

## Grundwissen

# Aussicht auf das große Geld durch die DSGVO?

---

David Wasilewski, LL.B.



**Open Peer Review**

Dieser Beitrag wurde lektoriert von: Joela Worm und Lisa Krebber



---

David studiert Rechtswissenschaften an der Universität zu Köln und ist wissenschaftliche Hilfskraft an der Kölner Forschungsstelle für Medienrecht. Er interessiert sich für Themen an der Schnittstelle zwischen Recht und neuen Technologien und arbeitet im Bereich Legal Affairs in einem DeepTech und KI Start-up.

## W arum überhaupt Legal Tech?

Das Argument der Legal-Tech-Anbieterinnen ist es, jeder<sup>1</sup> ‚Zugang zum Recht‘ zu verschaffen. Es soll nicht mehr auf Spezialwissen oder die Größe des eigenen Geldbeutels ankommen. Es heißt, dass Ansprüche mit ‚kleinen‘ Streitwerten oftmals nicht mehr von Anwältinnen angenommen würden, da der Kosten-Nutzen-Faktor in einem unökonomischen Verhältnis stünde. Im Gegensatz dazu versuchen Legal-Tech-Anbieterinnen Forderungen oder Ansprüche von einer großen Anzahl an Per-

---

<sup>1</sup> Der Beitrag wurde im generischen Femininum verfasst. Natürlich sollen alle Personen angesprochen werden.

sonen zu akquirieren, um diese dann einzufordern oder vor Gericht durchzusetzen.<sup>2</sup> Die Bündelung und Automatisierung von einer Vielzahl von Forderungen steigert damit die Attraktivität, Rechtsstreitigkeiten auch mit ‚geringeren‘ Streitwerten auszufechten. Allerdings nur, wenn diese auf einem größtenteils vergleichbaren Sachverhalt beruhen. Dies wurde in der Vergangenheit eindrucksvoll am Beispiel von Fluggastrechten, aber auch bei Hartz-IV-Bescheiden gezeigt. Je mehr Verbraucherinnen dieses Geschäftsmodell nutzen, desto größer sind die Gewinnchancen. Die Gewinnmaximierungsmöglichkeiten für Legal-Tech-Anbieterinnen steigen, wenn Unternehmen mehrfache Verstöße gegen die Rechtsordnung begangen haben und deswegen negativ in der breiten Öffentlichkeit auffallen. Deshalb werden diese Angebote auch verstärkt durch Marketingmaßnahmen angepriesen. So sollen die ‚unwissenden‘ Bürgerinnen auf ihre möglichen Schadensersatzansprüche aufmerksam gemacht werden. Durch die Übernahme der Kosten und Risiken der Legal-Tech-Anbieterinnen gehen diese Personen auch vermehrt auf die Angebote ein, wodurch der ‚Zugang zum Recht‘ mehr Menschen ermöglicht werden soll. Einen Teil der Zahlungen, die aufgrund der durchgesetzten Ansprüche geleistet werden,

---

„Die Bündelung und Automatisierung von einer Vielzahl von Forderungen steigert die Attraktivität, Rechtsstreitigkeiten auch mit ‚geringeren‘ Streitwerten auszufechten.“

---

<sup>2</sup> Zu diesem Vorgehen und inwieweit dies für Rechtsanwälte möglich ist und was sich durch die große BRAO-Reform im Berufsrecht der Anwälte in Bezug auf Legal Tech ändert: *Deckenbrock*, CTRL 2/22, 86 ff.

behalten sich die Legal-Tech-Anbieterinnen sodann als Gegenleistung ein. Teilweise lassen sich die Legal-Tech-Anbieterinnen entsprechende Ansprüche auch abtreten.

Man könnte behaupten, dass so eine Win-win-Situation geschaffen wird. Jedenfalls aus Verbraucherinnensicht. Eine breitere Masse bedient sich dem Recht und die Anbieterinnen verdienen daran. Eine nicht bediente Marktlücke wurde gefunden und wird nun zunehmend durch Legal-Tech-Anbieterinnen gefüllt.

## B. Was hat das Datenschutzrecht damit zu tun?

### Art. 82 I DSGVO:

„Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.“

Diese Möglichkeiten der Forderungsbündelung bieten sich auch für Legal-Tech-Anbieterinnen seit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Jahre 2018 im Bereich des Datenschutzrechts. Hauptgrund dafür ist, dass jeder Person nach Art. 82 DSGVO bei einem Verstoß gegen die DSGVO durch Verantwortliche oder Auftragsverarbeiterinnen ein Schadensersatzanspruch zusteht. Allerdings kann sich das Unternehmen bei fehlendem Verschulden gem. Art. 82 III DSGVO exkulpieren. Ungewöhnlich ist dabei, dass neben materiellen auch immaterielle Schäden einen Anspruch begründen. Dies führt bei Cyberangriffen zu einer potenziell großen Anzahl von möglichen Berechtigten.

Jede an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.

Dies soll ein Beispiel illustrieren: Ein Unternehmen speichert unbeabsichtigt Kundinnendaten auf einem öffentlichen Server. Dadurch werden tausende von E-Mail-Adressen von Kundinnen öffentlich ins Netz gestellt. Diese Daten könnten andere Akteurinnen illegitimerweise nutzen, um eigene Zwecke zu verfolgen; beispielsweise um Werbemails an die E-Mail-Adressen zu senden. Das Unternehmen könnte hier gegen ihre Pflicht zur Sicherstellung eines angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten gem. Art. 32 II, 5 I lit. f DSGVO verstoßen haben. Zusätzlich müsste das Unternehmen gegebenenfalls den Vorfall gem. Art. 33 I 1 DSGVO an die zuständige Aufsichtsbehörde melden. Wenn diese dann eine Geldbuße verhängt (vgl. Art. 83 DSGVO), werden diese meist auch veröffentlicht.<sup>3</sup> Hinzu kommt, dass in diesen Fällen gem. Art. 34 I DSGVO auch unverzüglich eine Meldung an die betroffenen Personen erfolgen muss. Dieser Vorfall wird somit durch die Behörde und der Presse einer breiten Öffentlichkeit bekannt. Dies gibt den Legal-Tech-Anbieterinnen die Möglichkeit, mit Betroffenen in Kontakt zu treten und die Durchsetzung eines Schadensersatzanspruches nach Art. 82 I DSGVO anzubieten.

In Bezug auf den Umfang des Schadensersatzanspruches aus Art. 82 I DSGVO haben deutsche Gerichte bislang sehr unterschiedlich geurteilt. Bisher erstrecken sich zugesprochene Schadensersatzansprüche – auch und gerade aufgrund von immateriellen Schäden – von 25 € bis 5.000 €. Diese Ansprüche können von den Legal-Tech-Anbieterinnen gebündelt und damit tausendfach geltend gemacht werden. Je nach Höhe des individuellen Schadenersatzes kann dies schnell zu einer existenzbedrohenden Situation für das betroffene Unternehmen führen. Bei einem bekannten Fall bezüglich eines Datenleaks aus dem Jahre 2020 wurden etwa drei Millionen Kundinnendaten offengelegt. Das Potenzial einer Bündelung von entsprechenden Schadensersatzansprüchen ist in derartigen Fallgruppen besonders groß, da alle Geschädigten vom exakt gleichen Sachverhalt betroffen sind und mittels Legal Tech oft nur der Name der Betroffenen in der Klageschrift geändert werden muss. An dieser Stelle soll nicht diskutiert werden, ob Legal-Tech-Anbieterinnen den ‚Zugang zum Recht‘ verbessern. Es soll vielmehr darauf eingegangen werden,

ob die aufgezeigte Entwicklung in Bezug auf den immateriellen Schadensersatz begrüßenswert ist, das Recht auf Schutz personenbezogener Daten wirklich stärkt oder damit ‚nur‘ das große Geld verdient werden soll.

### C. Der immaterielle Schadensersatz

Deutsche Gerichte haben aufgrund der Regelung des § 253 I BGB in der Vergangenheit sehr restriktiv immaterielle Schäden anerkannt und diesen dann meist auch nur in relativ geringem Umfang stattgegeben. Anerkannte Fallgruppen sind etwa Persönlichkeitsrechtsverletzungen (dann über § 823 I BGB i.V.m. Art. 2 I, 1 I GG)<sup>4</sup> oder Körper- und Gesundheitsverletzungen (vgl. § 253 II BGB). Diese Beschränkungen können für die DSGVO jedoch nicht ohne weiteres gelten, da nach Art. 82 I DSGVO der immaterielle Schaden dem materiellen Schaden gleichgestellt wird. In Bezug auf Art. 82 DSGVO gibt es unterschiedliche Meinungen, wann ein immaterieller Schaden zugesprochen werden sollte und ein Urteil des EuGH dazu steht noch aus.

Wie sieht es aber in dem gerade geschilderten Fall hinsichtlich der Speicherung auf öffentlichen Servern aus? Dort sind E-Mail-Adressen abhandengekommen und andere Akteurinnen haben infolgedessen die Kundinnen mit Werbemails ‚belästigt‘ (vgl. § 7 I, II Nr. 2 UWG). In diesem Fall entsteht den Kundinnen kein materieller Schaden. Aufgrund von Art. 82 I DSGVO müssen die Gerichte nun entscheiden, ob, unter welchen Voraussetzungen und in welchem Umfang ein immaterieller Schaden ersatzfähig ist.

<sup>3</sup> Vgl. für eine Übersicht *Luther*, DSGVO Bußgeldatlas, [hier](#) abrufbar (Stand: 16.06.2022).

<sup>4</sup> Hierbei handelt es sich dogmatisch nicht um einen direkten immateriellen Schadensersatzanspruch, sondern um einen von der Verfassung vorgegebenen Entschädigungsanspruch, da insb. § 253 II BGB keinen immateriellen Schadensersatzanspruch für die Verletzungen von Persönlichkeitsrechten vorsieht.

## I. Vertretene Ansichten

### 1. Enge Auslegung

Vertreterinnen des ‚engen‘ Schadensbegriffs verlangen teilweise eine Erheblichkeitschwelle. Es soll eine Bagatellgrenze für immaterielle Schäden bestehen. Grund ist, dass solche Schäden nicht grenzenlos zugesprochen werden sollen, da eine genaue Höhe des Schadens immer nur subjektiv vom jeweiligen Gericht ermittelt werden könne. Dieser Argumentationslinie hat das BVerfG jedoch einen Riegel vorgeschoben, da dies von der Rechtsprechung des EuGH weder erschöpfend geklärt, noch unmittelbar aus der DSGVO beantwortet werden könne.<sup>5</sup>

Außerdem müsse von der Klägerin nachgewiesen werden, dass der Schaden aufgrund einer rechtswidrigen Verarbeitung eingetreten ist. Dies wird aus dem Wortlaut des Art. 82 II DSGVO entnommen. Dementsprechend führe gerade ein Verstoß gegen die DSGVO, welcher nicht in Verbindung mit der Verarbeitung steht, nicht zu einer Haftung. Damit soll auch einem Missbrauchsrisiko unter anderem durch Legal-Tech-Anbieterinnen entgegengewirkt werden. Dem kann entgegengehalten werden, dass der Absatz 1 des Art. 82 DSGVO die Anspruchsgrundlage ist. Dieser spricht dabei nur von einem „Verstoß gegen die DSGVO.“ Dieser beschränkt den Anspruch also nicht nur auf die Verarbeitung.

Insgesamt besteht die Tendenz, dass eher die Zivilgerichte eine restriktive Auslegung an den Tag legen, im Gegensatz zu den Arbeitsgerichten, welche etwa im Rahmen des AGG nach § 15 II AGG – auch aus Abschreckungsgründen – höhere immaterielle Schäden zusprechen.

### 2. Weite Auslegung

Vertreterinnen des ‚weiten‘ Schadensbegriffs berufen sich unter anderem auf Art. 83 III DSGVO und Erwägungsgrund 146 S. 3 der DSGVO, der auch eine Abschreckungsfunktion des Schadensersatzanspruchs beinhalte. Erwägungsgrund 146 S. 3 besagt, dass **„der Begriff des Schadens [...] weit auf eine Art und Weise ausgelegt werden [sollte], die den Zielen dieser Verordnung in vollem Umfang entspricht“**. Daraus ist jedoch nicht - anders als teilweise angenommen - direkt das Ziel eines Abschreckungspotenzials des Schadensbegriffes abzulesen. Auch kann dies nicht aus systematischen Überlegungen abgeleitet werden. Im Wortlaut des Art. 83 I DSGVO wird für die Verhängung von Geldbußen durch Behörden explizit gefordert, dass diese „abschreckend“ sein sollen. Die europäische Gesetzgeberin hätte dies in Art. 82 DSGVO aufnehmen müssen, wenn sie eine vergleichbare Bemessungsregel angestrebt hätte.

### II. Weitere Aspekte

Im Hinblick auf Legal-Tech-Anbieterinnen kann überlegt werden, ob ein (zu) ‚weit‘ zugesprochener Schadensersatz dazu führen würde, dass Verantwortliche oder Auftragnehmerinnen in Gefahr laufen, hohe Verluste zu erleiden. Dazu gehören, auf der einen Seite, die massenhaften Zahlungen an Betroffene (durch die massenhaft eingereichten Klagen) bei einer Niederlage vor Gericht. Auf der anderen Seite kommt ein enormer Reputationsverlust schon bei Bekanntwerden eines potenziellen Verstoßes in Betracht, welcher bei einer Verurteilung nochmals steigen würde. Darüber hinaus wird darüber gestritten, ob immaterielle Schadensersatzansprüche gem. Art. 82 I DSGVO überhaupt abtretungsfähig i.S.d. §§ 398 ff. BGB sind. Dieser sei aufgrund des höchstpersönlichen Charakters des Anspruchs nicht übertragbar.

<sup>5</sup> BVerfG NJW 2021, 1005 m.w.N.



## D. Fazit

Ein Schadensersatzanspruch in Bezug auf Datenschutzverstöße und insbesondere auch auf immaterielle Schäden ist längst überfällig. Dieser stellt eine wichtige Stärkung des Rechts auf Schutz personenbezogener Daten dar. In Bezug auf die Frage, wann dieser Anspruch erteilt werden sollte, ist aber genauestens darauf zu achten, wie hoch der Ersatz ausfallen sollte. Aufgrund der vergangenen Rechtsprechung des EuGH ist davon auszugehen, dass entsprechende Entscheidungen eher zugunsten des weiten Schadensersatzbegriffs ausfallen werden.

Insoweit ist zu hoffen, dass die Richterinnen eine Entscheidung treffen, die den Interessen der Betroffenen und denen der Verantwortlichen ausgewogen gerecht wird. Zu hohe Anforderungen an das Bestehen eines ersatzfähigen immateriellen Schadens könnten die DSGVO nach anfänglichem Schrecken zum zahnlosen Tiger verkommen lassen. Gleichzeitig besteht durch die Angebote der Legal-Tech-Anbieterinnen die Gefahr einer ausufernden Geltendmachung von Schadensersatzansprüchen, die für die betroffenen Unternehmen erhebliche Haftungsrisiken bergen. Deshalb müssen Unternehmen verstärkt in ihre Cybersicherheit, Compliance und Datenschutzorganisation investieren, um solche Vorfälle zu vermeiden. Es kommt somit auch zu einer immer stärkeren Verzahnung von Cybersicherheit und Datenschutz.

Zurück zum  
Inhaltsverzeichnis

## Weiterführende Hinweise:

Überblicksartig *Wybitul/Leibold*, ZD 2022, 207.

Zur Rechtsprechungspraxis *Paal/Aliprandi*, ZD 2021, 241.

Letztlich für ein weites Verständnis *Buchner/Wessels*, ZD 2022, 251.

In Bezug auf die europarechtskonforme Auslegung *Korch*, NJW 2021, 978.

Ausführungen zu Art. 82 DSGVO im europäischen System *Hellgardt*, ZEuP 2022, 7.

Gegen die Abtretbarkeit von immateriellen Schäden *Spittka*, GRUR-Prax 2019, 475.



### Talking Legal Tech – Folge 1

„Was ist Legal Tech? mit Nico Kuhlmann“



### Talking Legal Tech – Folge 43

„Rightmart, Flightright, Geblitzt.de & Co - Der Stand im B2C-Rechtsmarkt mit Marco Klock von Rightmart“



### Talking Legal Tech – Folge 60

„UiPath - Ein Bot für alle Jurist:innen durch Robotic Process Automation (RPA), Joachim Grouven?“

# CTRL

2/22

2. Jahrgang, 1. Ausgabe  
[www.legaltechcologne.de/ctrl](http://www.legaltechcologne.de/ctrl)

Cologne Technology  
Review & Law



[Hier geht es zur ganzen Ausgabe!](#)

Reise in 15 Beiträgen durch die Legal-Tech-Welt:

[Von Kolumbien bis nach Finnland](#)  
[und von Compliance bis eSport.](#)



LEGAL TECH LAB  
COLOGNE