren nach einer Einwilligung. Dies könnte dazu führen, dass der Betroffene seine Daten oft, auch zu unbedeutenderen Zwecken, übertragen lässt. So konnte der Cambridge-Analytica-Skandal bspw. erst dadurch entstehen, dass Facebook-Nutzer im Ausgangspunkt ihre Daten übertragen ließen, um an einem Persönlichkeitsquiz teilzunehmen.[68]

Dabei ist fraglich, ob dem Betroffenen stets klar ist, wie viele Daten er mit Art. 20 übertragen lassen kann. Hier besteht ein fundamentaler Unterschied zur Einwilligung. Bei Art. 20 erhält der Verantwortliche wesentlich schneller wesentlich mehr Daten. Während die Einwilligung verlangt wird, um künftig Daten zu erheben, handelt es sich bei Art. 20 um Daten, die u. U. bereits über Jahre hinweg erhoben wurden. Um wie viele Daten es so gehen könnte, illustriert das Beispiel des Wiener Jura-Studenten *Max Schrems,* der 2011 öffentlichkeitswirksam seine Daten von

61 *Brüggemann,* K&R 2018, 1, 4; *v. Lewinski,* in: BeckOK (Fn. 3), Art. 20 Rn. 89; wohl auch *Herbst,* in: Kühling/Bucher (Fn. 2), Art. 20 Rn. 27.
62 *Peitz/Schweitzer,* NJW 2018, 275, 277.
63 *Peitz/Schweitzer,* NJW 2018, 275, 276.
64 S. o. Fn. 25; ebenso eher subjektiv-rechtlich: *Saad* (Fn. 26).
65 *Peitz/Schweitzer,* NJW 2018, 275, 279; *Körber,* NZKart 2016, 303, 308.
66 *Kühling,* in: BeckOK (Fn. 3), § 4a BDSG (a. F.) Rn. 1; vgl. *Masing,* NJW 2012, 2305, 2307.
67 *Simitis,* in: Simitis, BDSG, 8. Aufl. 2014, § 4a Rn. 4.
68 *Ingram* (Fn. 37).

Facebook herausverlangte und schon damals über tausend PDF-Seiten zurückerhielt.[69] Selbst wenn Art. 20 sich nicht auf all diese Daten erstreckt, dürfte es oft bei einem immensen Umfang an übertragbaren Daten bleiben. Nicht immer dürfte dies dem Betroffenen bewusst sein.

Der Gesetzgeber scheint dieses Risiko nicht wahrgenommen zu haben. Auch in der Literatur wurde darauf bisher, soweit ersichtlich, nicht hingewiesen. Möglicherweise geholfen hätte hier eine Informationspflicht über den Umfang der zu übertragenden Daten (Größe bzw. Anzahl der Datensätze). Eine solche Informationspflicht sieht die DSGVO jedoch nicht vor, vgl. Art. 13 f. In manchen Fällen dürfte der Verantwortliche immerhin aus Eigeninteresse vor der Übertragung warnen; dann nämlich, wenn er seine Daten nicht mit Konkurrenten teilen will. Für alle anderen Fälle bleibt hier jedoch eine gesetzgeberische Lücke.

IV. Fazit

Einen neuen Zugang zu Art. 20 wollte dieser Aufsatz eröffnen. Der Schlüssel dafür ist zunächst der historisch-ideologische Ursprung der Datenportabilität, der hier erstmals dargestellt wurde. Datenportabilität ist insofern auch als Gegenmaßnahme zu sog. „Walled Gardens“ zu sehen. Außerdem ist sie Ausdruck des Idealismus eines offenen Internet (sog. „Open Web“). Daneben wurde die Unterscheidung in „komplementäre“ und „substitutive Diensten“ herausgearbeitet.

Aufbauend auf diesen Erkenntnissen kann nun erklärt werden, weshalb soziale Netzwerke für Art. 20 so zentral waren, und möglicherweise auch, weshalb Art. 20 keine Marktmacht voraussetzt. Künftig können Auslegungsfragen mit diesem neuen Verständnis nuancierter behandelt werden.

Weiterhin ist nach hier vertretener Auffassung konsequent, dass Art. 20 im Datenschutzrecht verankert wurde, auch wenn dies bisher oft kritisiert wurde. Problematischer ist hingegen, dass dem Betroffenen oft nicht klar sein dürfte, welche Datenmassen er durch Art. 20 übertragen lassen kann. Daher könnte bei Art. 20 einer der seltenen Fälle vorgelegen haben, in denen mehr Informationspflichten dem Datenschutz auch in der Praxis gut getan hätten.

69 *Koops,* International Data Privacy Law 2014, 250, 252; *Thieme,* Frankfurter Rundschau (Online) vom 30.9.2011, http://www.fr.de/politik/datensicherheit-die-facebook-protokolle-a-1219420 (zuletzt abgerufen am 28.1.2019).

Report

Prof. Dr. Dagmar Gesmann-Nuissl*

Rechtsprechungsreport „Innovations- und Technikrecht“

I. Aktuelle Rechtsprechung zum Innovationsrecht

1. Urheberrechtlicher Schutz auf ein Geschmackserlebnis

Der EuGH hat mit Urteil vom 13.11.2018 (Az.: C-310/17) in der Rechtssache Levola Hengelo B.V. gegen Smilde Foods B.V. entschieden, dass der Geschmack eines Lebensmittels keinen Urheberrechtsschutz erlangen kann. Der Geschmack sei mangels Identifizierbarkeit nicht als „Werk“ einzustufen.

Die Levola Hengelo B.V. ist Inhaberin der geistigen Eigentumsrechte an einem Streichkäse aus Frischrahm und Kräutern, dem sog. „Heksenkaas“. Das Produkt wurde im Jahr 2007 von einem Frischproduktehändler in den Niederlanden kreiert, der seine Rechte an Levola abgetreten hat. Seit 2014 stellt die Smilde Foods B.V. ein vergleichbares Erzeugnis her, den „Witte Wievenkaas“, den sie in einer niederländischen Supermarktkette vertreibt. Levola ist der Auffassung, dass die Herstellung und der Vertrieb des „Witte Wievenkaas“ eine Verletzung ihres Urheberrechts darstelle, da der Geschmack des „Heksenkaas“ als eine eigene geistige Schöpfung anzusehen sei und die Beklagte dieses schöpferische Werk in unberechtigter Weise vervielfältige. Daher begehrte sie Unterlassen der Herstellung und des Vertriebs des Produkts. Nachdem das angerufene Gericht Gelderland[1] die Frage nach der Schutzfähigkeit des Geschmacks noch nicht aufgreifen musste, sollte diese Frage in der Berufungsinstanz vor dem Berufungsgericht Arnhem-Leeuwaarden[2] bedeutsam werden. Es setzte daher das Verfahren aus und legte dem EuGH die Fragen zur Auslegung des Werkbegriffs vor, insbesondere wollte das Gericht wissen, ob der Geschmack eines Lebensmittels überhaupt Schutz nach der Urheberrechtsrichtlinie 2001/29/EG (InfoSocRL) genießen könne.

Der EuGH entschied nun, dass der Geschmack eines Lebensmittels nur dann urheberrechtlichen Schutz genießen könne, wenn er als „Werk“ i. S. d. RL 2001/29/EG gelte (Rn. 34). Letzteres setze – auch in Ansehung an die Berner Übereinkunft, die bei der Auslegung zu berücksichtigen sei – voraus, dass das Werk zum einen Ausdruck eigener geistiger Schöpfung sei und zum anderen die zu schützende Ausdrucksform mit hinreichender Genauigkeit und Objektivität identifiziert werden könne (Rn. 35-40). Daran fehle

* Mehr über die Autorin erfahren Sie auf Seite III.

1 Gericht Gelderland, 10.6.2015, ECLI:NL:RBGEL:2015:4674.

2 Gerechtshof Arnhem-Leeuwarden, 23.5.2017, ECLI:NL:GHARL:2017:6697.

InTeR ISSN 2195-5743
Zeitschrift zum Innovations- und Technikrecht
Zitierweise InTeR **7. Jahrgang**

Herausgeber
Prof. Dr. Dr. Jürgen Ensthaler, Prof. Dr. Dagmar Gesmann-Nuissl, Prof. Dr. Stefan Müller
Schriftleitung
Lehrstuhl für Wirtschafts-, Unternehmens- und Technikrecht
Technische Universität Berlin, Sekr. H 41, Str. des 17. Juni 135, 10623 Berlin,
Tel +49/(0)30/314-29990, Fax +49/(0)30/314-29992,
E-Mail oberneyer@tu-berlin.de und S.Mueller@uni-paderborn.de
Herausgeberbeirat
Prof. Dr. Hans-Jürgen Ahrens, Dr. Wilhelm-Albrecht Achilles, Prof. Dr. Dr. Udo di Fabio, Lars Funk, Prof. Dr. Thomas Klindt, Dr. Roman Reiss, Philipp Reusch, Prof. Dr. Dr. Dr. h.c. mult. Franz Jürgen Säcker, Klaus Schülke, Christian Steinberger, Prof. Dr. Walther C. Zimmerli, Prof. Dr. Klaus J. Zink

dfv Mediengruppe

Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251,
60326 Frankfurt am Main, Tel: +49/(0)69/75 95-01, Fax: +49/(0)69/75 95-29 99,
www.innovationsundtechnikrecht.de www.technikrecht.info
In der dfv Mediengruppe, Fachmedien Recht und Wirtschaft, erscheinen außerdem folgende Fachzeitschriften: Betriebs-Berater (BB), Causa Sport (CASP), Compliance-Berater (CB), Datenschutz-Berater (DSB), Europäisches Wirtschafts- und Steuerrecht (EWS), Zeitschrift zum Innovations- und Technikrecht (InTeR), Kommunikation & Recht (K&R), Recht Automobil Wirtschaft (RAW), Recht der Finanzinstrumente (RdF), Recht innovativ (Ri), Recht der Internationalen Wirtschaft (RIW), Der Steuerberater (StB), Wettbewerb in Recht und Praxis (WRP), Zeitschrift für Umweltpolitik & Umweltrecht (ZfU), Zeitschrift für Wett- und Glücksspielrecht (ZfWG), Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (ZHR), Zeitschrift für das gesamte Lebensmittelrecht (ZLR), Zeitschrift für Vergleichende Rechtswissenschaft (ZVglRWiss), Zeitschrift für Neues Energierecht (ZNER).
Geschäftsführung
Angela Wisken (Sprecherin), Peter Esser, Markus Gotta, Peter Kley, Holger Knapp, Sönke Reimers
Aufsichtsrat
Klaus Kottmeier, Andreas Lorch, Catrin Lorch, Peter Ruß
Gesamtverlagsleitung Fachmedien Recht und Wirtschaft
RA Torsten Kutschke, Tel: +49/(0)69/75 95-27 01, Fax: +49/(0)69/75 95-27 80,
torsten.kutschke@dfv.de
Anzeigen
Lena Moneck, lena.moneck@dfv.de, Tel: +49/(0)69/75 95-27 13. Es gilt Preisliste 7.
Bereichsleitung Finanzen und Medienservices:
Thomas Berner, Tel. 069/7595-1147
Leitung Produktion: *Hans Dreier*, Tel. 069/7595-2463
Leitung Logistik: *Ilja Sauer*, Tel. 069/7595-2201
Erscheinungsweise, Bezugsbedingungen
4 Hefte pro Jahr. Abonnement € 259,00 (Versand nach Deutschland) bzw. € 242,94 (Versand ins Ausland) jährlich. Vorzugsabonnement für Studenten und Referendare € 74,00. Einzelheft € 65,–.
Für Mitglieder des Verein Deutscher Ingenieure e.V. € 119,65 jährlich.
Studentische VDI Mitglieder zahlen € 59,–.
In Kombination mit Recht Automobil Wirtschaft (RAW) statt € 418 nur € 369,–.
Preise jeweils inkl. Versandkosten und gesetzlicher Mehrwertsteuer.
Abonnementsgebühren sind im Voraus zahlbar. Das Jahresabonnement verlängert sich jeweils um 1 Jahr, wenn es nicht 3 Monate vor Ende des Bezugszeitraumes gekündigt wird.
Bankverbindungen: Frankfurter Sparkasse, Frankfurt am Main,
Kto.-Nr. 34 926 (BLZ 500 502 01)
Bestellungen
Deutscher Fachverlag GmbH, Regina Kühne,
Tel: +49/(0)69/75 95-2788, kundenservice@ruw.de

Gemäß § 5 Abs. 2 ff. des Hessischen Gesetzes über Freiheit und Recht der Presse wird mitgeteilt: Gesellschafter der Deutscher Fachverlag GmbH sind Herr Andreas Lorch, Heidelberg (42,1908 %); Frau Catrin Lorch, Königswinter (10,9385 %); Frau Anette Lorch, Büdingen (10,9367 %); Frau Britta Lorch, Berlin (10,9367 %) sowie die Deutscher Fachverlag GmbH, Frankfurt am Main (25 %).

Satz
DFV – inhouse production
Druck
medienhaus Plump GmbH | Rolandsecker Weg 33 | 53619 Rheinbreitbach